Report No. D-2011-114 September 30, 2011

Inspector General
United States Department of Defense

Summary of Information Assurance Weaknesses as Reported by Audit Reports Issued From August 1, 2010, Through July 31, 2011

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 Audits

To suggest or request audits, contact the Office of the Deputy Inspector General for Auditing by phone (703) 604-9142 (DSN 664-9142), by fax (703) 604-8932, or by mail:

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

Acronyms and Abbreviations

DON	Department of the Navy
FISMA	Federal Information Security Management Act
IA	Information Assurance
OMB	Office of Management and Budget
PII	Personally Identifiable Information
SSN	Social Security Number

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

September 30, 2011

MEMORANDUM FOR ASSISTANT SECRETARY OF DEFENSE FOR NETWORKS AND INFORMATION INTEGRATION/DOD CHIEF INFORMATION OFFICER
ASSISTANT SECRETARY OF THE AIR FORCE (FINANCIAL MANAGEMENT AND COMPTROLLER)
NAVAL INSPECTOR GENERAL
AUDITOR GENERAL, DEPARTMENT OF THE ARMY

SUBJECT: Summary of Information Assurance Weaknesses as Reported by Audit Reports Issued From August 1, 2010, Through July 31, 2011 (Report No. D-2011-114)

We are providing this summary report for your information and use. This report is a compilation of all audit reports issued during the given period that contained findings describing weaknesses in the Department's information assurance and information security arena. This report contains no recommendations for action, however, it does identify audit reports, previously issued, that contain open recommendations. The report concludes that proper information assurance measures are essential to protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation.

This summary report serves as a reference document to support the Department of Defense Office of Inspector General's response to the requirements of Public Law 107-347, Title III, "Federal Information Security Management Act (FISMA)," section 3545, December 17, 2002. We did not issue a draft report and no written response is required.

We appreciate the courtesies extended to the staff. Please direct questions to me at (703) 604-8866 (DSN 664-8866).

Alice F. Carey
Assistant Inspector General
Readiness, Operations, and Support

Results in Brief: Summary of Information Assurance Weaknesses as Reported by Audit Reports Issued From August 1, 2010, Through July 31, 2011

What We Did

We researched, obtained, and summarized all audit reports, issued between August 1, 2010, and July 31, 2011, that contained findings on information assurance weaknesses in DoD. The reports were issued by the Department of Defense Office of Inspector General (DoD OIG), Army Audit Agency, Naval Audit Service, Air Force Audit Agency, and the Government Accountability Office. This summary report is for information purposes only and supports the DoD OIG's response to the requirements of Public Law 107-347, Title III, "Federal Information Security Management Act (FISMA)," section 3545, December 17, 2002.

We included five additional information assurance categories in this year's report, as identified by the FY 2011 Inspector General Federal Information Security Management Act reporting requirements. This report is the 13th information assurance summary report issued by the DoD OIG since January 1999.

What We Found

Between August 1, 2010, and July 31, 2011, the DoD OIG, Army Audit Agency, Naval Audit Service, Air Force Audit Agency, and Government Accountability Office issued 42 reports addressing a wide range of information assurance weaknesses that persist throughout DoD systems and networks. The top four weaknesses identified were security policies and procedures/management oversight; security awareness, training, and education; access controls; and Privacy Act information.

The information security weaknesses in DoD continued to provide unauthorized personnel the opportunity to modify, steal, inappropriately disclose, and destroy sensitive DoD data. Persistent weaknesses in information security policies and practices continued to threaten the availability, integrity, authentication, confidentiality, and non-repudiation of critical information and information systems used to support operations, assets, and personnel.

What We Recommend

Recommendations are made in the individual audit reports that are identified in this Summary Report. Therefore, this report contains no new recommendations and is provided for information purposes only.

Management Comments

We did not issue a draft report because this report consolidates audit findings from audit reports that were published in the last year. No written response to this report is required.

Table of Contents

Introduction

Objectives

The purpose of this report is to provide a reference document that identifies all audit reports that contained findings outlining information assurance weaknesses in DoD. The overall objective was to summarize the information assurance (IA) weaknesses identified in reports and testimonies issued by the DoD audit community and the Government Accountability Office (GAO) between August 1, 2010, and July 31, 2011. This summary report supports the Department of Defense Office of Inspector General's (DoD OIG) response to the requirements of Public Law 107-347, Title III, "Federal Information Security Management Act (FISMA)," section 3545, December 17, 2002. See Appendix A for a discussion of the scope and methodology and Appendix B for prior coverage related to the objective.

Background

This report is the 13th annual IA summary the DoD OIG has issued since January 1999. Collectively, the 12 previous reports summarized 535 reports and testimonies on IA weaknesses found in DoD. Civil service and uniformed officers who develop, operate, or manage DoD information technology resources should read this report to be aware of potential IA challenges in both their own and shared DoD information technology environments.

Additional Information Assurance Categories

In 2010, the Office of Management and Budget (OMB) mandated the Department of Homeland Security provide guidance and operational oversight for FISMA reporting. Specifically, the Department of Homeland Security is responsible for the development and issuance of FISMA security metrics for Federal agencies. The Department of Homeland Security recently issued the FY 2011 Inspector General FISMA Reporting requirements. To remain consistent with the updated requirements, this year's IA summary report includes five additional IA categories. The new IA categories are remote access management, identity and access management, continuous monitoring management, contractor systems, and security capital planning. See the glossary for definitions of these categories.

