

# Inspector General

United States  
Department of Defense



Summary of Information Assurance Weaknesses Found in  
Audit Reports Issued From August 1, 2006,  
Through July 31, 2007

### **Additional Copies**

To obtain additional copies of this report, visit the Web site of the Department of Defense Inspector General at <http://www.dodig.mil/audit/reports> or 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 the Office of the Deputy Inspector General for Auditing at (703) 604-9142 (DSN 664-9142) or fax (703) 604-8932. Ideas and requests can also be mailed to:

ODIG-AUD (ATTN: Audit Suggestions)  
Department of Defense Inspector General  
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.mil](mailto:hotline@dodig.mil) [www.dodig.mil/hotline](http://www.dodig.mil/hotline)

### **Acronyms**

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



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

September 12, 2007

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, 2006, Through July 31, 2007  
(Report No. D-2007-123)

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 published. 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 664-8966) or Mr. Robert R. Johnson at (703) 604-9024 (DSN 664-9024). 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:

*for* Robert T. Pringbach II  
Wanda A. Scott  
Assistant Inspector General  
Readiness and Operations Support

## Department of Defense Office of Inspector General

Report No. D-2007-123

September 12, 2007

(Project No. D2007-D000LB-0115.000)

### Summary of Information Assurance Weaknesses Found in Audit Reports Issued From August 1, 2006, Through July 31, 2007

#### 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 challenges to information assurance and the potential risks those challenges pose in 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 Inspector General, the Army Audit Agency, the Naval Audit Service, and the Air Force Audit Agency reported between August 1, 2006, and July 31, 2007. It supports the Federal Information Security Management Act of 2002, which requires that 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 ninth information assurance summary report issued by the DoD Office of the Inspector General since January 1999.

**Summary of Information Assurance Weaknesses.** Between August 1, 2006, and July 31, 2007, the Government Accountability Office, the DoD Office of Inspector General, the Army Audit Agency, the Naval Audit Service, and the Air Force Audit Agency issued 36 reports addressing a wide range of information assurance weaknesses that persist throughout DoD systems and networks. If these weaknesses continue, they will impede the ability of DoD to mitigate risks in a shared information technology environment. Those risks include unauthorized access to information or information systems and their consequent loss, misuse, or modification. A loss of information is itself unacceptable and could result in loss of mission effectiveness.

# Table of Contents

---

<b>Executive Summary</b>	i
<b>Background</b>	1
<b>Objectives</b>	2
<b>Finding</b>	
Information Assurance Weaknesses Persist Throughout DoD	3
<b>Appendixes</b>	
A. Scope and Methodology	7
B. Prior Coverage	8
C. Glossary	9
D. Matrix of Information Assurance Weaknesses Reported From August 1, 2006, Through July 31, 2007	12
E. Audit Reports Issued From August 1, 2006, Through July 31, 2007, Identifying Information Assurance Weaknesses	14
F. Audit Reports From Prior Information Assurance Summary Reports With Unresolved Recommendations	17
G. Report Distribution	21

---

## Background

This report summarizes information assurance (IA) weaknesses that the Government Accountability Office (GAO) and the DoD audit community—the DoD Office of Inspector General (OIG), the Army Audit Agency, the Naval Audit Service, and the Air Force Audit Agency—identified in reports between August 1, 2006, and July 31, 2007. This report is the ninth annual IA summary the DoD OIG has issued since January 1999. The nine IA reports summarize 405 reports on IA weaknesses.

This report supports the DoD OIG response to section 3545 of 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 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.

**Privacy Act of 1974.** The intent of the Privacy Act of 1974, section 552a (as amended), Title 5, United States Code, is to require Federal agencies to protect individuals against unwarranted invasions of their privacy by limiting the collection, maintenance, use, and disclosure of personal information about them. The Act requires that Federal agencies establish information practices that restrict disclosure of personally identifiable records and grants individuals increased access to agency records maintained on them. The E-Government Act of 2002 additionally requires that Federal agencies protect the collection of personal information in Federal government information systems by conducting Privacy Impact Assessments. A Privacy Impact Assessment is an analysis of how personal information is collected, stored, shared, and managed in Federal information technology systems.

**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 comply 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 that standards and guidelines for Federal information systems be based on standards and guidelines developed by the National Institute of Standards and Technology. FISMA permits agencies to develop and use their own IA standards as long as they 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, part of the U.S. Department of Commerce, developed a series of

---

standards and guidelines to provide IA for operations and assets of Federal agencies. 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.

