September 14, 2006

Information System Security

Summary of Information Assurance Weaknesses Found in Audit Reports Issued from August 1, 2005, through July 31, 2006

(D-2006-110)

Department of Defense
Office of Inspector General

Quality *Integrity* *Accountability*

Additional Copies

To obtain additional copies of this report, contact the Secondary Reports Distribution Unit 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 Corporate Analysis and Planning at (703) 604-9142 (DSN 664-9142) or fax (703) 604-8932. Ideas and requests can also be mailed to:

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

Acronyms

FISMA	Federal Information Security Management Act
GAO	Government Accountability Office
IA	Information Assurance
OIG	Office of the Inspector General
OMB	Office of Management and Budget

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

September 14, 2006

MEMORANDUM FOR ASSISTANT SECRETARY OF THE AIR FORCE
(FINANCIAL MANAGEMENT AND COMPTROLLER)
NAVAL INSPECTOR GENERAL
AUDITOR GENERAL, DEPARTMENT OF THE ARMY

SUBJECT: Report on Summary of Information Assurance Weaknesses Found in Audit Reports Issued from August 1, 2005, through July 31, 2006 (Report No. D-2006-110)

We are providing this summary report for information and use. We did not issue a draft report because this report summarizes material that has already been staffed and reported. This report contains no recommendations; therefore, no written response to this report was required, and none was received.

We appreciate the courtesies extended to the staff. Questions should be directed to Ms. Kathryn M. Truex at (703) 604-8966 (DSN 664-9077) or Ms. Karen J. Goff at (703) 604-9005 (DSN 664-9005). See Appendix G for the report distribution. The team members are listed inside the back cover.

By direction of the Deputy Inspector General for Auditing:

Wanda A. Scott
Assistant Inspector General
Readiness and Operations Support

Department of Defense Office of Inspector General

Report No. D-2006-110 **September 14, 2006**
(Project No. D2006-D000LB-0145.000)

Summary of Information Assurance Weaknesses Found in Audit Reports Issued from August 1, 2005, through July 31, 2006

Executive Summary

Who Should Read This Report and Why? Military and civil service personnel who develop, manage, operate, or oversee DoD information technology resources should read this report to obtain better awareness of identified information security challenges and the potential risks those challenges pose within the context of a shared DoD information technology environment.

Background. This report summarizes information assurance weaknesses that the Government Accountability Office, the DoD Office of the Inspector General, the Army Audit Agency, the Naval Audit Service, and the Air Force Audit Agency reported between August 1, 2005, and July 31, 2006. It supports the Federal Information Security Management Act of 2002, which requires agencies submit to the Office of Management and Budget the results of an annual independent evaluation of the effectiveness of their information security programs and practices. The evaluation should include testing of the effectiveness of information security policies, procedures, and practices of a subset of the agency's information systems and may be based, in whole or in part, on an audit, evaluation, or report relating to agency programs or practices. This report is the eighth information assurance summary report issued by the DoD Office of the Inspector General since January 1999.

Summary of Information Assurance Weaknesses. Between August 1, 2005, and July 31, 2006, the Government Accountability Office, the DoD Office of the Inspector General, the Army Audit Agency, the Naval Audit Service, and the Air Force Audit Agency issued 28 reports that addressed a wide range of information assurance weaknesses that persist throughout DoD systems and networks. If the weaknesses the reports identify continue, they will impede the ability of DoD to mitigate risks in a shared information technology environment. Those risks include harm resulting from loss, misuse, unauthorized access, and modification of information or information systems. A loss of information is itself unacceptable and could result in loss of mission effectiveness.

Table of Contents

Background

This report summarizes information assurance (IA) weaknesses that the Government Accountability Office (GAO), the DoD Office of Inspector General (OIG), the Army Audit Agency, the Naval Audit Service, and the Air Force Audit Agency (DoD audit community) identify in reports between August 1, 2005, and July 31, 2006. This report is one in a series and is the eighth IA summary report the DoD OIG has issued since January 1999. The eight IA summary reports contain 369 reports summarizing IA weaknesses.

This report supports the DoD OIG response to section 3545, Public Law 107-347, Title III, "Federal Information Security Management Act," December 17, 2002, requiring agencies to submit the results of an annual independent evaluation of the effectiveness of their information security policies, procedures, and practices of a subset of the agency's information systems to the Office of Management and Budget (OMB). The evaluation results may be based, in whole or in part, on an audit, evaluation, or report relating to agency programs and practices.