Federal Information Security Management Act of 2002

Federal agencies are required to annually submit a FISMA assessment on questions related to information security management. The annual reports are submitted electronically in CyberScope, an automated, streamlined platform used for secure FISMA reporting for the collection of agency cyber security information.

FISMA provides a comprehensive framework for ensuring the effectiveness of information security controls over information resources that support Federal operations and assets. FISMA requires that each agency develop, document, and implement an agency-wide information security program to provide security 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." Under 40 U.S.C. 11331, standards and guidelines for Federal information systems are to be based on standards and guidelines developed by the National Institute of Standards and Technology. FISMA requires that each agency with an Inspector General appointed under the Inspector General Act of 1978, as amended, perform an independent evaluation of the information security program and practices of that agency to determine effectiveness. The agencies' Inspector General, Chief Information Officer, and Privacy Office all submit a single FISMA assessment report to OMB.

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 information security 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 certification and accreditation, 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.

Privacy Act of 1974 and E-Government Act of 2002

On June 13, 2005, OMB required Federal agencies to begin including information on their privacy programs. At the same time, OMB also discontinued agencies' annual privacy-related submissions under Public Law 107-347, "E-Government Act of 2002," December 17, 2002. OMB's privacy questions relate in part to the Privacy Act of 1974; section 552a, title 5 United States Code; and the E-Government Act of 2002. The intent of the Privacy Act 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 E-Government 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.

DoD Information Assurance Guidance

DoD IA guidance comprises the following documents.

- DoD Directive 5400.11, "DoD Privacy Program," May 8, 2007, establishes policy for the respect and protection of an individual's personal information and fundamental right to privacy.
- DoD Instruction 5400.16, "DoD Privacy Impact Assessment (PIA) Guidance," February 12, 2009, establishes policy and assigns responsibilities for completion and approval of Privacy Impact Assessments.
- DoD Directive 8500.01E, "Information Assurance (IA)," October 24, 2002, Certified Current as of April 23, 2007, establishes policy and assigns responsibility to achieve IA throughout DoD.
- DoD Instruction 8500.2, "Information Assurance (IA) Implementation," February 6, 2003, implements the policy, assigns responsibilities, and prescribes procedures for applying integrated layered protection of DoD information systems and networks as DoD Directive 8500.01E outlines.
- DoD Instruction 8510.01, "DoD Information Assurance Certification and Accreditation Process (DIACAP)," November 28, 2007, establishes a certification and accreditation process.
- DoD Directive 8570.01, "Information Assurance Training, Certification, and Workforce Management," August 15, 2004, Certified Current as of April 23, 2007, establishes policy and assigns responsibility for DoD IA training, certification, and workforce management.
- DoD Policy, "Web Site Administration Policies and Procedures," November 25, 1998, latest correction from January 11, 2002, delineates the policy and assigns responsibility related to establishing, operating, and maintaining unclassified Web sites and other related services.
- Deputy Secretary of Defense Memorandum, "Department of Defense (DoD) Web Site Security Policy Compliance," September 25, 2008, requires Components to ensure that they have processes in place that ensure all information posted to publicly accessible Web sites is reviewed and approved prior to posting.
- Deputy Secretary of Defense Memorandum, "Policy for Department of Defense (DoD) Interactive Internet Activities," June 8, 2007 provides authority and guidance for the use of interactive internet activities, systems accessible via the internet which allows for two-way communications.
- Deputy Secretary of Defense Memorandum, "Web Site Administration," December 7, 1998, provides policy, assigns responsibility, and describes the procedures for establishing, operating, and maintaining DoD unclassified Web sites. To maximize the availability of timely and accurate information to the public, as well as maintaining a secure framework, DoD Components have the responsibility to ensure sound information assurance practices are in place and operating for Web sites.

Results. Information Assurance Weaknesses Continue to Persist Throughout DoD

Between August 1, 2010, and July 31, 2011, the DoD audit community and GAO issued 42 reports addressing a wide range of IA weaknesses that persist throughout DoD systems and networks. This report summarizes the IA weaknesses listed in the reports. The top four weaknesses identified were security policies and procedures/management oversight; security awareness, training, and education; access controls; and Privacy Act information. The information security weaknesses in DoD continued to provide unauthorized personnel the opportunity to modify, steal, inappropriately disclose, and destroy sensitive DoD data. Persistent weaknesses in information security policies and practices identified in this report continued to threaten the availability, integrity, proper authentication, confidentiality, and non-repudiation of critical information and information systems used to support operations, assets, and personnel.

Reports on Information Assurance Weaknesses

The weaknesses identified in reports by the DoD audit community and GAO were defined by guidance described in FISMA, OMB memoranda, National Institute of Standards and Technology standards and guidelines, and DoD guidelines. On June 1, 2011, for the first time, the Department of Homeland Security issued the annual FISMA Reporting requirements. The following table shows the number of information assurance weaknesses that the 42 reports identified. See the glossary for specialized terms.

