

February 2, 2005



Acquisition

Implementation of Interoperability
and Information Assurance Policies
for Acquisition of Air Force Systems
(D-2005-034)

Department of Defense
Office of the Inspector General

Quality

Integrity

Accountability

Additional Copies

To obtain additional copies of this report, visit the Web site of the Inspector General of the Department of Defense at <http://www.dodig.osd.mil/audit/reports> or contact the Secondary Reports Distribution Unit, Audit Followup and Technical Support 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 Audit Followup and Technical Support at (703) 604-8940 (DSN 664-8940) or fax (703) 604-8932. Ideas and requests can also be mailed to:

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

DEPARTMENT OF DEFENSE

hotline

To report fraud, waste, mismanagement, and abuse of authority.

Send written complaints to: Defense Hotline, The Pentagon, Washington, DC 20301-1900
Phone: 800.424.9098 e-mail: hotline@dodig.osd.mil www.dodig.osd.mil/hotline

Acronyms

C4I	Command, Control, Communications, Computers, and Intelligence
DITSCAP	DoD Information Technology Security Certification Accreditation Program
GIG	Global Information Grid
IA	Information Assurance
KPP	Key Performance Parameter
NS	National Security
ORD	Operational Requirements Document
SSAA	System Security Authorization Agreement
TEMP	Test and Evaluation Master Plan



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

February 2, 2005

MEMORANDUM FOR ASSISTANT SECRETARY OF THE AIR FORCE (FINANCIAL
MANAGEMENT AND COMPTROLLER)

SUBJECT: Report on the Implementation of Interoperability and Information Assurance
Policies for Acquisition of Air Force Systems (Report No. D-2005-034)

We are providing this report for information and use. This report is the fourth in a series of reports that discusses the implementation of interoperability and information assurance policies for the acquisition of DoD systems. This report addresses the implementation of those policies within the Air Force. In preparing the final report, we considered comments on the draft report from the Director, Joint Staff and the Air Force Chief Information Officer.

Comments on the draft of this report conformed to the requirements of DoD Directive 7650.3 and left no unresolved issues. Therefore, no additional comments are required.

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

By direction of the Deputy Inspector General for Auditing:

A handwritten signature in cursive script, reading "Mary L. Ugone".

Mary L. Ugone
Assistant Inspector General
Acquisition and Technology Management

Office of the Inspector General of the Department of Defense

Report No. D-2005-034

February 2, 2005

(Project No. D2002AE-0188)

Implementation of Interoperability and Information Assurance Policies for Acquisition of Air Force Systems

Executive Summary

Who Should Read This Report and Why? Civil servants and military managers who are responsible for interoperability and information assurance requirements of Air Force acquisition programs should read this report. This report addresses the importance of adhering to DoD and Air Force interoperability and information assurance policies to exchange secure information with other DoD and allied systems.

Background. This report is the fourth in a series of reports on the implementation of interoperability and information assurance policies for the acquisition of DoD systems. This report addresses the implementation of those policies within the Air Force; the first report addressed the implementation of those policies within the Office of the Secretary of Defense and the Defense agencies; the second report addressed the implementation of those policies within the Army, and the third report addressed the implementation of those policies within the Navy.

Results. The Air Force made progress updating and certifying its capabilities documents to incorporate interoperability requirements. However, Air Force system program offices were not always preparing required command, control, communications, computers, and intelligence support plans (renamed information support plans) or obtaining Joint Staff supportability certifications for programs with interoperability requirements. As a result, milestone decision authorities do not have adequate information to determine whether a system should proceed further through the acquisition process. The Air Force Chief Information Officer, in collaboration with the Air Force Deputy Chief of Staff for Warfighting Integration, needs to issue policy to require program managers to prepare information support plans and obtain supportability certifications before program decision reviews and before fielding the system (finding A).

After DoD issued guidance on net-ready key performance parameters, the Air Force made progress identifying testable information assurance requirements in operational requirements documents for Air Force programs with interoperability and supportability requirements. However, Air Force system program offices did not always prepare required system security authorization agreements for systems with information technology requirements. Without those agreements, Air Force operational testers do not have information needed to assess compliance with security requirements affecting system confidentiality, integrity, availability, and accountability. The Air Force Chief Information Officer needs to verify that system program offices prepare system security authorization agreements for systems with information technology requirements (finding B).

The Air Force had not populated and maintained its portion of the Global Information Grid asset inventory for acquisition programs containing information technology

requirements. As a result, DoD cannot ensure that its acquisition programs have the most effective, efficient, and secure information-handling capabilities available. The Inspector General of the Department of Defense issued a report (Report No. D-2005-033, "Implementation of the Interoperability and Information Assurance Policies for Acquisition of Navy Systems," February 2, 2005) on the Navy's implementation of interoperability and information assurance policies in acquiring DoD systems. The report includes a recommendation on DoD guidance in populating and maintaining the GIG asset inventory and includes a recommendation addressing the issue (finding C). See the Findings section of the report for the detailed recommendations.

Management Comments. We received comments from the Director, Joint Staff and from the Air Force Chief Information Officer, who also responded for the Air Force Deputy Chief of Staff for Warfighting Integration. The Director agreed with the recommendations. The Chief Information Officer concurred with the recommendations and made suggestions to enhance the completeness and accuracy of this report. 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.

Table of Contents

Executive Summary	i
Background	1
Objectives	3
Findings	
A. Implementing Interoperability Policies	4
B. Testing Air Force Acquisition Programs for Information Assurance	10
C. Populating and Maintaining the Global Information Grid's Asset Inventory	17
Appendixes	
A. Scope and Methodology	22
B. Prior Coverage	24
C. Glossary	25
D. Global Information Grid	31
E. Results of the Air Force Interoperability and Information Assurance Survey	33
F. Air Force Programs Surveyed	40
G. Audit Response to Air Force Comments on the Report	41
H. Report Distribution	44
Management Comments	
Joint Staff	47
Department of the Air Force	48

Background

This report is the fourth in a series of reports on the implementation of interoperability and information assurance (IA) policies within DoD. This report addresses the Air Force's implementation of those policies in the Joint Capabilities Integration and Development System,¹ inclusion of adequate interoperability key performance parameters (KPPs)² in requirements documents, and the interoperability certification process for Air Force acquisition programs. Appendix C provides a glossary of technical terms used in this report.

Chairman of the Joint Chiefs of Staff Testimony on the President's Proposed Defense Program for FY 2005. On February 4, 2004, General Pace, the Vice Chairman of the Joint Chiefs of Staff, testified before the U.S. House of Representatives Committee on Armed Services. General Pace described how information sharing is critical for planning and executing military operations. He testified that:

Since this is a global war requiring an international effort, we must also improve coalition command and control capabilities, and consolidate the numerous networks that exist today. These disparate networks hinder our ability to plan in a collaborative environment and exercise timely and effective command and control with our multinational partners.

We must also review policies and implement technology that safeguard our vital sensitive information while ensuring critical operational information is shared with all those who fight beside us. JFCOM [Joint Forces Command] has been tasked to take the lead in identifying specific multinational information sharing requirements and recommending policy changes. Our goal is to establish a multinational family of systems with common standards as part of the Global Information Grid enterprise services. I view this as a top priority and ask for Congressional support — information sharing with our allies is critical to winning the War on Terrorism.

Top 10 Priorities. The Secretary of Defense issued a list of the top 10 DoD priorities. One priority is to strengthen joint warfighting capabilities, which was also one of the Secretary's priorities for FY 2004. The intent of this priority is to improve joint concepts of operation through integrating air, land, and

¹Chairman of the Joint Chiefs of Staff Instruction 3170.01C, "Joint Capabilities Integration and Development System," June 24, 2003, replaced the interoperability requirements generation process with the Joint Capabilities Integration and Development System. Subsequently, Chairman of the Joint Chiefs of Staff Instruction 3170.01D, "Joint Capabilities Integration and Development System," March 12, 2004, superseded Chairman of the Joint Chiefs of Staff Instruction 3170.01C.

²DoD Directive 4630.5, "Interoperability and Supportability of Information Technology (IT) and National Security Systems (NSS)" May 5, 2004, established the net-ready key performance parameter to replace the interoperability key performance parameter. However, this report addresses the interoperability key performance parameter because the programs reviewed during the audit were subject to the previous version of DoD Directive 4630.5, which addressed interoperability key performance parameters.

sea capabilities, and strengthen joint exercises and joint training. By enhancing interoperability and communication among warfighters, joint warfighting capabilities will be strengthened.

Joint Operations Concepts. In November 2003, the Secretary of Defense issued the Joint Operations Concepts (the Concepts), which elaborated on the joint warfighting requirements addressed in Joint Vision 2020 and provided the operational concept for the transformation of the Armed Forces to achieve joint force capabilities. The Concepts state that, to facilitate decision superiority, the joint force will use technology to provide actionable and precise intelligence at all levels of war, which requires a singular battlespace network to enable continuous and collaborative campaign planning and an adaptive command and control organization. The joint force must gain and maintain information superiority to facilitate decision superiority. Upon achieving decision superiority, the joint force can achieve full spectrum dominance when the joint force is integrated, networked, and interoperable with interagency and multinational partners. Full spectrum dominance is the defeat of any adversary or the control of any situation across the full range of military operations. Information superiority, decision superiority, and full spectrum dominance are elements of the Global Information Grid (GIG), which is discussed in Appendix D.

Scope of Air Force Programs Surveyed. We judgmentally selected 40 Air Force acquisition programs for review. Those programs were funded with research and development funds and were required to interface with other systems. We sent a questionnaire to the system program offices for those programs to survey their awareness of interoperability and IA requirements. Appendix E contains the results of the survey, and Appendix F lists the Air Force acquisition programs surveyed. In addition, we requested each system program office to provide the following documents:

- operational requirements document (ORD),³
- command, control, communications, computers, and intelligence (C4I) support plans,⁴
- test and evaluation master plan (TEMP), and
- system security authorization agreement (SSAA).

Overall Audit Project. This project is a continuation of work reported in the Inspector General of the Department of Defense Report No. D-2003-011,

³DoD Instruction 5000.2, "Operation of the Defense Acquisition System," May 12, 2003, states that, during system development and demonstration, the capabilities development document instead of the ORD will state the detailed operational performance parameters. Further, the Instruction states that the capabilities production document instead of the ORD will state the operational requirements resulting from system development and demonstration and will detail the performance expected of the production system. However, this report uses the term ORD because the programs reviewed during the audit usually provided ORDs.

⁴DoD Instruction 4630.8, "Procedures for Interoperability and Supportability of Information Technology (IT) and National Security Systems (NSS)," June 30, 2004, states that the information support plan replaces the C4I support plan specified in the DoD 5000 series documents. However, this report uses the term C4I support plan because the programs reviewed during the audit usually provided C4I support plans.