Federal Information Security Management Act. The Federal Information Security Management Act (FISMA) provides a comprehensive framework for ensuring the effectiveness of IA controls over information resources that support Federal operations and assets. FISMA requires that each agency develop, document, and implement an agency-wide IA program to provide IA for the information and information systems that support the operations and assets of the agency. Each agency is to ensure compliance with FISMA and related policies, procedures, standards, and guidelines, including the information security standards promulgated under section 11331, title 40, United States Code (40 U.S.C. 11331),"Responsibilities for Federal information systems standards." 40 U.S.C. 11331 requires standards and guidelines for Federal information systems to be based on standards and guidelines developed by the National Institute of Standards and Technology. FISMA permits agencies to employ IA standards developed by the agency as long as the standards are more stringent than those prescribed under FISMA.

National Institute of Standards and Technology. To meet its statutory responsibilities under FISMA, the National Institute of Standards and Technology, under the U.S. Department of Commerce, developed a series of standards and guidelines for Federal agencies that provide adequate IA for agency operations and assets. Specifically, the Computer Security Division of the Information Technology Laboratory developed computer security prototypes, tests, standards, and procedures designed to protect sensitive information from unauthorized access or modification. Focus areas include cryptographic technology and applications, advanced authentication, public key infrastructure, internetworking security, criteria and assurance, and security management and support. The standards and guidelines present the results of National Institute of Standards and Technology studies, investigations, and research on information technology security issues.

DoD Information Technology Security Certification and Accreditation Process. DoD continues to rely upon DoD Instruction 5200.40, "Department of

Defense Information Technology Security Certification and Accreditation Process (DITSCAP)," December 30, 1997, and DoD Manual 8510.1-M, "Department of Defense Information Technology Security Certification and Accreditation Process Application Manual," July 31, 2000, to direct the certification and accreditation process for DoD national security and non-national security information systems. On July 6, 2006, the office of the Assistant Secretary of Defense for Networks and Information Integration issued the "Department of Defense Information Assurance Certification and Accreditation Process," as interim guidance for IA certification and accreditation throughout DoD. The interim guidance is to supersede the DoD Information Technology Security Certification and Accreditation Process and was effective when issued.

DoD Information Assurance Guidance. The primary DoD IA guidance includes:

- DoD Directive 8500.1, "Information Assurance," October 24, 2002, which establishes policy and assigns responsibility to achieve IA throughout DoD;

- DoD Instruction 8500.2, "Information Assurance Implementation," February 6, 2003, which implements the policy, assigns responsibilities, and prescribes procedures for applying integrated layered protection of DoD information systems and networks as DoD Directive 8500.1 outlines; and

- DoD Directive 8570.1, "Information Assurance Training, Certification, and Workforce Management," August 15, 2004, which establishes policy and assigns responsibility for DoD IA training, certification, and workforce management.

Objectives

This is one in a series of summary reports that the DoD OIG has completed annually since 1999. The overall objective was to summarize reports by GAO and the DoD audit community between August 1, 2005, and July 31, 2006. This summary report supports the DoD OIG response to the requirements of FISMA.

See Appendix A for a discussion of the scope and methodology and Appendix B for prior coverage related to the objective.

Information Assurance Weaknesses Persist Throughout DoD

Between August 1, 2005, and July 31, 2006, GAO and the DoD audit community issued 28 reports addressing a wide range of IA weaknesses that persist throughout DoD systems and networks.[*] This report summarizes those reports.

If the IA weaknesses identified in the reports continue, they will impede the ability of DoD to mitigate risks in a shared information technology environment. Those risks include harm resulting from loss, misuse, unauthorized access, and modification of information or information systems. A loss of information in DoD information systems is itself unacceptable and could additionally result in the loss of mission effectiveness.

Persistent Information Assurance Weaknesses

GAO and the DoD audit community issued 28 reports between August 1, 2005, and July 31, 2006, that identify weaknesses in IA areas defined by FISMA, the DoD Information Technology Security Certification and Accreditation Process, or DoD Instruction 8500.2. The table on the next page shows the number of GAO and DoD audit community reports that identify weaknesses in IA areas. See Appendix C for a glossary of specialized terms.

[*] The DoD OIG reported similar IA weaknesses in seven previous IA summary reports.