Table. Information Assurance Weaknesses Reported From August 1, 2010, Through July 31, 2011

IA Areas	GAO	DoD OIG	Military Departments	Total
Access Controls	0	3	9	12
Certification and Accreditation	1	3	1	5
Configuration Management	1	3	1	5
Contingency Plans	0	0	1	1
Continuity of Operations Plans	0	2	0	2
Continuous Monitoring Management	0	3	1	4
Contractor Systems	0	0	0	0
Cyber Security	0	0	1	1
Identity and Access Management	1	4	2	7
Information Systems Inventory Reporting	1	0	1	2
Incident Handling	0	1	1	2
Interoperability	1	0	0	1
Personnel Security	1	0	1	2
Physical Security	0	1	2	3
Plans of Action and Milestones	6	2	1	9
Privacy Act Information	0	1	9	10
Remote Access Management	0	0	0	0
Risk, Threat, and Vulnerability Assessment	2	2	2	6
Security Capital Planning	2	0	0	2
Security Awareness, Training, and Education	1	1	11	13
Security Policies & Procedures/Management Oversight	8	4	26	38

Types of Information Assurance Weaknesses

Reports issued during the reporting period most frequently cited weaknesses in the IA areas of security policies and procedures/management oversight; security awareness, training, and education; access controls; and Privacy Act information. See Appendix C for a matrix of reports listed by their specific IA weaknesses and Appendix D for a list of reports summarized in this report.

Security Policies and Procedures/Management Oversight

The category of security policies and procedures/management oversight entails an organization's policies for operation and the procedures necessary to implement the

policies. The DoD audit community and GAO reported weaknesses related to security policies and procedures/management oversight in 38 reports. For example, Air Force Audit Agency Report No. F2010-0008-FC4000, "Temporary Duty Travel Management," September 13, 2010, found that travel management personnel did not properly segregate duties among accountable officials and allowed personnel multiple levels of access. In addition, travel management personnel did not always properly appoint or train accountable officials. Further, travel management personnel improperly granted contractor personnel approval authority in the Defense Travel System. These conditions existed because Air Force guidance did not include a requirement to periodically review accountable official permission levels to ensure proper segregation of duties, did not adequately address accountable official management, and did not adequately address the Defense Travel System rights and permission levels for contractor personnel. As a result, accountable officials with multiple permission levels inappropriately approved 4,775 vouchers, valued at over $6 million, accountable officials did not receive required training necessary to help ensure proper management of Air Force travel funds, and contractor personnel had permission to approve and manage Air Force funds. The report recommended that the Air Force Defense Travel System Financial Management Guide should define proper segregation of duties and include examples of jobs and permission levels that must be segregated; Air Force Lead Defense Travel Agents should verify all accountable officials have training certificates and signed DD Forms 577 on file; and revise the Air Force Defense Travel System Financial Management Guide to prohibit assigning contractor personnel to accountable-level positions. According to the report, management officials agreed with the audit issues in this report, and actions taken were responsive.

As a result, accountable officials with multiple permission levels inappropriately approved 4,775 vouchers, valued at over $6 million…

Security Awareness, Training, and Education

Security awareness, training, and education are defined as:

- 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 is teaching individuals the knowledge and skills that will enable them to perform their jobs more effectively.
- Education focuses on developing the ability and vision to perform complex, multidisciplinary activities and the skills needed to further the information technology security profession. Education activities include research and development to keep pace with changing technologies.

The DoD audit community and GAO reported weaknesses related to security awareness, training, and education in 13 reports. For example, DoD Inspector General (IG) Report No. D-2011-020, "DoD Controls Over Information Placed on Publicly Accessible Web Sites Require Better Execution," November 29, 2010, found that DoD organizations did not ensure all DoD Web site administrators received the required Web operations security training. Web operations security training is important to ensure the proper control and

proper posting of sensitive information to DoD public Web sites. Of 470 Web site administrators reviewed, 452 had not received required operations security training. This occurred because DOD organizations did not execute enforcement actions for noncompliance with Web site policies and procedures, and Components did not fully disseminate required policies and procedures governing publicly accessible Web sites. As a result, DoD is at a higher risk of posting sensitive information to DoD public Web sites. The report recommended the Assistant Secretary of Defense for Networks and Information Integration/DoD Chief Information Officer develop and issue a DoD Instruction that requires heads of DoD Components to annually assess and document DoD Internet services and use of Internet-based capabilities. This recommendation will allow for compliance with applicable policies and procedures, to include that all Web site administrators have received the proper Web operations security training. According to the report, management agreed with the recommendation, stating that the annual policy compliance assessment and corrective action will be mandated in the impending DoD Instruction 8430.aa.

Of 470 Web site administrators reviewed, 452 had not received required operations security training.

Access Controls

Access controls limit information system resources to authorized users, programs, processes, or other systems. The DoD audit community and GAO reported weaknesses related to access controls in 12 reports. For example, Air Force Audit Agency Report No. F2011-0002-FB2000, "Enterprise Environmental Safety and Occupational Health – Management Information System Application Controls," February 15, 2011, found that Enterprise Environmental Safety and Occupational Health – Management Information System program personnel need to strengthen implementation of general controls. Program and functional personnel did not maintain effective control over system access. Specifically, Enterprise Environmental Safety and Occupational Health – Management Information System points of contact incorrectly established user accounts without the required approvals, did not deactivate all invalid user accounts, and provided some users with excessive and unauthorized account privileges. This condition occurred because program and functional personnel bulk loaded user accounts when migrating from the former Air Force Environmental Management Information System to Enterprise Environmental Safety and Occupational Health – Management Information System without verifying user access requirements. As a result, the program could provide unauthorized users access to enter improper transactions into the system. The report recommended Enterprise Environmental Safety and Occupational Health – Management Information System points of contact conduct a one-time reconciliation and correction of all current accounts to user access forms and duty requirements. According to the report, management concurred and has taken corrective actions.