**DoD Information Assurance Guidance.** DoD IA guidance includes:

- DoD Instruction 5200.40, “DoD Information Technology Security Certification and Accreditation Process (DITSCAP),” December 30, 1997, which establishes policy, assigns responsibilities, and prescribes procedures for the certification and accreditation of information technology.
- DoD Directive 5400.11, “DoD Privacy Program,” May 8, 2007, which establishes policy for the respect and protection of an individual’s personal information and fundamental right to privacy.
- 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 issued annually since 1999. The overall objective was to summarize reports by GAO and the DoD audit community between August 1, 2006, and July 31, 2007. 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, 2006, and July 31, 2007, GAO and the DoD audit community issued 36 reports addressing a wide range of IA weaknesses that persist throughout DoD systems and networks.\* This report summarizes those reports.

If the IA weaknesses 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 undermine mission effectiveness.

## **Reports on Information Assurance Weaknesses**

The weaknesses identified in reports by GAO and the DoD audit community were defined by FISMA, DoD Instruction 5200.40, DoD Directive 5400.11, DoD Instruction 8500.2, or DoD Directive 8570.1. The table on the next page shows the number of GAO and DoD audit community reports, by agency, that identify weaknesses in IA areas. See Appendix C for a glossary of specialized terms.

---

\* DoD OIG reported similar IA weaknesses in eight previous IA summary reports.

**Audit Reports Identifying Information Assurance Weaknesses**  
(August 1, 2006, through July 31, 2007)

<u>IA Areas</u>	<u>GAO</u>	<u>DoD OIG</u>	<u>Military Departments</u>	<u>Total</u>
Access Controls	0	7	8	15
Certification and Accreditation	0	6	1	7
Configuration Management	0	5	2	7
Contingency Plans	0	3	4	7
Continuity of Operations Plans	0	4	3	7
Federal Information Systems				
Inventory Reporting	0	2	0	2
Incident Handling	0	1	0	1
Personnel Security	0	0	1	1
Physical Security	0	4	1	5
Plans of Action and Milestones	0	1	0	1
Privacy Act Information	0	1	9	10
Risk, Threat, and Vulnerability				
Assessments	0	1	1	2
Security Awareness, Training, and Education	0	4	4	8
Security Policies and Procedures/ Management Oversight	1	9	23	33

## Types of Weaknesses

Reports issued during the reporting period most frequently cited weaknesses in the following IA areas: access controls; Privacy Act information; security awareness, training, and education; and security policies and procedures. See Appendix D for a matrix of the specific IA weaknesses 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 to authorized users, programs, processes, or other systems. The DoD audit community reported weaknesses related to access controls in 15 reports. The weaknesses 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;
- actions allowed by the systems, including access to FOUO, Privacy Act, and protected health information by users without appropriate rights and permissions;
- separation of duties; and
- development and implementation of the required audit trail for recording changes in user access and permissions.

---

**Privacy Act Information.** Agencies are required to limit the collection, maintenance, use, and disclosure of privacy information on individuals. The DoD audit community identified weaknesses related to Privacy Act information in 10 reports. The reports identified weaknesses related to:

- disposal of documents containing personal protected information;
- timely and uniformly implementing privacy program policy; and
- meeting Privacy Impact Assessment requirements of the E-Government Act of 2002.

In response to DoD OIG Report No. D-2007-099, “DoD Privacy Program and Privacy Impact Assessments,” the Assistant Secretary of Defense for Networks and Information Integration/Chief Information Officer has agreed to implement measures that will enhance protection of all personal protected information in DoD information technology systems. The Navy’s Chief Information Officer has acknowledged the ever-increasing threats to personal identification information and taken actions to reduce threats and increase the awareness of Navy personnel. The DoD Senior Privacy Official is waiting until the DoD Privacy Office compiles the results of a Component Privacy Survey before taking action to correct deficiencies in the DoD Privacy Program.

**Security Awareness, Training, and Education.** The reports identified weaknesses in the area of training for personnel responsible for information security and the administration of training. The DoD audit community reported weaknesses relating to security awareness, training, and education in eight issued reports.

**Security Policies and Procedures.** The audit reports identified weaknesses in security policies and procedures. GAO and the DoD audit community reported weaknesses relating to security policies and procedures in 33 issued reports.