Audit Reports Identifying Information Assurance Weaknesses
(August 1, 2005, through July 31, 2006)

IA Areas	GAO	DoD OIG	Military Departments	Total
Access Controls	0	10	9	19
Audit Trails	0	6	0	6
Certification and Accreditation	1	5	6	12
Configuration Management	0	4	2	6
Contingency Plans	0	3	3	6
Continuity of Operations Plans	0	2	1	3
Federal Information Systems Inventory Reporting	0	1	0	1
Incident Response	0	2	0	2
Personnel Security	0	3	1	4
Physical Security	0	4	0	4
Plans of Action and Milestones	1	3	0	4
Risk Assessments	1	1	1	3
Security Awareness, Training, and Education	1	7	0	8
Security Policies and Procedures	0	9	3	12
Segregation of Duties	0	3	1	4

Reports issued during the reporting period most frequently cited weaknesses in the following IA areas: access controls; certification and accreditation; security awareness, training, and education; and security policies and procedures. See Appendix D for a matrix of the specific IA weakness listed by report and Appendix E for a list of reports reviewed for this IA summary report.

Access Controls. Access controls limit access to information system resources only to authorized users, programs, process, or other systems. GAO and the DoD audit community reported weaknesses related to access controls in 19 issued reports. The weaknesses reported related to:

- user account management, including maintaining complete user account forms, reviewing accounts periodically to determine whether access is still necessary, and reviewing user activity; and

- actions allowed by the systems, including denial of access as a result of invalid logon attempts.

Certification and Accreditation. Certification and accreditation is a combined process that makes up the DoD Information Technology Security Certification and Accreditation Process. The DoD certification and accreditation process is a standard process, set of activities, general tasks, and a management structure to certify and accredit information systems that will maintain the IA and security posture of the Defense Information Infrastructure. GAO and the DoD audit community identified weaknesses related to certification and accreditation in 12 reports. Issued reports identified systems not fully certified and accredited

and DoD Information Technology Security Certification and Accreditation Processes that were not fully implemented. In addition, System Security Authorization Agreements—the documentation used for the certification and accreditation process—were found deficient because the agreements:

- did not contain all the security requirements,
- did not reflect the system environment,
- were not approved by required individuals, and
- were not prepared in some instances.

Security Awareness, Training, and Education. Issued reports identified weaknesses in the area of training for personnel with information security responsibilities and administration of training. GAO and DoD OIG reported weaknesses relating to security awareness, training, and education in eight issued reports.

Security Policies and Procedures. Issued audit reports identified weaknesses in security policies and procedures. GAO and the DoD audit community reported weaknesses relating to security policies and procedures in 12 issued reports.

The seven previous IA summary reports summarized 341 reports citing IA weaknesses throughout DoD. Of those 341 reports, 45 reports were older than 12 months with final management action pending to correct agreed-upon IA weaknesses. Prompt action to correct the outstanding weaknesses is necessary to mitigate ongoing vulnerabilities in the DoD IA program. See Appendix F for a listing of reports with unresolved recommendations relating to IA weaknesses.

Conclusion

Many of the weaknesses reported occurred because adequate security program management including security policies and procedures were not in place. Without adequate security program management and security policies and procedures, DoD cannot provide and maintain appropriate security for managing, protecting, and distributing information. Implementing adequate security program management and security policies and procedures may reduce the risk of persistent IA weaknesses, thereby reducing harm from loss, misuse, unauthorized access, or modification of information or information systems.

Appendix A. Scope and Methodology

This report summarizes the DoD IA weaknesses identified in 28 reports that GAO and the DoD audit community issued from August 1, 2005, through July 31, 2006. We reviewed the Web sites of GAO and each component audit organization, as well as requested reports discussing IA weaknesses from each such organization to prepare this summary. We also reviewed prior IA summary reports and determined, with the assistance of GAO and DoD audit community follow-up organizations, summarized reports with unresolved recommendations on IA weaknesses.

This summary report does not make recommendations because recommendations were made in the summarized reports. We did not follow generally accepted government auditing standards in conducting this project because it is a summary project. We did not summarize congressional testimonies as originally announced because reviews of IA testimonies issued during the reporting period identified that the testimonies did not apply specifically, if at all, to DoD. Also, we did not include independent tests of management controls or validate the information or results reported in the summarized reports. This summary report supports the DoD OIG response to the OMB questions relating to FISMA. We conducted this summary work from March through August 2006.