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 (SSN); age; military rank; civilian grade; marital status; race; salary; home or office phone number; and other demographic, biometric, personal, medical, and financial information.

This information is also referred to as personally identifiable information (PII), or information which can be used to distinguish or trace an individual's identity. The DoD audit community and GAO reported weaknesses related to Privacy Act information in 10 reports. For example, Naval Audit Report No. N2011-0020, "Unnecessary Collection of Personally Identifiable Information in the Department of the Navy," January 28, 2011, found that the Department of the Navy (DON) was unable to ensure only necessary PII was being collected. Further, SSNs were printed or displayed on systems and forms without being masked or condensed, as required. These conditions occurred because:

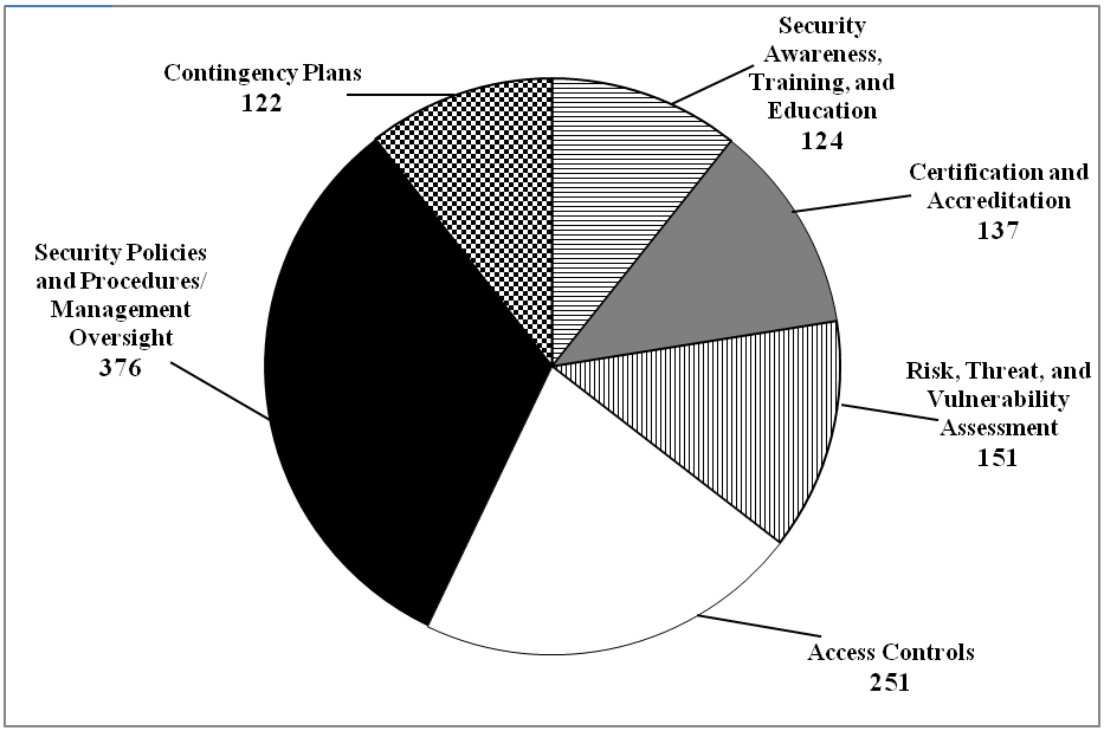
- There was no overall DON guidance to reduce the collection of SSNs;
- The DoD Information Technology Portfolio Registry-DON database was incomplete;
- DON could not identify all DON forms to reduce SSN collection; and
- There was no DON requirement limiting exposure of SSNs.

As a result, DON does not have assurance of the proper collection and use of SSNs and PII across the Department and puts the DON at a higher risk of identity theft. The report recommended the DON Chief Information Officer issue guidance to reduce the collection and limit the exposure of SSNs and other PII. According to the report, management agreed with the recommendations and is taking corrective action.

Persistent Information Assurance Weaknesses Reported in the Past 12 Years

The reports summarized in this report show that there continued to be a wide range of IA weaknesses throughout DoD. The DoD audit community and GAO have issued 535 audit reports and testimonies over the last 12 years (see Appendix E for details), which have frequently reported similar, if not identical, IA weaknesses. Security policies and procedures/management oversight issues were identified in 376 reports; inadequate access controls were identified in 251 reports; concerns related to risk, threat, and vulnerability assessments were identified in 151 reports; certification and accreditation were issues identified in 137 reports; security awareness, training, and education weaknesses were identified in 124 reports; and inadequate contingency plans were identified in 122 reports (see Appendix E). The figure below illustrates the number of reports that identified the above cited IA weaknesses.