“Implementation of Interoperability and Information Assurance Policies for Acquisition of DoD Weapon Systems,” October 17, 2002, which addressed whether the Office of the Secretary of Defense and the Defense agencies were effectively implementing DoD interoperability and IA policies. A subsequent audit, Report No. D-2004-008, “Implementation of Interoperability and Information Assurance Policies for Acquisition of Army Systems,” October 15, 2003, addressed the adequacy of interoperability and IA requirements for systems in the Army. Further, Inspector General of the Department of Defense Audit Report No. D-2005-033, “Implementation of the Interoperability and Information Assurance Policies for Acquisition of Navy Systems,” February 2, 2005, assessed how effectively the Navy was implementing DoD interoperability and IA policies.

Objectives

The primary audit objective was to evaluate whether the Air Force was effectively implementing DoD interoperability and IA policies for its acquisition programs. Specifically, the audit determined whether the Air Force was effectively identifying system interoperability and IA requirements in the requirements generation process. See Appendix A for a discussion of the audit scope and methodology. See Appendix B for prior coverage related to the audit objectives.

A. Implementing Interoperability Policies

The Air Force made progress updating and certifying its capabilities documents to incorporate interoperability requirements. Specifically, 38 of the 40 programs surveyed were required to have certified interoperability requirements. Of those 38 programs, 31 had updated capabilities documents to incorporate interoperability requirements and had obtained or were obtaining Joint Staff interoperability requirements certifications for those documents. However, the Air Force system program offices did not develop C4I support plans (renamed information support plans) as required or obtain Joint Staff supportability certifications for programs with interoperability requirements. Specifically, 36 of the 40 programs surveyed required certified C4I support plans; of the 36 programs, only 26 prepared C4I support plans and only 5 obtained supportability certification for those plans. The C4I support plans were not prepared and certified because the Air Force Chief Information Officer did not ensure that the Office of the Air Force Deputy Chief of Staff for Warfighting Integration updated policy to require program managers to prepare and submit certified C4I support plans before applicable program decision reviews. Without certified C4I support plans, milestone decision authorities do not have adequate information to determine whether a system should proceed further through the acquisition process. Specifically, the milestone decision authorities do not know whether the system is compatible with the existing C4I infrastructure for other DoD acquisition programs and whether it is able to meet warfighter interoperability and information needs.

Interoperability Requirements and Certification

Interoperability Requirements and Certification Policy. DoD Directive 4630.5, “Interoperability and Supportability of Information Technology (IT) and National Security Systems (NSS)” May 5, 2004; Chairman of the Joint Chiefs of Staff Instruction 3170.01D, “Joint Capabilities Integration and Development System,” March 12, 2004; Chairman of the Joint Chiefs of Staff Instruction 6212.01C, “Interoperability and Supportability of Information Technology and National Security Systems,” November 20, 2003; and Air Force Instruction 10-601, “Capabilities Based Requirements Development,” July 30, 2004, provide policy and responsibilities for interoperability and supportability of information technology and National Security (NS) systems.

DoD Policy. DoD Directive 4630.5 established the net-ready KPP that replaced the interoperability KPP and incorporated net-centric concepts for achieving information technology and NS system interoperability and supportability. The Directive requires, as did the previous version of the policy, the DoD Components to identify interoperability and supportability requirements for information technology and NS systems during the acquisition process and to update them as necessary throughout the system’s life.

Joint Staff Policy. Chairman of the Joint Chiefs of Staff Instruction 3170.01D requires all capability documents to include a net-ready KPP. In addition, Chairman of the Joint Chiefs of Staff Instruction 6212.01C requires the Director for Command, Control, Communications, and Computers Systems Directorate (J-6), Office of the Chairman of the Joint Chiefs of Staff (Joint Staff J-6) to certify interoperability requirements in the ORDs before milestone decisions for system acquisition programs.

Air Force Policy. Air Force Instruction 10-601 states that the net-ready KPP is documented in the capability development document and the capability production document.⁵

Review of Operational Requirements Documents. The Air Force Director of Operational Capability Requirements, Office of the Deputy Chief of Staff for Air and Space Operations made progress incorporating interoperability or net-ready KPP requirements into its capabilities documents and obtaining the Joint Staff J-6 interoperability requirements certification. Of the 40 Air Force programs surveyed, only 38 were required to have an interoperability or a net-ready KPP because the Air Force had fielded or placed 2 of the programs into operational use before DoD established the requirements for the interoperability or net-ready KPPs. As of May 2003, the Joint Staff J-6 either had certified or was certifying the interoperability requirements in the ORDs for 25 of the 38 Air Force programs. In August 2004, the number of ORDs with interoperability or net-ready KPPs that the Joint Staff J-6 had certified or was certifying had increased to 31 out of the 38 Air Force programs surveyed. By continuing to prepare requirements documents with certified net-ready KPPs, the Air Force programs surveyed have verifiable performance measures and associated metrics for the milestone decision authority to use at program milestone reviews to determine whether the systems have timely, accurate, and complete exchange and use of information to satisfy the warfighter needs.

C4I Support Plans

C4I Support Plan Policy. DoD Instruction 4630.8, “Procedures for Interoperability and Supportability of Information Technology (IT) and National Security Systems (NSS),” June 30, 2004; Chairman of the Joint Chiefs of Staff Instruction 6212.01C; and Assistant Secretary of the Air Force (Acquisition) Memorandum, “Command, Control, Communications, Computers, and Intelligence (C4I) Support Plan (C4ISP) and System Certifications Policy,” April 25, 2002,⁶ provide guidance on preparing and updating C4I support plans.

⁵The capability development document and the capability production document were previously referred to as the ORD.

⁶This memorandum superseded Assistant Secretary of the Air Force (Acquisition) Memorandum, “Air Force Command, Control, Communications, Computers, and Intelligence Support Plan (C4ISP) Policy,” June 13, 2000, which required Air Force system program offices to develop C4I support plans for all new or developing acquisition programs that connect with Air Force communications and information infrastructures or that give the warfighter or DoD decision maker an operational capability that depends on timely, effective C4I infrastructure support.

DoD Instruction. DoD Instruction 4630.8 states that the C4I support plan is a mechanism to identify and resolve implementation issues related to the infrastructure for information technology and NS systems and interface requirements. The Instruction requires program managers to:

- prepare an information support plan (C4I support plan) that identifies the capabilities that the information technology and NS systems require or the information needed to meet the proposed capability;
- develop the information support plan (C4I support plan) concurrently and collaboratively with the associated capability development document or capability production document (referred to as ORDs in the report), unless exceptions are noted in an acquisition decision memorandum; and
- update the information support plan (C4I support plan) as the program matures or proceeds through multiple evolutionary blocks or phases.

Further, the Instruction requires the Air Force Chief Information Officer to:

- ensure compliance with DoD Instruction 4630.8;
- ensure that the milestone decision authority or cognizant fielding authority has an approved information support plan (C4I support plan) before the system enters into the system development and demonstration phase of the acquisition process; and
- comply with Joint Staff procedures for interoperability certification.

Joint Staff Instruction. Chairman of the Joint Chiefs of Staff Instruction 6212.01C requires the Joint Staff J-6 to certify to the Assistant Secretary of Defense for Networks and Information Integration/DoD Chief Information Officer⁷ that C4I support plans, regardless of acquisition category, address information technology and NS system infrastructure requirements adequately and the availability of bandwidth and spectrum support, funding, and personnel; and identify dependencies and interface requirements among DoD acquisition programs. The Instruction also requires the Military Departments to provide guidance and direction to all program managers, specifying that all systems must be certified in accordance with applicable policy.

Air Force Memorandum. The Assistant Secretary of the Air Force (Acquisition) Memorandum requires Air Force system program managers to:

- Develop and maintain a C4I support plan for their systems.
- Conduct a self-assessment to determine whether the C4I surveillance and reconnaissance document for their system supports the requirements. If the self-assessment determines that a C4I support

⁷Formerly named the Assistant Secretary of Defense (Command, Control, Communications, and Intelligence).

plan is not required because a C4I surveillance and reconnaissance supportability issue does not exist, the program manager must prepare a justification letter and forward it to the Director for Information Dominance, Office of the Assistant Secretary of the Air Force (Acquisition) to obtain approval for not preparing a C4I support plan. The Director coordinates approval or disapproval with the Assistant Secretary of Defense for Networks and Information Integration/DoD Chief Information Officer and the Joint Staff, as required.

- Determine whether a modification or upgrade requires a C4I support plan. If the C4I support plan is not required, the system program manager will forward a justification letter with a self-assessment to the Director for Information Dominance for approval.

Review of C4I Support Plans. During our review of the 40 Air Force programs surveyed, we determined that not all Air Force program managers were preparing C4I support plans and obtaining Joint Staff supportability certification of those plans.

C4I Support Plan Preparation. We requested C4I support plans from the 40 Air Force system program offices⁸ and received 30 C4I support plans. Thirty-six of the 40 Air Force programs were past the system development and demonstration milestone decision, and 4 were yet to have a system development and demonstration milestone decision. As a result, the program managers for those 36 programs should have prepared a C4I support plan. However, only 26 of the 36 programs had a C4I support plan.⁹ The remaining 10 Air Force system program offices stated that they did not prepare a C4I support plan because:

- the program existed before the C4I support plan requirement (legacy system) (five system program offices),
- a waiver was issued (one system program office),
- the program office did not feel it was required to develop a C4I support plan (two system program offices), and
- the program office was in the planning stages of developing its C4I support plan (two system program offices).

Joint Staff Supportability Certification. Of the 26 C4I support plans obtained for the 36 Air Force programs required to have a C4I support plan:

- 5 C4I support plans had received the required supportability certification from the Joint Staff J-6,

⁸We requested C4I support plans by a data request and followed up with the program offices to verify the latest status of the C4I support plans.

⁹The program managers provided C4I support plans for the four programs that had not yet undergone a system development and demonstration milestone decision; however, those plans needed to be certified.

-
- 7 C4I support plans had been in the required supportability certification process for more than 1 year without advancement, and
 - 14 C4I support plans had not been submitted to the Joint Staff J-6 for the required supportability certification process.

Although DoD policy requires the Air Force Chief Information Officer to ensure that program managers have an approved and certified C4I support plan before the system enters into the system development and demonstration phase, the Air Force Chief Information Officer did not have procedures established to enforce compliance with the DoD policy. According to personnel in the Office of the Air Force Chief Information Officer, the procedures should have been promulgated; however, as the result of a reorganization of the Office of the Assistant Secretary of the Air Force (Acquisition) in 2001, the responsibility for preparing the procedures became that of the Office of the Air Force Deputy Chief of Staff for Warfighting Integration. Personnel in the Office of the Air Force Deputy Chief of Staff for Warfighting Integration confirmed the responsibility and stated that they were updating Air Force Instruction 33-108, "Compatibility, Interoperability, and Integration of Command, Control, Communications, and Computers (C4) Systems," July 14, 1994, to include C4I support plan guidance that complies with DoD Instruction 4630.8.