Use of Computer-Processed Data. We did not use computer-processed data when compiling information for this summary report.

Appendix B. Prior Coverage

The DoD OIG has issued seven information security summary reports. Report No. 99-069 can be obtained by contacting the Secondary Reports Distribution Unit at (703) 604-8937 (DSN 664-8937) or fax (703) 604-8932. The remainder of the reports are For Official Use Only and can be obtained by contacting the Freedom of Information Act Requester Service Center at (703) 604-9775 (DSN 664-9775) or fax (703) 602-0294.

DoD IG Report No. D-2005-110, "Summary of Information Security Weaknesses Reported by Major Oversight Organizations From August 1, 2004, through July 31, 2005 (FOUO)," September 23, 2005

DoD IG Report No. D-2004-116, "Information Security Weaknesses Reported by Major Oversight Organizations From August 1, 2003, through July 31, 2004 (FOUO)," September 23, 2004

DoD IG Report No. D-2004-038, "Information Assurance Challenges – A Summary of Results Reported from August 1, 2002, through July 31, 2003 (FOUO)," December 22, 2003

DoD IG Report No. D-2003-024, "Information Assurance Challenges – An evaluation of Audit Results Reported from August 23, 2001, through July 31, 2002 (FOUO)," November 21, 2002

DoD IG Report No. D2001-182, "Information Assurance Challenges – A Summary of Audit Results Reported April 1, 2000, through August 22, 2001 (FOUO)," September 19, 2001

DoD IG Report No. D2000-124, "Information Assurance Challenges – A Summary of Audit Results Reported December 1, 1998, through March 31, 2000 (FOUO)," May 15, 2000

DoD IG DoD Report No. 99-069, "Summary of Audit Results – DoD Information Assurance Challenges," January 22, 1999

Appendix C. Glossary

Access Controls – Access controls limit information system resources to authorized users, programs, processes, or other systems.

Audit Trail – An audit trail is a chronological record of system activities that enable the reconstruction and examination of the sequence of events and/or changes in an event.

Certification and Accreditation – Certification and accreditation is a combined process that makes up the DoD Information Technology Security Certification and Accreditation Process.

- **Accreditation** – Accreditation is the formal declaration by a designated accrediting authority that an information system is approved to operate in a particular security mode at an acceptable level of risk, based on the implementation of an approved set of technical, managerial, and procedural safeguards.

- **Certification** – Certification is a comprehensive evaluation of the technical and nontechnical security safeguards of an information system to support the accreditation process that establishes the extent to which a particular design and implementation meets a set of specified security requirements.

Configuration Management – Configuration management is the management of security features and assurances through control of changes made to hardware, software, firmware, documentation, test, test fixtures, and test documentation throughout the life cycle of an information system.

Contingency Plan – A contingency plan is maintained for emergency response, backup operations, and post-disaster recovery of an information system to ensure the availability of critical resources and to facilitate the continuity of operations in an emergency situation.

Continuity of Operations Plan – A continuity of operations plan is a plan for continuing an organization's essential functions at an alternate site and performing those functions for the duration of an event with little or no loss of continuity before returning to normal operations.

Federal Information Systems Inventory Reporting – The head of each agency must develop and maintain an inventory of major information systems, including major national security systems, operated by or under the control of the agency. The inventory of information systems or networks should include those not operated by or under the control of the agency.

Incident Response – Also known as incident handling, incident response is the mitigation of violations of security policies and recommended practices.

Personnel Security – The objective of the Personnel Security Program is to ensure that the military, civilian, and contractor personnel assigned to and retained in sensitive positions in which they could potentially damage national security are, and remain, reliable and trustworthy, and no reasonable basis exists for doubting their allegiance to the United States. Assignment to sensitive duties is granted only to individuals who are U.S. citizens and for whom an appropriate investigation has been completed.

Physical Security – Physical security refers to measures taken to protect systems, buildings, and related supporting infrastructure against threats associated with their physical environment.

Plan of Action and Milestones – A plan of action and milestones is a tool that identifies tasks that need to be accomplished. A plan of action and milestones details resources required to accomplish the elements of the plan, any milestones in meeting the task, and scheduled completion dates for the milestones. The purpose of a plan of action and milestones is to assist agencies in identifying, assessing, prioritizing, and monitoring the progress of corrective efforts for security weaknesses found in programs and systems.