The eight previous IA annual reports summarized 369 reports on IA weaknesses throughout DoD. Of those 369 reports, 40 reports had unresolved recommendations, meaning management had not corrected agreed-upon IA weaknesses within 12 months of the report issue date. 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 management of security programs was inadequate and 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 unauthorized access to information or information systems and their consequent loss, misuse, or modification.

---

## Appendix A. Scope and Methodology

This report summarizes the DoD IA weaknesses identified in 36 reports that GAO and the DoD audit community issued from August 1, 2006, through July 31, 2007. To prepare this summary, the OIG audit team reviewed the Web sites of GAO and each component audit organization, as well as requested reports discussing IA weaknesses from each such organization. The OIG audit team also reviewed prior IA summary reports and, 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 February through August 2007.

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

---

## Appendix B. Prior Coverage

DoD OIG has issued eight information security summary reports. Unrestricted DoD OIG reports can be accessed at <http://www.dodig.osd.mil/audit/reports>. 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-2006-110, "Summary of Information Assurance Weaknesses Found in Audit Reports Issued from August 1, 2005, through July 31, 2006," September 14, 2006

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 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.

**Privacy Act Information** – Privacy Act information is personal information about an individual that links, relates, or is unique to or identifies or describes him or her, such as social security number; age; military rank; civilian grade; marital status; race; salary; home or office phone numbers; and other demographic, biometric, personnel, medical, and financial information. This information is also referred to as personally identifiable information, or that which can be used to distinguish or trace an individual's identity.

**Risk Assessment** – Risk assessment is an analysis of threats to and vulnerabilities of information systems and the potential impact resulting from 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, 2006, Through July 31, 2007

Agency Report No.	Access Controls	Certification and Accreditation	Configuration Management	Contingency Plan	Continuity of Operations Plans	Federal Information Systems Inventory Reporting	Incident Handling	Personnel Security	Physical Security	Plan of Actions and Milestones	Privacy Act Information	Risk, Threat, and Vulnerability Assessment	Security Awareness, Training, Education	Security Policies and Procedures/Management Oversight
<b>Government Accountability Office</b>														
GAO-07-65														X
<b>Office of Inspector General of the DoD</b>														
D-2007-101	X	X												
D-2007-099	X										X		X	X
D-2007-096	X		X						X			X		X
D-2007-089	X	X	X	X	X	X				X				X
D-2007-082	X	X	X	X			X		X				X	X
D-2007-040	X		X	X	X				X					X
D-2007-039		X				X							X	
D-2007-031					X									X
D-2007-025		X												X
D-2007-006					X									X
D-2006-107	X	X	X						X				X	X
<b>Army Audit Agency</b>														
A-2006-0199-FFI														X
A-2006-0181-FFI														X
A-2006-0180-FFI														X
A-2006-0179-FFI														X

Agency Report No.	Access Controls	Certification and Accreditation	Configuration Management	Contingency Plan	Continuity of Operations Plans	Federal Information Systems Inventory Reporting	Incident Handling	Personnel Security	Physical Security	Plan of Actions and Milestones	Privacy Act Information	Risk, Threat, and Vulnerability Assessment	Security Awareness, Training, Education	Security Policies and Procedures/ Management Oversight
<b>Naval Audit Service</b>														
N2007-0036											X			X
N2007-0035											X			X
N2007-0025											X			X
N2007-0018											X			X
N2007-0017				X	X									X
N2007-0016				X	X									X
N2007-0014											X			X
N2007-0012											X			X
N2007-0004											X			X
N2006-0048											X			X
N2006-0045											X			X
<b>Air Force Audit Agency</b>														
F2007-0005-FB2000	X													X
F2007-0004-FB2000	X	X		X										
F2007-0006-FB4000	X			X										X
F2007-0004-FB4000	X								X				X	X
F2007-0001-FB4000													X	X
F2007-0001-FB2000	X				X									X
F2006-0011-FB2000	X		X									X		X
F2006-0009-FB2000	X		X										X	X
F2006-0008-FB4000	X							X					X	X
<b>Total</b>	<b>15</b>	<b>7</b>	<b>7</b>	<b>7</b>	<b>7</b>	<b>2</b>	<b>1</b>	<b>1</b>	<b>5</b>	<b>1</b>	<b>10</b>	<b>2</b>	<b>8</b>	<b>33</b>