Effects of Developing and Certifying C4I Support Plans

Without Air Force system program offices preparing and certifying C4I support plans, milestone decision authorities do not have adequate information to determine whether a system should proceed further through the acquisition process. Specifically, the milestone decision authorities do not know whether the system is compatible with the existing C4I infrastructure for other DoD acquisition programs and whether it is able to meet warfighter interoperability and information needs.

Management Comments on the Finding and Audit Response

A summary of management comments on the finding and audit responses is in Appendix G.

Recommendation and Management Comments

A. We recommend that the Air Force Chief Information Officer, in collaboration with the Air Force Deputy Chief of Staff for Warfighting Integration, issue policy to require program managers to prepare information support plans and obtain supportability certifications before program decision reviews and before fielding the system, in accordance with DoD Instruction 4630.8, “Procedures for Interoperability and Supportability of Information Technology (IT) and National Security Systems (NSS),” June 30, 2004.

Air Force Chief Information Officer Comments. The Air Force Chief Information Officer, who also responded for the Air Force Deputy Chief of Staff for Warfighting Integration, concurred, stating that Air Force Policy Directive 33-2, “Information Assurance Program,” will address the requirement for program managers to prepare information support plans and obtain supportability certification before program decision reviews and before fielding the system. Further, the Air Force Chief Information Officer stated that the Directive will be staffed in early 2005 and that his staff contacted the Office of the Assistant Secretary of the Air Force (Acquisition) to ensure that Air Force acquisition guidance also included the correct guidance. For the complete text of the Air Force Chief Information Officer’s comments, see the Management Comments section of the report.

Director, Joint Staff Comments. Although not required to comment, the Director agreed with the recommendation, stating that the Joint Staff will support the recommendation through its role as a principal member of the Interoperability Test Panel. For the complete text of the Director’s comments, see the Management Comments section of the report.

B. Testing Air Force Acquisition Programs for Information Assurance

After DoD issued guidance on net-ready KPPs, the Air Force made progress in identifying testable IA requirements in ORDs for Air Force programs with interoperability and supportability requirements. However, Air Force system program offices were not always preparing required SSAAs for systems with information technology requirements. Only 26 of 40 system program offices surveyed had prepared SSAAs. For the remaining 14 system program offices, the SSAAs were not prepared because the Air Force Chief Information Officer did not verify that the respective system program offices had prepared SSAAs when the system was subject to the DoD Information Technology Security Certification Accreditation Program (DITSCAP). For those programs with SSAAs, the Air Force operational testers were coordinating with the SSAA signatories to minimize duplicative testing efforts. Without an SSAA, the testers do not have information needed to assess compliance with the technical and nontechnical implementation of the security design and to determine whether the system program office properly implemented security features affecting system confidentiality, integrity, availability, and accountability.

Defining Information Assurance Requirements for Testing

Information Assurance Requirements Policy. DoD Directive 4630.5; DoD Directive 8500.1, “Information Assurance,” October 24, 2002; DoD Instruction 8500.2, “Information Assurance Implementation,” February 6, 2003; DoD Instruction 8580.1, “Information Assurance (IA) in the Defense Acquisition System,” July 9, 2004; Chairman of the Joint Chiefs of Staff Instruction 3170.01D; Chairman of the Joint Chiefs of Staff Instruction 6212.01C; and Air Force Instruction 10-601 provide policy and responsibilities for information assurance of information technology and NS systems.

DoD Directive 4630.5. DoD Directive 4630.5 requires the DoD Components to develop and use net-ready KPPs to assess IA attributes for the technical exchange of information and the operational effectiveness of that exchange.

DoD Directive 8500.1. DoD Directive 8500.1 requires the DoD Components to identify and include IA requirements in the design, acquisition, installation, operation, upgrade, or replacement of all DoD information systems for which they have responsibility.

DoD Instruction 8500.2. DoD Instruction 8500.2 requires IA managers to ensure that IA inspections, tests, and reviews are coordinated. In addition, the Instruction states that:

- the ability to test and verify is an essential competency of the DoD IA program, and

-
- the IA objective condition is testable, IA compliance is measurable, and the activities required to achieve the IA control are assignable and accountable.

DoD Instruction 8580.1. DoD Instruction 8580.1 implements acquisition policy for IA, assigns responsibilities, and prescribes procedures to integrate IA into the DoD acquisition system. The Instruction requires:

- DoD Components to implement IA in all DoD system acquisitions in accordance with the DoD 5000 series; and
- program managers to fully integrate IA into all phases of their acquisition, upgrade, or modification programs, including initial design, development, testing, fielding, and operation.

Joint Staff Policy. Chairman of the Joint Chiefs of Staff Instruction 3170.01D requires all capability documents to include a net-ready KPP.¹⁰ In addition, Chairman of the Joint Chiefs of Staff Instruction 6212.01C requires the net-ready KPP, including the information assurance component, to consist of measurable, testable, or calculable characteristics and performance metrics required for timely, accurate, and complete exchange and use of information.

Air Force Policy. Air Force Instruction 10-601 states that the net-ready KPP is documented in the capability development document and the capability production document.

Review of Operational Requirements Documents. Before DoD issued guidance on net-ready KPPs, the Air Force did not always identify testable IA requirements in ORDs for Air Force programs with interoperability and supportability requirements. During the audit, the Air Force began to incorporate IA requirements into its capability documents as part of the net-ready KPP requirements.

During our review of the 40 Air Force programs, we determined whether the ORDs for the programs contained IA requirements that could be measured, tested, and evaluated. Although 28 of the 40 ORDs contained IA requirements, only 16 of them were written in output-oriented and measurable terms. Personnel from the Office of the Air Force Director of Operational Capability Requirements stated that, as a result of the Chairman of the Joint Chiefs of Staff Instruction 6212.01C requiring all capability documents to include a net-ready KPP, they began requiring programs to incorporate net-ready KPP requirements with testable IA requirements into capability documents. Of the 40 programs surveyed, the personnel stated that 3 had net-ready KPPs in their capability documents, 1 had begun to incorporate a net-ready KPP into its capability document, and 3 had net-ready KPP migration strategies to convert the interoperability KPPs into net-ready KPPs as of September 2004. When

¹⁰Chairman of the Joint Chiefs of Staff Instruction 6212.01C stated that interoperability KPPs were superseded by net-ready KPPs.

capability documents specify testable IA requirements, testers can more readily determine whether an acquisition program's IA requirements are operationally effective and suitable to meet warfighter requirements.

Preparing and Maintaining System Security Authorization Agreements

SSAA Policy. DoD Instruction 5200.40, "DoD Information Technology Security Certification and Accreditation Process (DITSCAP)," December 30, 1997; and Air Force Instruction 33-202, "Network and Computer Security," June 17, 2004, provide policies and procedures for the DITSCAP, including SSAAs.

DoD Instruction 5200.40. DoD Instruction 5200.40 states that the DITSCAP applies to the acquisition, operation, and sustainment of any DoD system that collects, stores, transmits, or processes unclassified or classified information. Further, the Instruction states that a critical element of the DITSCAP is the agreement among the information technology system program manager,¹¹ the designated approving authority, the certification authority, and the user representative to resolve critical schedule, budget, security, functionality, and performance issues. This agreement is documented in the SSAA that is used to guide and document the results of the certification and accreditation process. The SSAA establishes a binding agreement on the level of security required before the system is developed or changes begin. The SSAA is used throughout the entire DITSCAP to guide actions, document decisions, specify information technology security requirements, document certification tailoring and level of effort, identify possible solutions, and maintain operational system security.

Air Force Instruction 33-202. Air Force Instruction 33-202 establishes Air Force computer security requirements for information protection in compliance with DoD Instruction 5200.40. The Instruction applies to all personnel who develop, acquire, deliver, use, operate, or manage Air Force information systems. Further, the Instruction requires:

- the Air Force Chief Information Officer to ensure that IA is an integral part of information systems and applications design, and
- the program manager to develop the SSAA.

SSAA Implementation. In practice, Air Force system program offices were not preparing SSAAs for acquisition programs with information technology requirements in that only 26 of the 40 system program offices surveyed had prepared SSAAs. To determine whether Air Force system program offices had an SSAA, we requested SSAAs from the program managers for the 40 system program offices surveyed. We also contacted the Air Force Operational Test and

¹¹The term program manager refers to the acquisition program manager during the system acquisition, the system manager during the operation of the system, or the maintenance organization's program manager when a system is undergoing a major change.

Evaluation Center, which conducts the Air Force's operational testing and evaluation to determine whether it required and received SSAAs for use in conducting operational testing.

SSAA Survey. In the survey questionnaire on the implementation of interoperability and IA requirements, we asked the program managers the following question concerning SSAAs: Of the following documentation normally provided to the milestone decision authority at the system development and demonstration decision point and the production and deployment decision point, which adequately describes IA requirements and strategies? In response, 20 of the 40 program managers believed that the SSAA best described the IA requirements and strategies for the system development and demonstration milestone decision and 8 of the 40 program managers believed that it best described the IA requirements and strategies for the production and deployment milestone decision (Appendix E contains the results of the survey).

SSAA Request. Based on our request, 26 of the 40 Air Force system program offices provided an SSAA. We did not determine whether the contents of the SSAAs were adequate. Only through the preparation of SSAAs before program milestone decision points can the milestone decision authority have assurance that the SSAA signatories¹² have all agreed on the method for implementing information technology security requirements and maintaining operational systems security.

Air Force Operational Test and Evaluation Center. Air Force Operational Test and Evaluation Center personnel stated that they required SSAAs as part of their operational test readiness review. When an SSAA was not available, the testers did not have information needed to assess compliance with the technical and nontechnical implementation of the security design and to determine whether the system program office had properly implemented security features affecting system confidentiality, integrity, availability, and accountability.

Coordination of DITSCAP Testing and Program Evaluation

DITSCAP Coordination Requirements. DoD Instruction 5000.2, "Operation of the Defense Acquisition System," May 12, 2003; DoD Guidebook, "Interim Defense Acquisition Guidebook," October 30, 2002;¹³ Director, Operational Test and Evaluation memorandum, "Policy for Operational Test and Evaluation of Information Assurance," November 17, 1999; and Air Force Instruction 33-202, "Network and Computer Security," June 17, 2004, discuss the coordination of DITSCAP testing.

¹²The SSAA signatories are the program manager, the designated approving authority, the certification authority, and the user.