Policies and Procedures – Policies and procedures are the aggregate of directives, regulations, rules, and practices that regulate how an organization manages, protects, and distributes information. Information security policy can be contained in public laws, Executive orders, DoD Directives, and local regulation.

Risk Assessment – Risk assessment is an analysis of threats to and vulnerabilities of information systems and the potential impact resulting form the loss of an information system and its capabilities. The analysis is used as a basis for identifying appropriate and cost-effective security measures.

Security Awareness, Training, and Education

- **Awareness** – Awareness is a learning process that sets the stage for training by changing individual and organization attitudes to realize the importance of security and the adverse consequences of its failure.

- **Training** – Training is teaching people the knowledge and skills that will enable them to perform their jobs more effectively.

- **Education** – Education focuses on developing the ability and vision to perform complex, multi-disciplinary activities and the skills needed to further the information technology security profession. Education activities include research and development to keep pace with changing technologies.

Segregation of Duties – Segregation of duties refers to dividing roles and responsibilities so that a single individual cannot subvert a critical process.

Appendix D. Matrix of Information Assurance Weaknesses Reported From August 1, 2005, through July 31, 2006

Report No.	Access Controls	Audit Trails	Certification and Accreditation	Configuration Management	Contingency Plan	Continuity of Operations Plans	Federal Information Systems Inventory Reporting	Incident Response	Personnel Security	Physical Security	Plan of Action and Milestones	Risk Assessment	Security Awareness, Training, Education	Security Policies and Procedures	Segregation of Duties
Government Accountability Office															
GAO-06-31			X								X	X	X		
Office of the Inspector General of the DoD															
D-2006-096	X	X	X		X			X	X		X		X	X	
D-2006-086	X	X		X	X					X		X	X	X	X
D-2006-084														X	
D-2006-079	X		X			X					X		X		
D-2006-078														X	
D-2006-074	X			X						X			X		
D-2006-069	X	X		X		X				X			X	X	X
D-2006-060			X	X											
D-2006-053	X	X	X		X			X			X		X	X	
D-2006-052		X							X				X		
D-2006-046	X	X	X											X	X
D-2006-042							X								
D-2006-033	X													X	

Report No.	Access Controls	Audit Trails	Certification and Accreditation	Configuration Management	Contingency Plan	Continuity of Operations Plans	Federal Information Systems Inventory Reporting	Incident Response	Personnel Security	Physical Security	Plan of Action and Milestones	Risk Assessment	Security Awareness, Training, Education	Security Policies and Procedures	Segregation of Duties
D-2006-030	X														
D-2006-003	X								X	X					
D-2005-099														X	
Army Audit Agency															
A-2006-0152-FFH				X											
Naval Audit Service															
N2006-0003	X								X					X	
Air Force Audit Agency															
F2006-0008-FB2000	X		X		X										
F2006-0007-FB2000	X		X			X									
F2006-0006-FB2000	X		X		X										
F2006-0004-FB2000			X											X	
F2006-0003-FB2000	X														
F2006-0001-FB2000	X		X	X	X							X		X	X
F2005-0010-FB2000	X		X												
F2005-0010-FD4000	X														
F2005-0009-FB2000	X														
Total	**19**	**6**	**12**	**6**	**6**	**3**	**1**	**2**	**4**	**4**	**4**	**3**	**8**	**12**	**4**

Appendix E. Audit Reports Issued Between August 1, 2005, and July 31, 2006, Identifying Information Assurance Weaknesses

GAO

GAO Report No. GAO-06-3, "The Defense Logistics Agency Needs to Fully Implement Its Security Program," October 7, 2005

DoD IG

DoD IG Report No. D-2006-096, "Select Controls for the Information Security of the Command and Control Battle Management Communications System (FOUO)," July 14, 2006

DoD IG Report No. D-2006-086, "Report on General and Applications Controls at the Defense Information Systems Agency, Center for Computing Services (FOUO)," May 18, 2006

DoD IG Report No. D-2006-084, "Information Assurance of Commercially Managed Collaboration Services for the Global Information Grid," May 17, 2006

DoD IG Report No. D-2006-079, "Review of the Information Security Operational Controls of the Defense Logistic Agency's Business Systems Modernization-Energy," April 24, 2006

DoD IG Report No. D-2006-078, "Defense Information Systems Agency Encore II Information Technology Solutions Contract (FOUO)," April 21, 2006