Figure. Reports Identifying Information Assurance Weaknesses From 1999 Through 2010



Unresolved Recommendations

Since August 1, 2010, management had taken action to resolve IA-related recommendations made in 49 of the previous reports. There were still 45 reports with unresolved recommendations that required management action. Prompt action to correct the outstanding IA weaknesses is necessary to mitigate ongoing vulnerabilities in the DoD IA program. See Appendix F for a listing of the 45 reports with unresolved recommendations relating to IA weaknesses.

Summary

Many of the IA weaknesses reported occurred because management of security programs was inadequate and security policies and procedures were not in place. Without effective management oversight, DoD cannot be assured that systems are accurately reported and maintained, information systems contain reliable data, and personnel are properly trained in security policies and procedures. Effective management oversight will remedy persistent IA weaknesses, thereby increasing assurance that DoD information systems maintain an appropriate level of confidentiality, integrity, authentication, and availability.

Appendix A. Scope and Methodology

This report summarizes the DoD IA weaknesses identified in 42 reports that GAO and the DoD audit community issued from August 1, 2010, through July 31, 2011. To prepare this summary, the DoD OIG audit team reviewed the Web sites of GAO and each DoD Component audit organization and requested reports discussing IA weaknesses from each organization. The DoD OIG audit team also reviewed prior IA summary reports and, with the assistance of the DoD audit community and GAO follow-up organizations, summarized reports with unresolved recommendations on IA weaknesses.

This summary report does not make recommendations because recommendations have already been made in the summarized reports. We did not follow generally accepted government auditing standards in conducting this project because it is a summary project. 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 requirements of Public Law 107-347, Title III, "Federal Information Security Management Act (FISMA)," section 3545, December 17, 2002. We conducted this summary work from February 2011 through September 2011.

Use of Computer-Processed Data

We did not use computer-processed data when compiling information for this summary report.

Appendix B. Prior Coverage

During the last 12 years, DoD OIG has issued 12 summary reports detailing IA weaknesses. Unrestricted DoD IG reports can be accessed at http://www.dodig.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 by telephone, (703) 604-9775 (DSN 664-9775), or fax (703) 602-0294.

DoD IG Report No. D-2010-090, "Summary of Information Assurance Weaknesses Identified in Audit Reports Issued From August 1, 2009, Through July 31, 2010," September 30, 2010 **(FOUO)**

DoD IG Report No. D-2009-110, "Summary of Information Assurance Weaknesses Identified in Audit Reports Issued From August 1, 2008, Through July 31, 2009," September 28, 2009 **(FOUO)**

DoD IG Report No. D-2008-125, "Summary of Information Assurance Weaknesses Found in Audit Reports Issued From August 1, 2007, Through July 31, 2008," September 2, 2008

DoD IG Report No. D-2007-123, "Summary of Information Assurance Weaknesses Found in Audit Reports Issued From August 1, 2006, Through July 31, 2007," September 12, 2007

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," September 23, 2005 **(FOUO)**

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

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

DoD IG 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 **(FOUO)**

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

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

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

Appendix C. Matrix of Information Assurance Weaknesses Reported From August 1, 2010, Through July 31, 2011

Agency Report No.	Access Controls	Certification and Accreditation	Configuration Management	Contingency Plans	Continuity of Operations Plans	Continuous Monitoring Management	Contractor Systems	Cyber Security	Identity and Access Management	Information Systems Inventory Reporting	Incident Handling	Interoperability	Personnel Security	Physical Security	Plans of Actions and Milestones	Privacy Act Information	Remote Access Management	Risk, Threat, and Vulnerability Assessment	Security Capital Planning	Security Awareness, Training, Education	Security Policies and Procedures / Management Oversight
Government Accountability Office																					
GAO-10-636																					X
GAO-10-916		X													X						X
GAO-11-148															X			X			
GAO-11-265									X												X
GAO-11-276												X									X
GAO-11-421													X							X	
GAO-11-621			X															X			X
GAO-11-684															X				X		X
GAO-11-75															X				X		X
GAO-11-565										X					X						
GAO-11-566R															X						X

Agency Report No.	Access Controls	Certification and Accreditation	Configuration Management	Contingency Plans	Continuity of Operations Plans	Continuous Monitoring Management	Contractor Systems	Cyber Security	Identity and Access Management	Information Systems Inventory Reporting	Incident Handling	Interoperability	Personnel Security	Physical Security	Plans of Actions and Milestones	Privacy Act Information	Remote Access Management	Risk, Threat, and Vulnerability Assessment	Security Capital Planning	Security Awareness, Training, Education	Security Policies and Procedures / Management Oversight
DoD Inspector General																					
D-2010-074 (FOUO)	X	X	X		X	X			X					X							X
D-2011-020															X	X				X	X
D-2011-064 (FOUO)		X			X				X		X				X			X			X
D-2011-079 (FOUO)	X		X			X			X												
D-2011-089 (FOUO)	X	X	X			X			X									X			X
Army Audit Agency																					
A-2010-0162-FFI	X								X												X
A-2010-0212-FFI	X																				X
A-2011-0100-IET	X																				X
A-2011-0147-IET																				X	X
A-2011-0143-IET															X						X
A-2011-0150-IET																X				X	X