¹³Formerly DoD Regulation 5000.2-R, "Mandatory Procedures for Major Defense Acquisition Programs (MDAPs) and Major Automated Information System (MAIS) Acquisition Programs," April 5, 2002. The former DoD Regulation 5000.2-R will serve as the guidebook while the Defense Acquisition Policy Working Group creates a streamlined guidebook.

DoD Instruction. DoD Instruction 5000.2 requires the program manager, together with the user and test and evaluation communities, to coordinate developmental test and evaluation, operational test and evaluation, live-fire test and evaluation, family-of-systems interoperability testing, IA testing, and modeling and simulation activities into an efficient process that is integrated with the system requirements definition and the system design and development.

DoD Guidebook. The Guidebook states that testers should conduct IA testing on information systems to verify that planned and implemented security measures satisfy ORD and SSAA requirements when the system is installed and operated in its intended environment. Further, the Guidebook states that the program manager, the operational test and evaluation authority, and the designated approving authority should coordinate and determine the level of risk associated with operating a system and the extent of security testing¹⁴ required.¹⁵

Director, Operational Test and Evaluation Policy. The Director, Operational Test and Evaluation memorandum¹⁶ requires the operational test agencies for programs subject to the DITSCAP to coordinate with the SSAA signatories throughout the acquisition cycle to minimize duplicative testing by the operational test agencies. Further, the memorandum requires the operational test agencies and the SSAA signatories to maximize opportunities to meet operational requirements through concurrent testing, particularly in DITSCAP vulnerability assessments, security tests and evaluations, and penetration testing.

Air Force Instruction 33-202. Air Force Instruction 33-202 establishes Air Force computer security requirements associated with information protection. The Instruction requires the program manager to ensure the appropriate coordination and review of all decisions concerning security trade-offs and changes in requirements with the SSAA signatories.

Coordination of IA Test Results. The Air Force operational testers for programs subject to the DITSCAP were coordinating with the SSAA signatories to minimize duplicative testing. To determine how effectively the Air Force operational testers were coordinating with the SSAA signatories to minimize duplicative IA testing, we contacted personnel from the Air Force Operational Test and Evaluation Center and the Air Force Information Warfare Center and reviewed applicable test reports.

Air Force Operational Test and Evaluation Center. Air Force Operational Test and Evaluation Center representatives stated that their organization did not have the internal resources to conduct IA technical evaluations. Instead, they incorporate and rely on IA test results from the

¹⁴Security testing is the examination and analysis of the safeguards, which are required to protect an information technology system, to determine the security capabilities of that system.

¹⁵The April 2002 and the June 2001 versions of DoD Regulation 5000.2-R had the same requirements as the DoD Guidebook.

¹⁶According to personnel in the Office of the Director, Operational Test and Evaluation, the Office of the Secretary of Defense incorporated the intent of the memorandum into the May 2003 version of the DoD 5000 series documents; however, as of October 2004, that office was updating the policy to address IA operational test and evaluation.

Air Force Information Warfare Center for inclusion in their test reports. In addition, the representatives stated that, as members of the integrated test team, they were aware of developmental as well as operational testing events. Specifically, they include in their test reports IA test results from developmental testing, as applicable. To further enhance the test and evaluation process, the representatives stated that their organization was preparing an IA checklist to ensure compliance with DITSCAP, DoD Instruction 8500.2, and National Institute of Standards and Technology Act¹⁷ requirements associated with information technology.

Air Force Information Warfare Center. The Air Force Information Warfare Center plans and conducts operations security, IA, and system vulnerability assessments as described in program documentation and integrated test plans, and participates in integrated test teams and test integrated product teams. Representatives from the Air Force Information Warfare Center stated that their ability to facilitate and coordinate with SSAA signatories concerning whether programs meet interoperability and IA requirements has improved as a result of the requirement to include specific IA requirements in capability documents.

Test Reports. To determine the extent of Air Force Information Warfare Center coordination with SSAA signatories, we reviewed three Air Force Information Warfare Center test reports on Air Force acquisition programs subject to the DITSCAP. Of the three test reports, two addressed system security and vulnerability findings and recommendations that the Air Force Information Warfare Center had coordinated with the respective system program offices. The test reports addressed the accompanying recommendations to the respective SSAA signatories and included actions to mitigate the system vulnerabilities that were identified during testing and analysis. By coordinating with the SSAA signatories for programs subject to the DITSCAP and with the Air Force Operational Test and Evaluation Center, the Air Force Information Warfare Center operational testers minimized duplicative testing for decisions concerning security trade-offs and changes in IA requirements.

Management Comments on the Finding and Audit Response

A summary of management comments on the finding and audit responses is in Appendix G.

¹⁷The National Institute of Standards and Technology Act requires the Institute to develop standards, guidelines, and associated methods and techniques for information systems. Those standards and guidelines are to include standards to be used by all agencies to categorize information and information systems collected or maintained by or on behalf of each agency. Further, the standards and guidelines are to include guidelines developed with DoD, including the National Security Agency, for identifying an information system as an NS system.

Recommendation and Management Comments

B. We recommend that the Air Force Chief Information Officer verify that Air Force system program offices prepared system security authorization agreements before milestone decision points for systems subject to the DoD Information Technology Security Certification and Accreditation Process, in accordance with DoD Instruction 5200.40, “DoD Information Technology Security Certification and Accreditation Process (DITSCAP),” December 30, 1997, and Air Force Instruction 33-202, “Network and Computer Security,” June 17, 2004.

Air Force Chief Information Officer Comments. The Air Force Chief Information Officer concurred, stating that SSAA information is collected in the Air Force Enterprise Information Technology Data Repository.¹⁸ Further, the Air Force Chief Information Officer stated that his staff now verify the existence of an SSAA as part of the information assurance strategy review process. For the complete text of the Air Force Chief Information Officer’s comments, see the Management Comments section of the report.

Director, Joint Staff Comments. Although not required to comment, the Director agreed with the recommendation, stating that the Joint Staff will support the recommendation through its role as a principal member of the Interoperability Test Panel. For the complete text of the Director’s comments, see the Management Comments section of the report.

¹⁸The Air Force Enterprise Information Technology Data Repository, formerly called the Systems Compliance Database, is a repository of information on information technology systems and initiatives to support the Clinger-Cohen Act information technology registration, Federal Information Security Management Act compliance, and information technology portfolio management, and will support C4I support planning beginning in November 2005.

C. Populating and Maintaining the Global Information Grid's Asset Inventory

The Air Force had not populated and maintained its portion of the GIG¹⁹ asset inventory for acquisition programs containing information technology requirements. The GIG asset inventory was not populated because DoD had not issued guidance specifying:

- the composition of the GIG asset inventory for acquisition programs containing information technology requirements, and
- the process that the Air Force and the other DoD Components need to follow to populate and maintain their respective GIG asset inventories.

Without a defined policy describing how the DoD Components will populate and maintain the GIG asset inventory for acquisition programs containing information technology requirements, DoD cannot ensure that its acquisition programs have the most effective, efficient, and secure information-handling capabilities available, consistent with national military strategy and warfighter operational requirements.

GIG Statutory Requirements and Policy

The Federal Information Security Management Act of 2002; section 2223, title 10, United States Code, "Information Technology: Additional Responsibilities of Chief Information Officers;" DoD Directive 4630.5; and DoD Directive 8100.1, "Global Information Grid (GIG) Overarching Policy," November 21, 2003, provide statutory requirements and policy for the GIG asset inventory.

Federal Information Security Management Act of 2002. Section 305, "Technical and Conforming Amendments," of the Act requires DoD to develop and maintain an inventory of major information systems, including major NS systems, that it operates or controls. Further, section 301, "Information Security," states that NS systems include information systems used or operated by an agency or contracted by an agency, the function, operation, or use of which involves intelligence activities, cryptologic agencies related to NS, command and control of military forces, and equipment that is an integral part of a weapon or weapons system that is critical to direct fulfillment of military or intelligence missions.

¹⁹The GIG is not one system; it is 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, NS systems, and associated services necessary to achieve information superiority.

Section 2223. Section 2223 requires the DoD Chief Information Officer to maintain a consolidated inventory of DoD mission-critical and mission-essential information systems, identify interfaces between those systems and other information systems, and develop and maintain contingency plans for responding to a disruption in the operation of any of those information systems.

DoD Directive 4630.5. The Directive updates DoD policy and responsibilities for interoperability and supportability of information technology, including NS systems, and implements DoD Chief Information Officer’s responsibilities. The Directive requires the DoD Chief Information Officer to ensure the development, implementation, and maintenance of the GIG architecture in accordance with DoD Directive 8100.1.

DoD Directive 8100.1. The Directive establishes policy and assigns responsibilities for GIG configuration management and architecture to the Office of the Secretary of Defense as well as the Military Departments. The Directive requires:

- the establishment and maintenance of an enterprise-wide inventory of GIG assets;
- the Under Secretary of Defense for Acquisition, Technology, and Logistics to ensure that acquisition programs fully consider documented GIG requirements;
- the Under Secretary of Defense (Comptroller) to collaborate with the DoD Chief Information Officer, where necessary, to identify and coordinate improvements to identify and describe information technology resources;
- the DoD Components, including the Joint Chiefs of Staff, to populate and maintain their portions of the GIG asset inventory; and
- the Chairman of the Joint Chiefs of Staff to develop joint doctrine and ensure the compatibility of the Chairman of the Joint Chiefs of Staff instructions with GIG policy and guidance.

Before DoD issued DoD Directive 8100.1, the above requirements were included in Deputy Secretary of Defense Memorandum, “DoD Chief Information Officer (CIO) Guidance and Policy Memorandum No. 8-8001 – March 31, 2000 – Global Information Grid,” March 31, 2000.

GIG Asset Inventory

Compiling a GIG Asset Inventory. Personnel in the Office of the Air Force Chief Information Officer stated that the Air Force had not compiled a GIG asset inventory of major information systems, including acquisition programs containing information technology requirements.²⁰ Although no Air Force GIG

²⁰Although not a GIG asset inventory, the Air Force Chief Information Officer noted that the Air Force did conduct an inventory of assets using the Enterprise Information Technology Data Repository, which feeds into the DoD Information Technology Registry.

asset inventory existed, we asked the 40 Air Force program offices surveyed whether they considered their programs to be part of the GIG asset inventory. The program offices' responses were as follows:

- 14 Air Force program offices responded that their programs were part of the GIG asset inventory,
- 16 Air Force program offices responded that their programs were not part of the GIG asset inventory, and
- 10 Air Force program offices were not sure whether their programs were part of GIG asset inventory.

Appendix E contains the complete results of the program offices' survey.