---

## **Appendix E. Audit Reports Issued From August 1, 2006, Through July 31, 2007, Identifying Information Assurance Weaknesses**

### **GAO**

GAO Report No. GAO-07-65, "Information Security: Agencies Need to Develop and Implement Adequate Policies for Periodic Testing," October 20, 2006

### **DoD IG**

DoD IG Report No. D-2007-099, "Report on Audit of Privacy Program and Privacy Impact Assessments," June 13, 2007

DoD IG Report No. D-2007-101, "DFAS Corporate Database/DFAS Corporate Warehouse Compliance with the Defense Business Transformation Certification Criteria," May 18, 2007

DoD IG Report No. D-2007-096, "Information Assurance Controls for the Defense Civilian Pay System (FOUO)," May 14, 2007

DoD IG Report No. D-2007-089, "Selected Controls for Information Security of the U.S. Transportation Command's Integrated Computerized Deployment System (FOUO)," April 30, 2007

DoD IG Report No. D-2007-082, "Defense Information Systems Agency Controls over the Center for Computing Services," April 9, 2007

DoD IG Report No. D-2007-040, "The General and Application Controls over the Financial Management System at the Military Sealift Command," January 2, 2007

DoD IG Report No. D-2007-039, "Audit of Information Assurance of Missile Defense Agency Information Systems (FOUO)," December 21, 2006

DoD IG Report No. D-2007-031, "The Effects of Hurricane Katrina on the Defense Information Systems Agency Continuity of Operations and Test Facility," December 12, 2006

DoD IG Report No. D-2007-025, "Acquisition of the Pacific Mobile Emergency Radio System (FOUO)," November 22, 2006

DoD IG Report No. D-2007-006, "Hurricane Katrina Disaster Recovery Efforts Related to Army Information Technology Resources," October 19, 2006

---

DoD IG Report No. D-2006-107, "Defense Departmental Reporting System and Related Financial Statement Compilation Process Controls Placed in Operation and Tests of Operating Effectiveness for the Period October 1, 2004, through March 31, 2005 (FOUO)," August 18, 2006

## **Army Audit Agency**

Army Audit Agency Report No. A-2006-0199-FFI, "Installation Campus Area Network Connectivity - Terrestrial-Based Connections," September 29, 2006

Army Audit Agency Report No. A-2006-0181-FFI, "Installation Campus Area Network Connectivity - Wireless Networks (U.S. Army Garrison, Aberdeen Proving Ground, Maryland)," September 28, 2006

Army Audit Agency Report No. A-2006-0180-FFI, "Installation Campus Area Network Connectivity - Wireless Networks (U.S. Army Garrison, Fort Huachuca, Arizona)," September 28, 2006

Army Audit Agency Report No. A-2006-0179-FFI, "Installation Campus Area Network Connectivity - Wireless Networks (U.S. Army Garrison, Fort Gordon, Georgia)," September 15, 2006

## **Naval Audit Service**

Naval Audit Service Report No. N2007-0036, "Disposal of Protected Personal Information at Naval Support Activity Mid-South, Millington, TN (FOUO)," May 25, 2007

Naval Audit Service Report No. N2007-0035, "Disposal of Protected Personal Information at Naval Station Norfolk and Naval Amphibious Base Little Creek, Norfolk, VA (FOUO)," May 25, 2007

Naval Audit Service Report No. N2007-0025, "Disposal of Protected Personal Information at Naval Medical Center, VA," April 12, 2007

Naval Audit Service Report No. N2007-0018, "Disposal of Protected Personal Information at Naval District Washington, DC (FOUO)," March 1, 2007

Naval Audit Service Report No. N2007-0017, "Ordnance Information System (FOUO)," February 28, 2007

Naval Audit Service Report No. N2007-0016, "Information Systems Restoration and Data Recovery Related to Hurricane Katrina (FOUO)," February 23, 2007

Naval Audit Service Report No. N2007-0014, "Disposal of Protected Personal Information at Marine Corps Base Camp Pendleton, CA (FOUO)," February 15, 2007

---

Naval Audit Service Report No. N2007-0012, "Disposal of Protected Personal Information at Naval Station San Diego, CA (FOUO)," February 2, 2007

Naval Audit Service Report No. N2007-0004, "Management of Privacy Act Information at Naval District Washington (FOUO)," November 21, 2006