Agency Report No.	Access Controls	Certification and Accreditation	Configuration Management	Contingency Plans	Continuity of Operations Plans	Continuous Monitoring Management	Contractor Systems	Cyber Security	Identity and Access Management	Information Systems Inventory Reporting	Incident Handling	Interoperability	Personnel Security	Physical Security	Plans of Actions and Milestones	Privacy Act Information	Remote Access Management	Risk, Threat, and Vulnerability Assessment	Security Capital Planning	Security Awareness, Training, Education	Security Policies and Procedures / Management Oversight
Naval Audit Service																					
N2010-0046 (FOUO)																					X
N2010-0052 (FOUO)														X		X		X		X	X
N2011-0001 (FOUO)	X																				X
N2011-0017 (FOUO)																					X
N2011-0020 (FOUO)																X					X
N2011-0025 (FOUO)																					X
N2011-0028 (FOUO)																X					X
N2011-0038 (FOUO)																					X
N2011-0040 (FOUO)														X		X				X	X
N2011-0041 (FOUO)																X					X
N2011-0046 (FOUO)																X					X

Agency Report No.	Access Controls	Certification and Accreditation	Configuration Management	Contingency Plans	Continuity of Operations Plans	Continuous Monitoring Management	Contractor Systems	Cyber Security	Identity and Access Management	Information Systems Inventory Reporting	Incident Handling	Interoperability	Personnel Security	Physical Security	Plans of Actions and Milestones	Privacy Act Information	Remote Access Management	Risk, Threat, and Vulnerability Assessment	Security Capital Planning	Security Awareness, Training, Education	Security Policies and Procedures / Management Oversight
Air Force Audit Agency																					
F2010-0005-FC2000										X											X
F2010-0007-FB4000	X																			X	X
F2010-0008-FC4000	X								X							X				X	X
F2011-0001-FB4000		X	X																	X	X
F2011-0002-FB4000	X					X														X	X
F2011-0002-FB2000	X			X																X	X
F2011-0003-FB4000	X															X		X		X	X
F2011-0004-FB4000								X													X
F2011-0006-FB4000											X		X							X	X
Total	**12**	**5**	**5**	**1**	**2**	**4**	**0**	**1**	**7**	**2**	**2**	**1**	**2**	**3**	**9**	**10**	**0**	**6**	**2**	**13**	**38**

Note: Totals do not equal the number of reports and testimonies reviewed because one report may cover several IA weaknesses.

Appendix D. Audit Reports Issued From August 1, 2010, Through July 31, 2011

Unrestricted GAO reports can be accessed over the Internet at http://www.gao.gov. Unrestricted DoD IG reports can be accessed at http://www.dodig.mil/audit/reports. Unrestricted Army reports can be accessed from .mil and gao.gov domains over the Internet at https://www.aaa.army.mil/. Naval Audit Service reports are unavailable over the Internet. Air Force Audit Agency reports can be accessed by certain government users at https://afkm.wpafb.af.mil/ASPs/CoP/OpenCoP.asp?Filter=OO-AD-01-41.

GAO

GAO Report No. GAO-10-636, "Global Positioning System: Challenges in Sustaining and Upgrading Capabilities Persist," September 2010

GAO Report No. GAO-10-916, "Information Security: Progress Made on Harmonizing Policies and Guidance for National Security and Non-National Security Systems," September 2010

GAO Report No. GAO-11-148, "Health Information Technology: DoD Needs to Provide More Information on Risks to Improve Its Program Management," November 2010

GAO Report No. GAO-11-265, "Electronic Health Records: DoD and VA Should Remove Barriers and Improve Efforts to Meet Their Common System Needs," February 2011

GAO Report No. GAO-11-276, "Defense Biometrics: DoD Can Better Conform to Standards and Share Biometric Information with Federal Agencies," March 2011

GAO Report No. GAO-11-421, "Defense Department Cyber Efforts: More Detailed Guidance Needed to Ensure Military Services Develop Appropriate Cyberspace Capabilities," May 2011

GAO Report No. GAO-11-621, "Intelligence, Surveillance, and Reconnaissance: DoD Needs a Strategic, Risk-Based Approach to Enhance Its Maritime Domain Awareness," June 2011

GAO Report No. GAO-11-684, "Department of Defense: Further Actions Needed to Institutionalize Key Business System Modernization Management Controls," June 2011

GAO Report No. GAO-11-75, "Defense Department Cyber Efforts: DoD Faces Challenges In Its Cyber Activities," July 2011

GAO Report No. GAO-11-565, "Data Center Consolidation: Agencies Need to Complete Inventories and Plans to Achieve Expected Savings," July 2011

GAO Report No. GAO-11-566R, "Defense Logistics: Oversight and a Coordinated Strategy Needed to Implement the Army Workload and Performance System," July 14, 2011

DoD IG

DoD IG Report No. D-2010-074, "Information Assurance Controls for the Defense Civilian Pay System for FY 2009," August 2, 2010 **(FOUO)**

DoD IG Report No. D-2011-020, "DoD Controls Over Information Placed on Publicly Accessible Web Sites Require Better Execution," November 29, 2010

DoD IG Report No. D-2011-064, "Audit of the Information Security Controls Over the Marine Corps Total Force System Need Improvement," May 5, 2011 **(FOUO)**

DoD IG Report No. D-2011-079, "Defense Information Systems Agency Controls Placed in Operation and Tests of Operating Effectiveness as of October 1, 2010, Through April 30, 2011," June 30, 2011 **(FOUO)**