Issuing GIG Asset Inventory Guidance. According to representatives from the Office of the Air Force Chief Information Officer, the Air Force did not populate and maintain its portion of the GIG asset inventory because DoD had not issued guidance specifying the composition of the GIG asset inventory and the process that the Air Force and the other DoD Components need to follow to populate and maintain their respective GIG asset inventories. The representatives noted that the Deputy DoD Chief Information Officer had issued a memorandum, "Component Support of DoD Information Technology Portfolio Review Process," July 13, 2004, which discusses populating the DoD Information Technology Portfolio Data Repository with DoD information systems,²¹ and that DoD Directive 8100.1 discusses what the GIG includes. However, the representatives stated that the DoD Information Technology Portfolio Data Repository was not the GIG asset inventory and that DoD Directive 8100.1 did not discuss how to populate and maintain the GIG asset inventory.

Complying With the GIG Asset Inventory Requirement. According to the Principal Director to the Deputy DoD Chief Information Officer, DoD did not have a GIG asset inventory; however, the nearest DoD equivalent was the DoD Information Technology Registry,²² which DoD uses to compile data to meet the Federal Information Security Management Act reporting requirements.²³ Further,

²¹A DoD information system is a set of information resources organized for the collection, storage, processing, maintenance, use, sharing, dissemination, disposition, display, or transmission of information. The DoD information system includes automated information system applications, enclaves, outsourced information-technology-based processes, and platform information technology connections.

²²The DoD Information Technology Registry is the repository for information about the DoD mission-critical and mission-essential information technology systems. The Military Department Chief Information Officers were told to add all non-mission-critical and non-mission-essential information technology systems to the Registry by September 30, 2006.

²³Inspector General of the Department of Defense response on October 6, 2004, to the Office of Management Budget regarding Federal agencies information security associated with the Federal Information Security Management Act of 2002 also addressed the GIG asset inventory issue. Further, Inspector General of the Department of Defense Report No. D-2005-029, "Management of Information Technology Resources Within DoD," January 27, 2005, addressed the requirement for the Assistant Secretary of Defense for Networks and Information Integration to report the asset inventory relating to the status of DoD information systems to the Office of Management and Budget and for congressional purposes associated with the Federal Information Security Management Act of 2002.

the Principal Director stated that, even though the DoD Information Technology Registry was not adequate to use as the GIG asset inventory, DoD may develop it into the GIG asset inventory. To this end, DoD is considering using the Department of the Navy Application and Database Management System on an interim basis for the GIG asset inventory. The Principal Director also stated that the Department of the Navy Application and Database Management System could:

- absorb the DoD Information Technology Registry and
- be expanded to include necessary GIG data elements if the System was used to build the GIG asset inventory.

Further, the Principal Director stated that the Joint Staff J-6 contacted the Office of the DoD Chief Information Officer about using the DoD Information Technology Registry to replace the Joint C4I Program Assessment Tool to track systems that have completed the Joint Staff J-6 interoperability certification process. In conclusion, the Principal Director stated that changes in the application of the DoD Information Technology Registry may require DoD Directive 8100.1 to be updated.

Policy for Populating and Maintaining the GIG Asset Inventory

Without a defined policy describing how the DoD Components will populate and maintain the GIG asset inventory for acquisition programs containing information technology requirements, DoD cannot ensure that its acquisition programs have the most effective, efficient, and secure information-handling capabilities available, consistent with national military strategy and warfighter operational requirements.

Conclusion

To establish and maintain an enterprise-wide inventory of GIG assets, including acquisition programs containing information technology requirements, DoD guidance should be issued to define policy describing how the DoD Components will populate and maintain the GIG asset inventory. Inspector General of the Department of Defense Report No. D-2005-033, "Implementation of the Interoperability and Information Assurance Policies for Acquisition of Navy Systems," February 2, 2005, addressed the need for DoD guidance in populating and maintaining the GIG asset inventory and will include a recommendation addressing the issue. Specifically, the resulting report recommended that the Assistant Secretary of Defense for Networks and Information Integration/DoD Chief Information Officer prepare and staff a DoD directive that specifies the:

- types of systems and system information capability requirements to be included in the GIG asset inventory and
- responsibilities of DoD Components in populating and maintaining the GIG asset inventory.

Management Comments on the Finding

A summary of management comments on the finding and audit responses is in Appendix G.

Appendix A. Scope and Methodology

We reviewed documentation dated from March 1994 to July 2004. To accomplish the audit objective, we reviewed:

- the Air Force's efforts to implement interoperability and information assurance requirements during the acquisition process for acquisition programs;
- system requirements and capabilities documentation for interoperability and information assurance requirements;
- the controls over the Joint Staff J-6 interoperability certification process and the Joint Command, Control, Communications, Computers, and Intelligence Program Assessment Tool; and
- applicable criteria.

We also contacted the staffs of the Assistant Secretary of Defense for Networks and Information Integration/DoD Chief Information Officer; the Air Force Air Combat Command; the Air Force Air Mobility Command; the Air Force Space Command; the Director for Command, Control, Communications, and Computers Systems Directorate (J-6), Office of the Chairman of the Joint Chiefs of Staff; the Defense Information Systems Agency; the Deputy Assistant Secretary of the Air Force (Management Policy and Program Integration), Office of the Assistant Secretary of the Air Force (Acquisition); the Air Force Chief Information Officer; the Directorate of Command, Control, Communications, and Computers, Intelligence, Surveillance, and Reconnaissance Infostructure, Office of the Air Force Deputy Chief of Staff for Warfighting Integration; the Directorate of Operational Capabilities Requirements, Office of the Air Force Deputy Chief of Staff for Air and Space Operations; the Air Force Operational Test and Evaluation Center; the Joint Interoperability Test Command; the Air Force Test and Evaluation Directorate; the Air Force Communications Agency; and the Air Force Information Warfare Center.

In addition, we judgmentally selected for review 40 Air Force acquisition programs²⁴ to:

- obtain the program managers' perspectives on interoperability and IA requirements;
- review ORDs, C4I support plans, TEMPs, and SSAAs; and

²⁴The Predator Unmanned Aerial Vehicle program comprises two systems: the Predator Medium Altitude Endurance Unmanned Aerial Vehicle (RQ-1A) and the Predator Hunter-Killer Unmanned Aerial Vehicle (MQ-9). However, the audit reviewed only the RQ-1A because the supporting documentation for the MQ-9 was not available at the time of the audit.

-
- determine the stage of each program in the Joint Command, Control, Communications, Computers, and Intelligence Program Assessment Tool repository for Joint Staff J-6 interoperability certification.

We performed this audit from July 2002 through November 2004 in accordance with generally accepted government auditing standards. We did not review the management control program because the audit focused on interoperability and IA 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 Technical Support. The Technical Assessment Division, Office of the Assistant Inspector General for Audit Followup and Technical Support assisted the audit by reviewing the ORDs, C4I support plans, TEMPs, and SSAAs for the programs reviewed. In addition, the Technical Assessment Division reviewed selected test reports that the Air Force Operational Test and Evaluation Command prepared during FYs 2001, 2002, and 2003 to determine whether testers performed IA testing in accordance with DoD and Air Force policy.

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

Appendix B. Prior Coverage

During the last 5 years, the Government Accountability Office, the Inspector General of the Department of Defense, and the Defense Science Board have issued nine reports addressing interoperability and IA requirements for DoD systems. Unrestricted Government Accountability 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.

Government Accountability Office (GAO)

GAO Report GAO-04-858, “Defense Acquisitions - The Global Information Grid and Challenges Facing Its Implementation,” July 2004

GAO Report GAO-03-329, “Defense Acquisitions - Steps Needed to Ensure Interoperability of Systems that Process Intelligence Data,” March 2003

Inspector General of the Department of Defense (IG DoD)

IG DoD Report No. D-2005-033, “Implementation of the Interoperability and Information Assurance Policies for Acquisition of Navy Systems,” February 2, 2005

IG DoD Report No. D-2004-008, “Implementation of Interoperability and Information Assurance Policies for Acquisition of Army Systems,” October 15, 2003

IG DoD Report No. D-2003-024, “Information Assurance Challenges – An Evaluation of Audit Results Reported from August 23, 2001, through July 31, 2002,” November 21, 2002

IG DoD Report No. D-2003-011, “Implementation of Interoperability and Information Assurance Policies for Acquisition of DoD Weapon Systems,” October 17, 2002

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

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

Appendix C. Glossary

Accreditation. Accreditation is the formal declaration by the designated approving authority that an information technology system is approved to operate in a particular security mode using a prescribed set of safeguards at an acceptable level of risk.

Acquisition Category. An acquisition category is an attribute of an acquisition program that determines the 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 Air Force, Navy, and Marine Corps.

Air Force Enterprise Information Technology Data Repository. The Air Force Enterprise Information Technology Data Repository, formerly called the Systems Compliance Database, is a repository of information on information technology systems and initiatives to support the Clinger-Cohen Act information technology registration, Federal Information Security Management Act compliance, and information technology portfolio management, and will support C4I support planning beginning in November 2005.

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

Capstone Requirements Document. A capstone requirements document contains capabilities-based requirements that facilitate the development of individual capability development documents by providing a common framework and operational concept to guide their development.

Certification Authority. Certification authority is the official responsible for performing the comprehensive evaluation of the technical and nontechnical security features of an information technology system and other safeguards to determine the extent to which a particular design and implementation meet a set of specified security requirements.

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.

Designated Approving Authority. The designated approving authority is an official with the authority to formally assume responsibility for operating a system at an acceptable level of risk. The term designated approving authority is synonymous with designated accrediting authority and delegated accrediting authority.

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.

DoD Information Technology Registry. The DoD Information Technology Registry is the repository for accurate and current information about the DoD mission-critical and mission-essential information technology systems. The Military Department Chief Information Officers plan to add all non-mission-critical and non-mission-essential information technology systems to the Registry by September 30, 2006.

DoD Information System. A DoD information system is a set of information resources organized for the collection, storage, processing, maintenance, use, sharing, dissemination, disposition, display, or transmission of information. The DoD information system includes automated information system applications, enclaves, outsourced information technology-based processes, and platform information technology connections.

DoD Information Technology Security Certification and Accreditation Process (DITSCAP). The DITSCAP is the standard DoD process for identifying information security requirements, providing security solutions, and managing information system security activities.

Global Information Grid. The Global Information Grid provides the foundation for net-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 and will not be connected to the enterprise network.

Global Information Grid Key Interface Profile. A Global Information Grid key interface profile provides a net-centric approach for managing interoperability across the GIG based on the configuration control of key interfaces.

Information Assurance. Information assurance is measures that protect and defend the information and information systems by ensuring their availability, integrity, confidentiality, authentication, 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 is the hardware, firmware, and software used as part of the information system to perform DoD information functions. Information technology includes computers, telecommunications, automated information systems, automatic data processing equipment, and any assembly of computer hardware, software, and firmware configured to collect, create, communicate, compute, disseminate, process, store, and control data or information.

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. Certification as it applies to interoperability is a formal statement of adequacy provided by a responsible agency (usually Joint Staff) attesting that a system has met its interoperability and supportability requirements.