DoD IG Report No. D-2006-074, "Technical Report on the Defense Civilian Pay System General and Application Controls (FOUO)," April 12, 2006

DoD IG Report No. D-2006-069, "Technical Report on the Defense Business Management System (FOUO)," April 3, 2006

DoD IG Report No. D-2006-060, "System Engineering Planning for the Ballistic Missile Defense System (FOUO)," March 2, 2006

DoD IG Report No. D-2006-053, "Select Controls for the Information Security of the Ground-Based Midcourse Defense Communications Network," February 24, 2006

DoD IG Report No. D-2006-052, "DoD Organization Information Assurance Management of Information Technology Goods and Services Acquired Through Interagency Agreements," February 23, 2006

DoD IG Report No. D-2006-046, "Technical Report on the Defense Property Accountability System," January 27, 2006

DoD IG Report No. D-2006-042, "Security Status for Systems Reported in DoD Information Technology Databases," December 30, 2005

DoD IG Report No. D-2006-033, "Defense Finance and Accounting Service Corporate Database User Access Controls," December 7, 2005

DoD IG Report No. D-2006-030, "Report on Diagnostic Testing at the Defense Information Systems Agency, Center for Computing Services (FOUO)," November 30, 2005

DoD IG Report No. D-2006-003, "Security Controls Over Selected Military Health System Corporate Databases (FOUO)," October 7, 2005

DoD IG Report No. D-2005-099, "Status of Selected DoD Policies on Information Technology Governance," August 19, 2005

Army Audit Agency

Army Audit Agency Report No. A-2006-0152-FFH, "Information Assurance for Medical Communications for Combat Casualty Care," June 30, 2006

Naval Audit Service

Naval Audit Service Report No. N2006-0003, "Safeguarding Department of the Navy Protected Health Information in Medical Automated Information Systems," November 10, 2005

Air Force Audit Agency

Air Force Audit Agency Report No. F2006-0008-FB2000, "System Controls for Item Manager Wholesale Requisition Process System," June 21, 2006

Air Force Audit Agency Report No. F2006-0007-FB2000, "Missile Readiness Integrated Support Facility/Integrated Missile Database System Controls," May 30, 2006

Air Force Audit Agency Report No. F2006-0006-FB2000, "Controls for the Wholesale and Retail Receiving and Shipping System," May 19, 2006

Air Force Audit Agency Report No. F2006-0004-FB2000, “Implementation of Selected Aspects of Security in Air Force Systems,” April 17, 2006

Air Force Audit Agency Report No. F2006-0003-FB2000, “Automated Civil Engineer System - Real Property Controls,” April 12, 2006

Air Force Audit Agency Report No. F2006-0001-FB2000, “Reliability of Data Supporting Air Force Information and Logistics Systems,” November 15, 2005

Air Force Audit Agency Report No. F2005-0010-FB2000, “System Controls for Financial Inventory Accounting and Billing System,” September 20, 2005

Air Force Audit Agency Report No. F2005-0010-FD4000, “Military Equal Opportunity,” August 9, 2005

Air Force Audit Agency Report No. F2005-0009-FB2000, “Base Realignment and Closer Facility Analysis Capability Tool,” August 8, 2005

Appendix F. Audit Reports from Prior Information Assurance Summary Reports with Unresolved Recommendations

IA weaknesses continue to exist throughout DoD. Of the 341 reports included in seven prior IA summary reports, 45 reports were older than 12 months with final management action pending to correct agreed-upon IA weaknesses earlier reports identify. The listing of reports with unresolved recommendations was compiled based on information GAO and the DoD audit community provided in June 2006 and may be incomplete based on the extent of information maintained in their respective follow-up systems.