DoD IG Report No. D-2011-089, "Reducing Vulnerabilities at the Defense Information Systems Agency Defense Enterprise Computing Centers," July 22, 2011 **(FOUO)**

Army Audit Agency

Army Audit Agency Report No. A-2010-0162-FFI, "Data at Rest, Fort Carson, Colorado," August 11, 2010

Army Audit Agency Report No. A-2010-0212-FFI, "Data at Rest, Chief Information Officer/G-6," September 29, 2010

Army Audit Agency Report No. A-2011-0100-IET, "Data at Rest, Fort Bragg, North Carolina," April 29, 2011

Army Audit Agency Report No. A-2011-0147-IET, "Information Assurance Certification for Contractors," June 23, 2011

Army Audit Agency Report No. A-2011-0143-IET, "Application Migration, Office of the Chief Information Officer/G-6," July 6, 2011

Army Audit Agency Report No. A-2011-0150-IET, "The Army's Use of Social Media, External Official Presence Sites," July 26, 2011

Naval Audit Service

Naval Audit Service Report No. N2010-0046, "Defense Travel System," August 3, 2010 **(FOUO)**

Naval Audit Service Report No. N2010-0052, "Managing Personally Identifiable Information at Selected Commander, Navy Installations Command Activities," September 10, 2010 **(FOUO)**

Naval Audit Service Report No. N2011-0001, "Navy Enterprise Resource Program - Purchase Card Capabilities," October 1, 2010 **(FOUO)**

Naval Audit Service Report No. N2011-0017, "Navy Reserve Southwest Region Annual Training and Active Duty for Training Orders," January 19, 2011 **(FOUO)**

Naval Audit Service Report No. N2011-0020, "Unnecessary Collection of Personally Identifiable Information in the Department of the Navy," January 28, 2011 **(FOUO)**

Naval Audit Service Report No. N2011-0025, "Navy/Marine Corps Intranet Internal Controls Over Computers During Turn-In Process," March 18, 2011 **(FOUO)**

Naval Audit Service Report No. N2011-0028, "Followup of Management of Privacy Act Information at the Navy Recruiting Command," March 31, 2011 **(FOUO)**

Naval Audit Service Report No. N2011-0038, "Controls Over Navy Marine Corps Intranet Contractors and Subcontractors Accessing Department of the Navy Information," May 26, 2011 **(FOUO)**

Naval Audit Service Report No. N2011-0040, "Managing Personally Identifiable Information at Marine Corps Base, Camp Lejeune," June 1, 2011 **(FOUO)**

Naval Audit Service Report No. N2011-0041, "Followup on Management of Privacy Act Information at Naval District Washington," June 15, 2011 **(FOUO)**

Naval Audit Service Report No. N2011-0046, "Followup on Management of Personally Identifiable Information at Marine Corps Recruiting Command," July 29, 2011 **(FOUO)**

Air Force Audit Agency

Air Force Audit Agency Report No. F2010-0005-FC2000, "Nuclear Certification of Aircraft and Test Equipment Software," August 23, 2010

Air Force Audit Agency Report No. F2010-0007-FB4000, "Access Controls For Air and Space Operations Center Networks," August 31, 2010

Air Force Audit Agency Report No. F2010-0008-FC4000, "Temporary Duty Travel Management," September 13, 2010

Air Force Audit Agency Report No. F2011-0001-FB4000, "Voice Over Internet Protocol Implementation," December 20, 2010

Air Force Audit Agency Report No. F2011-0002-FB4000, “Information Assurance Workforce Improvement Program,” January 26, 2011

Air Force Audit Agency Report No. F2011-0002-FB2000, “Enterprise Environmental Safety and Occupational Health – Management Information System Application Controls,” February 15, 2011

Air Force Audit Agency Report No. F2011-0003-FB4000, “Access Controls For Electronic Medical Records,” April 1, 2011

Air Force Audit Agency Report No. F2011-0004-FB4000, “Computer Network Incident Response and Reporting,” April 20, 2011

Air Force Audit Agency Report No. F2011-0006-FB4000, “Privacy Breach Reporting,” July 14, 2011

Appendix E. Matrix of Reports that Identified Key Information Assurance Weaknesses Reported From January 1, 1995, Through July 31, 2010

Year	Number of Reports and Testimonies Reviewed	Security Policies and Procedures / Management Oversight	Access Controls	Risk, Threat, and Vulnerability Assessment	Certification and Accreditation	Security Awareness, Training, Education	Contingency Plans
2010	47	40	28	8	8	7	10
2009	48	29	14	9	3	4	5
2008	21	15	9	5	4	4	2
2007	36	33	15	2	7	8	7
2006	28	12	19	3	12	8	6
2005	46	30	21	17	16	17	19
2004	40	33	19	22	18	12	10
2003	57	13	19	23	19	5	17
2002	57	32	16	10	22	12	17
2001	59	50	21	24	0	10	11
2000	21	0	11	10	6	8	8
1999	75	89	59	18	22	29	10
Total	**535**	**376**	**251**	**151**	**137**	**124**	**122**

Note: The top six IA weaknesses over the previous 12 reporting cycles are discussed in the table above. Totals do not equal the number of reports and testimonies reviewed because one report may cover several IA weaknesses.