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 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 system 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 a critical subset of the performance parameters found in the ORD. Each key performance parameter has a threshold and an objective value. Key performance parameters represent those capabilities or characteristics so significant that failure to meet the threshold value of performance can be cause for the concept or system selected to be reevaluated or the program to be reassessed or terminated.

National Security System. A national security system is any telecommunication or information system operated by the U.S. 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 warfare²⁵ 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.

Net-Ready Key Performance Parameter (Net-Ready KPP). A net-ready KPP assesses information needs, information timeliness, information assurance, and net-enabled attributes required for information exchange and use. A net-ready KPP consists of measurable and testable characteristics, performance metrics, or both, required for the timely, accurate, and complete exchange and use of information to satisfy information needs for a given capability. The net-ready KPP comprises the following elements: compliance with the net-centric operations and warfare reference model, compliance with applicable GIG key interface profiles, verification of compliance with DoD information assurance requirements, and supporting integrated architecture products required to assess information exchange and use for a given capability. A net-ready KPP is documented in the following requirements documents: a capability development document, a capability production document, and a capstone requirements document.

Non-Acquisition Category. Non-acquisition category systems are all defense information technology and national security system projects, pre-acquisition demonstration, joint experimentations, joint tests and evaluations, and non-DoD 5000 series information technology and NS system acquisitions and procurements.

Objective. The objective is the performance value that is desired by the user and which the program manager is attempting to obtain. The objective represents an operationally meaningful, time critical, and cost-effective increment above the performance threshold for each program parameter.

Operational Architecture View. The operational architecture view is a description of the tasks and activities, operational elements, and information flows required to accomplish or support a military operation.

²⁵An 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.

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 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.

Penetration Testing. Penetration testing assesses a system's ability to withstand intentional attempts to circumvent system security features by exploiting technical security vulnerabilities. Penetration testing may include insider and outsider penetration attempts based on common vulnerabilities for the technology being used.

Program. A program is a weapon system 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 Manager. Program manager refers to the acquisition program manager during the system acquisition, the system manager during the operation of the system, or the maintenance organization's program manager when a system is undergoing a major change.

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 Evaluation Plan. The system evaluation plan documents the integrated test and evaluation strategy, which the testers and evaluators use throughout the system acquisition life cycle. The system evaluation plan:

- addresses system critical operational issues and criteria, critical technical parameters, and additional evaluation focus areas;
- identifies data needs and sources, and the approach to be used to evaluate the system;
- specifies the analytical plan; and
- identifies program constraints.

The system evaluation plan details the evaluator's planned actions for the evaluation of the system and is prepared and updated by the system evaluator.

System Security Authorization Agreement. The system security authorization agreement is a formal agreement among the designated approving authority, the certification authority, the information technology system user representative, and the program manager. The agreement is used throughout the entire DITSCAP to guide actions, document decisions, specify information technology security requirements, document certification tailoring and level-of-effort, identify potential solutions, and maintain operational systems security.

System Security Authorization Agreement Signatories. The system security authorization agreement signatories include the information technology system program manager, the designated approving authority, the certification authority, and the user representative.

Technical Architecture View. A technical architecture view is a minimal set of rules governing the arrangement, interaction, and interdependence of system parts or elements, whose purpose is to ensure that a conformant system satisfies a specified set of requirements.

Test and Evaluation Master Plan (TEMP). The 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.

Threshold. Threshold is the minimum acceptable value that, in the user's judgment, is necessary to satisfy the need. If threshold values are not achieved, program performance is seriously degraded, the program may be too costly, or the program may no longer be timely.

User Representative. The user representative is the liaison for the user or the user community, particularly during the initial development of a system. The user representative is the individual or organization that represents the user community in the specification, acquisition and maintenance of information technology system. The user representative defines the system mission and functionality and is responsible for ensuring that the user's interests are maintained throughout system development, modification, integration, acquisition, and deployment.

Vulnerability. Vulnerability is the characteristics of a system that cause it to suffer a definite loss or reduction of capability to perform its designated mission as a result of having been subjected to a certain level of effects in a man-made hostile environment.

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 in the figure below.



Foundation for Achieving Full Spectrum Dominance²⁶

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 requirements 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

²⁶Figure obtained from the GIG Capstone Requirements Document, August 30, 2001.

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 implement them 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. Results of the Air Force Interoperability and Information Assurance Survey

Survey Question	Survey Answers	Number of Program Managers Responded
1. What acquisition category is your program?	a. Acquisition Category IAM or Acquisition Category IAC	6
	b. Acquisition Category ID or Acquisition Category IC	19
	c. Acquisition Category II	1
	d. Acquisition Category III	12
	e. Non-DoD Acquisition Process	0
	f. Other	2
2. What type of system is your program? (Some program offices had multiple responses)	a. NS system	7
	b. Information technology system (that is not an NS system)	4
	c. Weapon system	19
	d. Automated information system	3
	e. None of the above	10
3. What is the last milestone your program completed?	a. Pre-acquisition (for example, science and technology, concept development, demonstration)	1
	b. Milestone A (or 0)	3
	c. Milestone B (or II or system development and demonstration)	14
	d. Milestone C (or III or low-rate initial production)	6
	e. Beyond Milestone C (or full-rate production)	7
	f. Other	9
4. Which joint mission area does your program support? Select the appropriate answer based on the Chairman of the Joint Chiefs of Staff Memorandum (CM-1014-00), "Joint Mission Areas to Organize the Joint Operational Architectures."	a. Dominant maneuver	14
	b. Deployment redeployment	19
	c. Precision engagement	20
	d. Strategic deterrence	8
	e. Overseas presence and force projection	18
	f. Special operations	15
	g. Joint command and control	18
	h. Information superiority	18
	i. Focused logistics	7
	j. Full dimensional protection	6
	k. Multinational operations/interagency coordination	12
l. Other	6	

<u>Survey Question</u>	<u>Survey Answers</u>	<u>Number of Program Managers Responded</u>
5. For information technology or NS systems, the ORD must include interoperability requirements, thus requiring an interoperability KPP. These systems must also have related elements of IA. In this respect, do you think IA is a subcomponent of interoperability?	a. Yes	30
	b. No	8
	c. Unsure	2
6. Should IA requirements be tested in addition to interoperability requirements?	a. Yes	35
	b. No	4
	c. Unsure	1
7. Has the Director for Command, Control, Communications, and Computers Systems Directorate (J-6), Office of the Chairman of the Joint Chiefs of Staff (Joint Staff J-6) certified your program's ORD for interoperability requirements?	a. Yes	14
	b. No, the ORD has not been through the process yet.	6
	c. No, the ORD went through the process but was not certified	4
	d. In process	4
	e. Unsure	12
8. Is your program part of the GIG asset inventory?	a. Yes	14
	b. No	16
	c. Unsure	10
9. How is your program compatible with the GIG? Select all that apply.	a. Uses current Defense Information Switched Network services	19
	b. Uses approved allocated frequency plans	26
	c. Uses approved cryptology	30
	d. Meets appropriate standards (for example, Defense Information Infrastructure Common Operating Environment compliance)	27
	e. None of the above	0
	f. Other	11
	g. Unsure	1

Survey Question	Survey Answers	Number of Program Managers Responded
10. Which Air Force oversight entity(ies) or command(s) assures that your Acquisition Category IAM, IAC, ID, or IC operates with other Defense agency and Military Department acquisition programs as envisioned by the warfighter.	a. Program executive officer/milestone decision authority	22
	b. Headquarters, Air Force Assistant Chief of Staff, Systems for Command, Control, and Communications	2
	c. Headquarters, Air Force Deputy Chief of Staff, Air and Space Operations	5
	d. Assistant Secretary of the Air Force (Acquisition)	13
	e. Headquarters, Air Force Director of Test and Evaluation	9
	f. Assistant Secretary of Defense for Command, Control, Communications, and Intelligence	8
	g. Major Command and Field Operating Agencies	8
	h. Joint Staff J-6	8
	i. Director for Operational Plans and Interoperability Directorate (J-7), Office of the Chairman of the Joint Chiefs of Staff	0
	j. U.S. Joint Forces Command (J-6)	3
	k. Director, Operational Test and Evaluation	13
l. Other	18	
11. Which Air Force oversight entity(ies) or command(s) assures that your Acquisition Category II or below program operates with other Defense agency and Military Department acquisition programs as envisioned by the warfighter.	a. Program executive officer/milestone decision authority	6
	b. Headquarters, Air Force Assistant Chief of Staff, Systems for Command, Control, and Communications	0
	c. Headquarters, Air Force Deputy Chief of Staff, Air and Space Operations	4
	d. Assistant Secretary of the Air Force (Acquisition)	6
	e. Headquarters, Air Force Director of Test and Evaluation	1
	f. Major Command and Field Operating Agencies	5
	g. Other	18

Survey Question	Survey Answers	Number of Program Managers Responded
12. Of the following documentation normally provided to the milestone decision authority at Milestone B, which documents fully describe interoperability requirements and strategies? Select all that apply.	a. ORD	34
	b. Capstone requirements document	10
	c. C4I support plan	21
	d. TEMP	15
	e. Developmental test results	5
	f. Operational test results	5
	g. System evaluation plan	2
	h. Event design plan	0
	i. Operational architecture view	11
	j. Systems architecture view	11
	k. Technical architecture view	7
	l. Security plans	9
	m. Other	12
	n. None	1
13. Of the following documentation normally provided to the milestone decision authority at Milestone C, which documents fully describe interoperability requirements and strategies? Select all that apply.	a. ORD	29
	b. Capstone requirements document	9
	c. C4I support plan	19
	d. TEMP	20
	e. Developmental test results	10
	f. Operational test results	10
	g. System evaluation plan	4
	h. Event design plan	0
	i. Operational architecture view	14
	j. Systems architecture view	14
	k. Technical architecture view	11
	l. Security plans	11
	m. Other	16
	n. None	1
14. Of the following documentation normally provided to the milestone decision authority at Milestone B, which documents fully describe IA requirements and strategies? Select all that apply.	a. ORD	23
	b. Capstone requirements document	5
	c. C4I support plan	16
	d. TEMP	15
	e. SSAA	20
	f. Developmental test results	6
	g. Operational test results	5
	h. System evaluation plan	2
	i. Event design plan	0
	j. Operational architecture view	4
	k. Systems architecture view	5
	l. Technical architecture view	3
	m. Security plans	16
	n. Other	9
	o. None	4