Naval Audit Service Report No. N2006-0048, "Disposal of Protected Personal Information at Naval Station Great Lakes, IL," September 27, 2006

Naval Audit Service Report No. N2006-0045, "Disposal of Protected Personal Information at Naval Station Pensacola, FL (FOUO)," September 13, 2006

## **Air Force Audit Agency**

Air Force Audit Agency Report No. F2007-0005-FB2000, "Standard Base Supply System Controls," July 13, 2007

Air Force Audit Agency Report No. F2007-0004-FB2000, "Reliability, Availability, Maintainability Support System for Electronic Combat Pods System Controls," May 25, 2007

Air Force Audit Agency Report No. F2007-0006-FB4000, "Shared Network Storage Management (FOUO)," April 27, 2007

Air Force Audit Agency Report No. F2007-0004-FB4000, "Security of Remote Computer Devices (FOUO)," March 13, 2007

Air Force Audit Agency Report No. F2007-0001-FB4000, "Selected Aspects of Computer Network Intrusion Detection (FOUO)," December 12, 2006

Air Force Audit Agency Report No. F2007-0001-FB2000, "Military Personnel Data System Controls," November 20, 2006

Air Force Audit Agency Report No. F2006-0011-FB2000, "Air Force Equipment Management System Controls," September 25, 2006

Air Force Audit Agency Report No. F2006-0008-FB4000, "Follow-Up Audit, Controls Over Access to Air Force Networks and Systems (FOUO)," September 11, 2006

Air Force Audit Agency Report No. F2006-0009-FB2000, "Contract Writing System Controls," August 3, 2006

---

## **Appendix F. Audit Reports From Prior Information Assurance Summary Reports With Unresolved Recommendations**

IA weaknesses continue to exist throughout DoD. Of the 369 reports included in 8 prior IA summary reports, 40 had unresolved recommendations; management had not corrected agreed-upon IA weaknesses within 12 months of the report issue date. The list of reports with unresolved recommendations was compiled based on information GAO and the DoD audit community provided in July 2007 and may be incomplete because of the extent of information maintained in their respective follow-up systems.

### **GAO**

GAO Report No. GAO-06-31, "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-2006-084, "Information Assurance of Commercially Managed Collaboration Services for the Global Information Grid (FOUO)," May 17, 2006

DoD IG Report No. D-2006-079, "Review of the Information Security Operational Controls of the Defense Logistics 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 3, 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 Agreement," February 23, 2006

DoD IG Report No. D-2006-046, "Technical Report on the Defense Property Accountability System (FOUO)," 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-2006-030, "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

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-2005-033, "Implementation of Interoperability and Information Assurance Policies for Acquisition of Navy Systems," February 2, 2005

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-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

## **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. N2003-0012, "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. 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. F2005-0010-FB2000, "System Controls for Financial Inventory Accounting and Billing System," September 20, 2005

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. 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  
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, Business Transformation Agency  
Chief Information Officer, Defense Advanced Research Projects Agency  
Chief Information Officer, Defense Commissary Agency  
Chief Information Officer, Defense Contract Audit Agency  
Chief Information Officer, Defense Contract Management Agency  
Chief Information Officer, Defense Finance and Accounting Service  
Chief Information Officer, Defense Information Systems Agency  
Chief Information Officer, Defense Logistics Agency  
Chief Information Officer, Defense Security Cooperation Agency  
Chief Information Officer, Defense Security Service  
Chief Information Officer, Defense Technical Information Center  
Chief Information Officer, Defense Technology Security Administration  
Chief Information Officer, Defense Threat Reduction Agency  
Chief Information Officer, DoD Education Activity  
Chief Information Officer, DoD Human Resources Activity  
Chief Information Officer, DoD Inspector General  
Chief Information Officer, DoD Test Resource Management Center  
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 Homeland Security and Governmental Affairs

House Committee on Appropriations

House Subcommittee on Defense, Committee on Appropriations

House Committee on Armed Services

House Committee on Oversight and Government Reform

House Subcommittee on Government Management, Organization, and Procurement,

Committee on Oversight and Government Reform

House Subcommittee on National Security and Foreign Affairs,

Committee on Oversight and 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  
Donald A. Bloomer  
Robert R. Johnson  
Gloria A. Young  
Cory M. James  
Allison Tarmann



# Inspector General Department of Defense