DoD IG

DoD IG Report No. D-2005-094, "Proposed DoD Information Assurance Certification and Accreditation Process (FOUO)," July 21, 2005

DoD IG Report No. D-2005-069, "Audit of the General and Application Controls of the Defense Civilian Pay System (FOUO)," May 13, 2005

DoD IG Report No. D-2005-054, "Audit of the DoD Information Technology Security Certification and Accreditation Process (FOUO)," April 28, 2005

DoD IG Report No. D-2005-034, "Implementation of Interoperability and Information Assurance Policies for Acquisition of Air Force Systems," February 2, 2005

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

DoD IG Report No. D-2005-025, "DoD FY 2004 Implementation of the Federal Information Security Management Act for Information Technology Training and Awareness," December 17, 2004

DoD IG Report No. D-2005-023, "Assessment of DoD Plan of Action and Milestone Process (FOUO)," December 13, 2004

DoD IG Report No. D-2004-114, "The Follow-up on the Government Accountability Office and U.S. Army Audit Agency Recommendations for the U.S. Army Corps of Engineers (FOUO)," September 21, 2004

DoD IG Report No. D-2004-041 "The Security of the Army Corps of Engineers Enterprise Infrastructure Services Wide-Area Network (FOUO)," December 26, 2003

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

DoD IG Report No. D-2003-134, "System Security of the Army Corps of Engineers Financial Management System (FOUO)," September 15, 2003

DoD IG Report No. D-2003-114, "Defense Logistics Agency's Implementation of the Government Information Security Reform (FOUO)," June 30, 2003

DoD IG Report No. D-2002-108, "Standard Procurement System Certification and Accreditation Process (FOUO)," June 19, 2002

DoD IG Report No. D-2001-148, "Automated Transportation Payments," June 22, 2001

DoD IG Report No. D-2001-141, "Allegations to the Defense Hotline on the Defense Security Assistance Management System," June 19, 2001

DoD IG Report No. D-2001-016, "Security Controls Over Contractor Support for Year 2000 Renovation," December 12, 2000

Army Audit Agency

Army Audit Agency Report No. A-2005-0200-FFI, "Headquarters, Department of the Army Information Technology Purchase Process," June 27, 2005

Army Audit Agency Report No. A-2005-0204-FFC, "Security of Civil Works Water Resources Infrastructure U.S. Army Corps of Engineers," June 23, 2005

Army Audit Agency Report No. A-2005-0175-FFI, "Common-User Support (Single Directorate of Information Management Project)," June 14, 2005

Army Audit Agency Report No. A-2004-0486-FFC, "Follow-up Audit of Corps of Engineers Financial Management System, General and Application Controls," September 9, 2004

Army Audit Agency Report No. A-2004-0216-FFB, "Information Systems Security Material Weakness," April 8, 2004

Army Audit Agency Report No. A-2003-0366-FFB, "The Army's FY 01 Response to DoD for the Government Information Security Reform Act," August 5, 2003

Army Audit Agency Report No. A-2003-0287-FFB, "Selected Aspects of Information Assurance," June 5, 2003

Army Audit Agency Report No. A-2003-0283-FFB, "Selected Aspects of Information Assurance," May 30, 2003

Army Audit Agency Report No. A-2002-0610-FFC, "Corps of Engineers Financial Management System: General and Application Controls," September 30, 2002

Army Audit Agency Report No. A-2002-0587-FFB, "The Army's Implementation of the Government Information Security Reform Act - Lessons Learned," September 30, 2002

Army Audit Agency Report No. AA 01-319, "Corps of Engineers Financial Management System: General and Application Controls," June 26, 2001

Army Audit Agency Report No. AA 00-287, "Information Assurance -Phase V: Information Assurance Vulnerability Alert Process (FOUO)," June 30, 2000

Army Audit Agency Report No. AA 00-286, "Information Assurance - Phase IV: Reporting Process and Vulnerability Assessment Results (FOUO)," June 30, 2000

Naval Audit Services

Naval Audit Services Report No. N2005-0049, "Information Security Controls at Naval Shipyards," July 7, 2005

Naval Audit Services Report No. N2005-0036, "Verification of the Reliability and Validity of the Navy Enlisted System Data (FOUO)," March 30, 2005

Naval Audit Services Report No. N2004-0063, "Information Security - Operational Controls at Naval Aviation Depots," July 9, 2004

Naval Audit Services Report No. N2003-0060, "Reliability and Validity of the Optimized Naval Logistics Command Management Information System," July 22, 2003

Naval Audit Services Report No. N2003-0012, "Verification of the Reliability and Validity of the Department of the Navy's Total Force Manpower Management System (TFMMS) Data," November 8, 2002

Air Force Audit Agency

Air Force Audit Agency Report No. F2005-0005-FB4000, "Certification and Accreditation of Air Force Major Command Systems," July 11, 2005

Air Force Audit Agency Report No. F2004-0006-FB2000, "System Controls for Reliability and Maintainability Information System," September 27, 2004