Survey Question	Survey Answers	Number of Program Managers Responded
15. Of the following documentation normally provided to the milestone decision authority at Milestone C, which documents fully describe IA requirements and strategies? Select all that apply.	a. ORD	25
	b. Capstone requirements document	6
	c. C4I support plan	17
	d. TEMP	13
	e. SSAA	8
	f. Developmental test results	7
	g. Operational test results	6
	h. System evaluation plan	3
	i. Event design plan	0
	j. Operational architecture view	9
	k. Systems architecture view	10
	l. Technical architecture view	7
	m. Security plans	18
	n. Other	10
o. None	4	
16. The inclusion of IA requirements in an ORD would benefit from the addition of high-level information exchange requirements. (See Chairman of the Joint Chiefs of Staff Instruction 3170.01B, "Requirements Generation System.")	a. I agree	22
	b. I disagree	8
	c. No opinion	7
	d. I am unsure	3
17. The ORD must define information exchange requirements for information technology and NS system acquisition programs.	a. I agree	28
	b. I disagree	3
	c. No opinion	4
	d. I am unsure	5
18. IA should be a key performance parameter in my acquisition program that must exchange data external to the information technology system, NS system, or weapon system's host platform.	a. I agree	18
	b. I disagree	13
	c. No opinion	6
	d. I am unsure	3
19. My acquisition program will include the following IA security techniques or technologies before production. Select all that apply.	a. Public key infrastructure	10
	b. Firewalls	23
	c. Smart cards	8
	d. Passwords	30
	e. Encryption/decryption	29
	f. Physical security	33
	g. Frequency hopping	9
	h. Restoration of capability	20
	i. None of the above	1
	j. Other	13

Survey Question	Survey Answers	Number of Program Managers Responded
20. My acquisition program will include the following IA security techniques or technologies after production. Select all that apply.	a. Public key infrastructure	12
	b. Firewalls	24
	c. Smart cards	13
	d. Passwords	30
	e. Encryption/decryption	34
	f. Physical security	35
	g. Frequency hopping	12
	h. Restoration of capability	23
	i. None of the above	0
	j. Other	9
21. List all IA products that are commercial-off-the-shelf products related and/or integrated into your acquisition program.	The system program offices identified different commercial-off-the-shelf products. A list of the products identified is available upon request.	
22. Are all the products listed in question 21 certified for IA by the National Security Agency?	a. Yes	9
	b. No	14
	c. Unsure	13
23. Do you plan to have all products listed in question 21 certified for IA by the National Security Agency? Answer if question 22 was No. (Some program offices answered even if they had answered Yes to Question 22)	a. Yes	13
	b. No	19
24. Do fluctuations in funding and prioritization impact system development as it relates to interoperability requirements?	a. Yes	25
	b. No	13
25. Is your program in compliance with the Clinger-Cohen Act?	a. Yes	32
	b. No	7
26. Do you believe the GIG currently addresses all IA requirements?	a. Yes	21
	b. No	13
27. Does the system program office have an interoperability specialist assigned to the program?	a. Yes	23
	b. No	17
28. Does the system program office have an IA specialist assigned to the program?	a. Yes	27
	b. No	13

<u>Survey Question</u>	<u>Survey Answers</u>	<u>Number of Program Managers Responded</u>
29. Has a risk assessment been conducted on meeting the program's interoperability requirement?	a. Yes b. No	25 15
30. Has a risk assessment been conducted on meeting the program's IA requirements?	a. Yes b. No	23 17
31. Who is completing the DITSCAP testing (for all appropriate phases) for your program? Provide name of point of contact, organization, title, telephone number, and email.	The system program offices identified different points of contact that are completing the DITSCAP testing. A list of the points of contact identified is available upon request.	
32. For the program's System Threat Analysis Report (STAR), who determined the threat, specifically the IA threat, and who validated that threat?	The system program offices identified different entities that determined the IA threat and validated that threat. A list of the entities identified is available upon request.	

Appendix F. Air Force Programs Surveyed

1. Advanced Extremely High Frequency
2. Advanced Remote Ground Unattended Sensor
3. Air Force Mission Support System
4. B-1B Conventional Mission Upgrade Program
5. C-5 Avionics Modernization Program
6. C-17 A/C-17A Upgrades
7. C-130 Avionics Modernization Program
8. C-130J All Variants
9. Combat Survivor Evader Locator
10. Defense Meteorological Satellite Program
11. Deliberate and Crisis Action Planning and Execution Segments
12. Air Force-Distributed Common Ground System
13. E-3A Airborne Warning and Control System
14. F-22 Raptor (Engineering and Manufacturing Development and Squadrons)
15. Global Broadcast Service
16. Global Combat Support System - Air Force
17. Aerospace Operations Center
18. Theater Battle Management Core System
19. Global Hawk Unmanned Aerial Vehicle
20. Global Positioning System
21. Global Transportation Network-21
22. Information Warfare Planning Capability
23. Integrated Maintenance Data System
24. Joint Air-to-Surface Standoff Missile
25. Joint Direct Attack Munition (500, 1,000, and 2,000 pounds)
26. Joint Precision Approach and Landing System
27. Joint Primary Aircraft Training System
28. Joint Strike Fighter
29. Joint Surveillance Target Attack Radar System
30. MILSTAR Satellite Communication System
31. Mobile Approach Control System
32. Multi-Platform - Common Data Link
33. National Airspace System
34. National Polar-Orbiting Operational Environment Satellite System
35. P-5 Combat Training System
36. Predator Medium Altitude Endurance Unmanned Aerial Vehicle
37. Space-Based Infrared System-High
38. Theater Deployable Communications
39. Time Critical Targeting Functionality
40. Wideband Gapfiller Satellite

Appendix G. Audit Response to Air Force Comments on the Report

Our detailed response to the comments from the Air Force Chief Information Officer on statements in the draft report follow. The complete text of those comments is in the Management Comments section of this report. The Air Force Chief Information Officer commented on the inclusion of the Clinger-Cohen Act; the applicability of information support plans; Air Force Instruction 33-202 “Network and Computer Security” June 17, 2004, or Air Force Pamphlet 63-1701, “Program Protection Planning” March 27, 2003; Air Force Instruction 63-101, “Operation of the Capabilities Based Acquisition System,” April 2004; Air Force Asset Inventory; and Air Education and Training Command.

Clinger-Cohen Act. The Air Force Chief Information Officer stated that the paragraphs on “Interoperability, Requirements and Certification Policy” and “DoD Policy” in finding A discuss DoD policy related to interoperability requirements and certification, but do not address the interoperability requirements that are discussed in Enclosure 4 of DoD Instruction 5000.2, “Operation of the Defense Acquisition System.” In Enclosure 4, program managers are provided statutory and regulatory requirements for interoperability as part of Clinger-Cohen Act compliance certification for mission-critical and mission-essential systems. It states that, at a minimum, the DoD Component Chief Information Officer’s confirmation or certification will include a written description of the three materiel questions of section 3.6.4 and requirements related to the Clinger-Cohen Act of 1996. The three materiel questions are:

- Do the acquisition support core/priority mission functions need to be performed by the Federal Government?
- Does the acquisition need to be undertaken by the DoD Component because no alternative private sector or governmental source can better support the function?
- Do the acquisition support work processes that have been simplified or otherwise redesigned reduce costs, improve effectiveness, and make maximum use of commercial off-the-shelf technology?

The Air Force Chief Information Officer stated that a recommendation for updating DoD Instruction 5000.2 should be added to the report so that it requires all information-technology-related systems, including automated information systems connecting to the Global Information Grid, to meet the interoperability requirements in DoD Directive 4630.5, “Interoperability and Supportability of Information Technology (IT) and National Security Systems (NSS),” May 5, 2004. Further, the Air Force Chief Information Officer stated that, if a system does not fall into the mission-critical or mission-essential system definition or if the system is an automated information system, program managers likely disregard the need for Clinger-Cohen Act compliance.

Audit Response. DoD Directive 5000.1, “The Defense Acquisition System,” May 12, 2003, does state that DoD policy for the information technology aspects of interoperability and supportability appears in DoD Directive 4630.5.

Information Support Plan. The Air Force Chief Information Officer commented on the “C4I Support Plans, C4I Support Plan Policy” and “DoD Instruction” paragraphs in finding A. He stated that it appears that the DoD 5000 series, and its direction on C4I support plans or information support plans, was not part of the audit. The Air Force Chief Information Officer suggested a recommendation be included in the report that DoD Instruction 5000.2 be updated to require a C4I support plan or information support plan for all information technology systems, including automated information systems connected to the Global Information Grid, rather than for only mission-critical and mission-essential systems.

Audit Response. The Defense Acquisition Guidebook, December 2004, identifies Chairman of the Joint Chiefs of Staff Instruction 6212.01C “Interoperability and Supportability of Information Technology and National Security Systems,” November 20, 2003, as mandatory requirements for all acquisition programs, including information technology and NS systems. Chairman of the Joint Chiefs of Staff Instruction 6212.01C applies to all information technology and NS systems or services acquired, procured, or operated by any DoD Component. The information support plan requirement in Chairman of the Joint Chiefs of Staff Instruction 6212.01C applies to all acquisition category, non-acquisition category,²⁷ and fielded programs regardless of approval authority, designation, increment, or block. The Instruction specifically states that the program authority for those programs will prepare an information support plan to document the information technology and NS systems needs, objectives, and interface requirements.

Air Force Instruction and Pamphlet. The Air Force Chief Information Officer stated that the “Air Force Memorandum” paragraph in finding A discusses only an Assistant Secretary of the Air Force (Acquisition) memorandum on C4I support plans. He stated that the paragraph did not address direction contained in Air Force Instruction 33-202 or Air Force Pamphlet 63-1701. The Air Force Chief Information Officer recommended that those documents be reviewed to determine whether the audit results should be updated to include salient information from those documents in finding A.

Audit Response. We reviewed Air Force Instruction 33-202 and determined that it does not contain additional requirements for the C4I support plan or the information support plan beyond the requirements of DoD Instruction 4630.8, which we cited in finding A. Requirements of the Instruction apply to finding B and are cited on pages 14 and 16 of the report. Air Force Pamphlet 63-1701 addresses C4I certification and accreditation but does not address preparing a C4I support plan or information support plan.

²⁷ Chairman of the Joint Chiefs of Staff Instruction 6212.01C defines a non-acquisition category as all defense information technology and national security system projects, pre-acquisition demonstration, joint experimentations, joint tests and evaluations, and non-DoD 5000 series information technology and NS system acquisitions and procurements.

Air Force Instruction 63-101. The Air Force Chief Information Officer stated that although Air Force Pamphlet 63-1701 makes information technology system certification and accreditation a part of the program managers' program protection planning responsibilities, Air Force Instruction 63-101 does not include those information technology security and certification requirements. The Air Force Chief Information Officer suggested an additional recommendation be included in finding A to update Air Force Instruction 63-101 to include the requirements for interoperability and information support plans for all information technology systems, including automated information systems connected to the Global Information Grid.

Audit Response. Air Force Instruction 63-101 is interim Air Force guidance that program managers should use in conjunction with Air Force Instruction 10-601, "Capabilities Based Requirements Development," July 30, 2004. Air Force Instruction 10-601 implements the requirements of Chairman of the Joint Chiefs of Staff Instruction 6212.01C. Air Force Instruction 10-601 states that program authorities should use information support plans to document the information technology and NS system needs; objectives; and interface requirements for all acquisition category, non-acquisition category, and fielded programs.

Air Force Asset Inventory. The Air Force Chief Information Officer stated that the Air Force uses the Air Force Enterprise Information Technology Data Repository (formerly called the Systems Compliance Database) as its asset inventory. The Air Force Enterprise Information Technology Data Repository feeds into the DoD Information Technology Registry. Further, he stated that pending additional guidance, the Air Force will continue to populate the DoD Information Technology Registry.

Audit Response. Because DoD has not defined the content of the Global Information Grid asset inventory, the Air Force is not able to populate and maintain a Global Information Grid asset inventory for Air Force systems, as stated in the report. Although the Enterprise Information Technology Data Repository feeds into the DoD Information Technology Registry, the Principal Director to the Deputy DoD Chief Information Officer stated that the DoD Information Technology Registry is not adequate to use as the GIG asset inventory. However, the Principal Director stated that DoD may develop the DoD Information Technology Registry into the GIG asset inventory. We updated the report to reflect the Air Force asset inventory efforts.

Air Education and Training Command. The Air Force Chief Information Officer recommended changing "Air Force Training and Doctrine Command" to "Air Education and Training Command."

Audit Response. Neither command was mentioned in the report.

Appendix H. Report Distribution

Office of the Secretary of Defense

Under Secretary of Defense for Acquisition, Technology, and Logistics
Under Secretary of Defense (Comptroller)/Chief Financial Officer
 Deputy Chief Financial Officer
 Deputy Comptroller (Program/Budget)
Assistant Secretary of Defense for Networks and Information Integration/DoD Chief
 Information Officer
Director, Program Analysis and Evaluation
Director, Operational Test and Evaluation

Joint Staff

Director, Joint Staff
 Director for Command, Control, Communications, and Computers Systems
 Directorate (J-6)

Department of the Navy

Naval Inspector General
Auditor General, Department of the Navy

Department of the Air Force

Commander, Air Force Air Combat Command
 Commander, Air Intelligence Agency
 Commander, Air Force Information Warfare Center
Commander, Air Force Air Mobility Command
Commander, Air Force Space Command
Assistant Secretary of the Air Force (Acquisition)
 Deputy Assistant Secretary of the Air Force (Management Policy and Program
 Integration)
Assistant Secretary of the Air Force (Financial Management and Comptroller)
Air Force Deputy Chief of Staff for Air and Space Operations
 Director, Operational Capabilities Requirements Directorate
Air Force Deputy Chief of Staff for Warfighting Integration
 Director, Command, Control, Communications, and Computers, Intelligence,
 Surveillance, and Reconnaissance Infostructure Directorate
Auditor General, Department of the Air Force
Air Force Chief Information Officer
Commander, Air Force Operational Test and Evaluation Center
Director, Air Force Test and Evaluation Directorate
Commander, Air Force Communications Agency

Combatant Command

Inspector General, 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

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 and Financial Management, Committee on Government Reform
House Subcommittee on National Security, Emerging Threats, and International Relations, Committee on Government Reform
House Subcommittee on Technology, Information Policy, Intergovernmental Relations, and the Census, Committee on Government Reform

Joint Staff Comments



THE JOINT STAFF
WASHINGTON, DC

Reply ZIP Code:
20318-0300

DJSM 0024-05
08 January 2005

**MEMORANDUM FOR THE INSPECTOR GENERAL, DEPARTMENT OF
DEFENSE**

Subject: Draft Report on the Audit of the Implementation of Interoperability and Information Assurance Policies for Acquisition of Air Force Systems (D2002AE-0188)

1. Thank you for the opportunity to review the subject report.¹ The Joint Staff concurs in the draft report recommendations and will support them through participation as a principal member on the Interoperability Test Panel.
2. The Joint Staff point of contact is Commander Charles Moore II, USN; J-6I; 703-697-4232.

A handwritten signature in black ink that reads "NASchwartz".

NORTON A. SCHWARTZ
Lieutenant General, USAF
Director, Joint Staff

Reference:

1. OIG DOD E-mail, 19 November 2004, "FOUO: Draft Report for the Audit of the Implementation of Interoperability and Information Assurance Policies for Acquisition of Air Force Systems (D2002AE-0188)"

Department of the Air Force Comments



CHIEF INFORMATION OFFICER

DEPARTMENT OF THE AIR FORCE
OFFICE OF THE UNDER SECRETARY,
WASHINGTON DC

JAN 03 2005

MEMORANDUM FOR DEPUTY INSPECTOR GENERAL FOR AUDITING
OFFICE OF THE INSPECTOR GENERAL DEPARTMENT OF DEFENSE

FROM: 1155 Air Force Pentagon
Washington DC 20330-1155

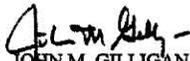
SUBJECT: Draft Report - Implementation of Interoperability and Information Assurance
Policies for Acquisition of Air Force Systems (Project No. D2002AE-0188)

This is in reply to your memorandum requesting the Assistant Secretary of the Air Force (Financial Management and Comptroller) provide Air Force comments on subject report.

We have reviewed the draft report and concur with the recommendation for the Chief Information Officer to "...issue policy to require program managers to prepare information support plans and obtain supportability certification before program decision reviews and before fielding the system...." This issue will be addressed in Air Force Policy Directive 33-2, *Information Assurance Program* that will undergo staffing early in 2005. We contacted SAF/AQ to ensure Air Force acquisition guidance includes the correct guidance as well.

We also concur with the recommendation that the Chief Information Officer "...verify that Air Force system program office prepared system security authorization agreements (SSAAs) before milestone decision points...." This information is collected in the Air Force Enterprise Information Technology Data Repository (EITDR). Further, AF-CIO personnel now verify the existence of SSAA as part of the Information Assurance Strategy review process.

Attached is a comments matrix with additional comments to assist you in improving the accuracy and completeness of the report. My point of contact for this issue is Lt Col David Biros at (703) 696-6317.


JOHN M. GILLIGAN
Chief Information Officer

Attachment
Comments Matrix

AF/XI Comments Matrix

Document: Draft Report for the Audit of the Implementation of Interoperability and IA Policies for Acquisition of AF Systems (D2002AE-0188)

Organization	Item #	Type	Page #	Comment	Rationale
XIC & CIO/P	1		4	<p>"Interoperability, Requirements and Certification Policy" and "DoD" Policy Paragraph. The paragraphs discuss DoD Policy related to Interoperability Requirements and Certification, but do not address DoDI 5000.2, <i>Operation of the Defense Acquisition System</i>, interoperability requirements discussed in Enclosure 4, IT Considerations, particularly Table E4.T1, CCA Compliance Table. In this enclosure, program managers are provided statutory and regulatory requirements regarding interoperability as part of Clinger Cohen Act compliance certification for mission critical and mission essential systems. In particular, paragraph E4.2.1 states, "At a minimum, the DoD Component CIO's confirmation or certification shall include a written description of the three material questions of section 3.6.4 and the considerations in Table E4.T1." Table E4.T.1 includes "Requirements Related to the Clinger-Cohen Act (CCA) of 1996 - The acquisition is consistent with the Global Information Grid policies and architecture, to include relevant standards. --- Applicable Program Documentation - APB (Interoperability KPP)." The DoD 5000 series are the DoD's primary acquisition program documents. If a system does not fall into the mission critical or essential system definition or if the system is an Automated Information System (AIS), program managers likely disregarded the need for CCA compliance.</p> <p>A recommendation should be added to the report that the DoDI 5000.2 should be updated so that it requires all IT related systems (including AIS connecting to the GIG) to meet the interoperability requirements found in DoDD 4630.5, <i>Interoperability and Supportability of Information Technology (IT) and National Security Systems (NSS)</i>.</p>	Completeness
XIC & CIO/P	2		5	<p>"C4I Support Plans, C4I Support Plan Policy" and "DoD Instruction" paragraphs. The same problem exists with these paragraphs in the report. It appears the DoD 5000 series, and its direction on C4ISP's or Information Support Plans was not part of the audit.</p> <p>Suggest a recommendation be included in the report that the DoDI 5000.2 be updated to state a C4ISP or Information Support Plan is required for all IT (including AIS connected to the GIG), rather than only requiring it for mission critical and mission essential systems.</p>	Completeness
XIC & CIO/P	3		6	<p>Air Force Memorandum paragraph discusses only a SAF/AQ Air Force Memorandum on C4I support plans. It does not address direction contained in AFI 33-202, <i>Network and Computer Security</i> or Air Force Pamphlet (AFPAM) 63-1701, <i>Program Protection Planning</i>.</p> <p>Recommend those documents be reviewed to determine if the audit results should be updated and including the salient information from those documents in this part of the report.</p>	Completeness

Page 4

Page 5

Page 6

XIC & CIO/P	4		8			<p>Recommendation: While AFPAM 63-1701 makes IT system certification and accreditation a part of the program managers program protection planning responsibilities, AFI 63-101, <i>Acquisition System</i> does not include IT security or certification requirements.</p> <p>Suggest an additional recommendation be included in this section of the report stating, "Air Force Instruction 63-101, <i>Acquisition System</i> should be updated to include interoperability and Information Support Plans for all IT systems (including Automated Information Systems (AIS) connected to the Global Information Grid (GIG))."</p>	Completeness
XIC & CIO/P	5		16-20			<p>Air Force does asset inventory using the Enterprise Information Technology Data Repository (EITDR) (formerly called the Systems Compliance Database (SCD). The EITDR feeds into the DoD IT Registry.</p> <p>Pending additional guidance, the Air Force will continue to populate the DoD IT Registry.</p> <p>Recommend auditors contact HQ USAF/ILCS, Mr. Ken Page (DSN 425-6300) for clarification.</p>	Accuracy
XIC & CIO/P	6		20			<p>Recommend changing "Air Force Training and Doctrine Command" to "Air Education and Training Command"</p>	Accuracy.

Team Members

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

John E. Meling
Jack D. Snider
Suellen R. Brittingham
Alice F. Carey
Neal J. Gause
Kevin W. Klein
Tracey E. Dismukes
Patricia A. Joyner
Lidet K. Negash
Tomaso Pack
Todd L. Kowalski
Christopher M. Scrabis
Zachary M. Williams
Deborah J. Thomas
Joyce Tseng
Julie B. Vaillancourt
Peter C. Johnson
Anh H. Tran
Lieutenant Colonel Shurman L. Vines, USA
Ernest G. Fine
Cindy L. Gladden
Jacqueline N. Pugh