Air Force Audit Agency Report No. F2004-0006-FB4000, "Visibility of Air Force Information Technology Resources," May 4, 2004

Air Force Audit Agency Report No. F2004-0020-FBP000, "PACAF Storage Area Network, 15th Airlift Wing, Hickam AFB, Hawaii," March 3, 2004

Air Force Audit Agency Report No. F2004-0021-FBP000, "PACAF Storage Area Network, HQ Pacific Air Force, Hickam AFB, Hawaii," March 3, 2004

Air Force Audit Agency Report No. F2003-0010-FB4000, "Air Force Space Command Information Security Program and Practices (FOUO)," June 30, 2003

Air Force Audit Agency Report No. F2003-0005-FB1000, "Comptroller Quality Assurance Program" July 24, 2003

Air Force Audit Agency Report No. F2003-0014-FB4000, "Certification and Accreditation of Air Force Classified System (FOUO)," August 20, 2003

Air Force Audit Agency Report No. F2002-0019-WH0000, "Classified Computer Equipment, 353d Special Operations Group, Kadena Air Base, Japan," December 11, 2001

Air Force Audit Agency Report No. F2002-0017-WH0000, "Classified Computer Equipment, 18th Wing, Kadena Air Base, Japan," November 29, 2001

Air Force Audit Agency Report No. 00054006, "Air Force Restoration Information Management System Controls," May 18, 2001

Appendix G. Report Distribution

Office of the Secretary of Defense

Under Secretary of Defense for Acquisition, Technology, and Logistics
    Director, Defense Business Transformation Agency
Under Secretary of Defense (Comptroller)/Chief Financial Officer
Under Secretary of Defense for Personnel and Readiness
Assistant Secretary of Defense for Networks and Information Integration/Chief Information Officer
Assistant Secretary of Defense for Health Affairs/Chief Information Officer
Assistant Secretary of Defense for Intelligence Oversight/Chief Information Officer
Chief Information Officer, Office of the Secretary of Defense
Director, Program Analysis and Evaluation

Joint Staff

Director, Joint Staff
Chief Information Officer, Joint Staff

Department of the Army

Assistant Secretary of the Army (Financial Management and Comptroller)
Auditor General, Department of the Army
Chief Information Officer, Department of Army

Department of the Navy

Assistant Secretary of the Navy (Financial Management and Comptroller)
Naval Inspector General
Auditor General, Department of the Navy
Chief Information Officer, Department of the Navy
Chief Information Officer, U.S. Marine Corps

Department of the Air Force

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

Unified Commands

Chief Information Officer, U.S. Central Command
Chief Information Officer, U.S. European Command
Chief Information Officer, U.S. Joint Forces Command
Chief Information Officer, U.S. Northern Command
Chief Information Officer, U.S. Pacific Command
Chief Information Officer, U.S. Southern Command
Chief Information Officer, U.S. Special Operations Command
Chief Information Officer, U.S. Strategic Command
Chief Information Officer, U.S. Transportation Command

Other Defense Organizations

Chief Information Officer, American Forces Information Service
Chief Information Officer, Defense Advanced Research Projects Agency
Chief Information Officer, Defense Contract Audit Agency
Chief Information Officer, Defense Contract Management Agency
Chief Information Officer, Defense Commissary Agency
Chief Information Officer, Defense Finance and Accounting Agency
Chief Information Officer, Defense Human Resource Activity
Chief Information Officer, Defense Information Systems Agency
Chief Information Officer, Defense Logistics Agency
Chief Information Officer, Department of Defense Education Activity
Chief Information Officer, Department of Defense Inspector General
Chief Information Officer, Defense Security Cooperation Agency
Chief Information Officer, Defense Security Service
Chief Information Officer, Defense Technical Information Center
Chief Information Officer, Defense Threat Reduction Agency
Chief Information Officer, DoD Test Resources Management Center
Chief Information Officer, Defense Technology Security Administration
Chief Information Officer, Missile Defense Agency
Chief Information Officer, Pentagon Force Protection Agency
Chief Information Officer, TRICARE Management Agency
Chief Information Officer, U.S. Mission North Atlantic Treaty Organization
Chief Information Officer, Washington Headquarters Service

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

Team Members

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

Kathryn M. Truex
Karen J. Goff
Michael D. Durda
Courtney E. Woodruff
Dawn M. Russell