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

IA weaknesses continue to exist throughout DoD. Of the 535 reports and testimonies included in 12 prior IA summary reports, 45 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 2011 and may be incomplete because of the extent of information maintained in their respective follow-up systems.

Unrestricted GAO reports can be accessed over the Internet at http://www.gao.gov. Unrestricted DoD IG reports can be accessed at http://www.dodig.mil/audit/reports. Unrestricted Army reports can be accessed from .mil and gao.gov domains over the Internet at https://www.aaa.army.mil/. Naval Audit Service reports are unavailable over the Internet. Air Force Audit Agency reports can be accessed by certain government users at https://afkm.wpafb.af.mil/ASPs/CoP/OpenCoP.asp?Filter=OO-AD-01-41.

GAO

GAO Report No. GAO-07-528, "Information Security: Selected Departments Need to Address Challenges in Implementing Statutory Requirements," August 2007

GAO Report No. GAO-08-922, "DOD Business Systems Modernization: Planned Investment in Navy Program to Create Cashless Shipboard Environment Needs to Be Justified and Better Managed," September 2008

GAO Report No. GAO-09-49, "Defense Management: DOD Can Establish More Guidance for Biometrics Collection and Explore Broader Data Sharing," October 2008

GAO Report No. GAO-09-268, "Electronic Health Records: DOD's and VA's Sharing of Information Could Benefit from Improved Management," January 2009

GAO Report No. GAO-09-586, "DOD Business Systems Modernization: Recent Slowdown in Institutionalizing Key Management Controls Needs to Be Addressed," May 2009

GAO Report No. GAO-09-566, "Information Technology: Federal Agencies Need to Strengthen Investment Board Oversight of Poorly Planned and Performing Projects," June 2009

GAO Report No. GAO-09-775, "Electronic Health Records: DOD and VA Efforts to Achieve Full Interoperability Are Ongoing; Program Office Management Needs Improvement," July 2009

GAO Report No. GAO-09-546, “Information Security: Agencies Continue to Report Progress, but Need to Mitigate Persistent Weaknesses,” July 2009

GAO Report No. GAO-09-740R, “Defense Critical Infrastructure: Actions Needed to Improve the Consistency, Reliability, and Usefulness of DOD’s Tier 1 Task Critical Asset List,” July 2009

GAO Report No. GAO-09-617, “Information Security: Concerted Effort Needed to Improve Federal Performance Measures,” September 2009

GAO Report No. GAO-09-888, “Information Technology: DOD Needs to Strengthen Management of Its Statutorily Mandated Software and System Process Improvement Efforts,” September 2009

GAO Report No. GAO-10-148, “Critical Infrastructure Protection: OMB Leadership Needed to Strengthen Agency Planning Efforts to Protect Federal Cyber Assets,” October 2009

GAO Report No. GAO-10-202, “Information Security: Agencies Need to Implement Federal Desktop Core Configuration Requirements,” March 2010

GAO Report No. GAO-10-663, “Scope and Content of DOD’s Congressional Report and Executive Oversight of Investments Need to Improve,” May 2010

DoD IG

DoD IG Report No. D-2005-0054, “Audit of the DOD Information Technology Security Certification and Accreditation Process,” April 28, 2005 **(FOUO)**

DoD IG Report No. D-2009-0097, “Data Migration Strategy and Information Assurance for the Business Enterprise Information Services,” July 30, 2009

DoD IG Report No. D-2009-0086, “Controls Over the Contractor Common Access Card Life Cycle in the Republic of Korea,” June 9, 2009

DoD IG Report No. D-2010-0058, “Selected Controls for Information Assurance at the Defense Threat Reduction Agency,” May 14, 2010

Army Audit Agency

Army Audit Report No. A-2008-0186-FFI, “Installation Campus Area Network Connectivity - Wireless Network and Devices,” July 8, 2008

Army Audit Report No. A-2009-0037-FFI, “Information Technology Contingency Plans - Chief Information Officer/G-6,” January 26, 2009

Army Audit Report No. A-2010-0046-FFI, "Army Networthiness Certification Program," February 2, 2010

Naval Audit Service

Naval Audit Service Report No. N-2007-0017, "Ordinance Information System," February 28, 2007 **(FOUO)**

Naval Audit Service Report No. N-2008-0023, "Information Security Within the Marine Corps," February 20, 2008 **(FOUO)**

Naval Audit Service Report No. N-2009-0027, "Processing of Computers and Hard Drives During the Navy Marine Corps Intranet (NMCI) Computer Disposal Process," April 28, 2009 **(FOUO)**

Naval Audit Service Report No. N2010-005, "Information Security for Research, Development, Test, and Evaluation and Education Legacy Networks," January 7, 2010 **(FOUO)**

Naval Audit Service Report No. N2010-0040, "Protecting Personally Identifiable Information at the Office of Civilian Human Resources and Human Resources Services Centers," June 30, 2010 **(FOUO)**

Air Force Audit Agency

Air Force Audit Agency Report No. F2010-0009-FB2000, "Implementation of Chief Financial Officer Compliance Tracking for Financial Systems," July 28, 2010

Air Force Audit Agency Report No. F2010-0005-FB4000, "Publicly Accessible Air Force Web Sites," May 14, 2010

Air Force Audit Agency Report No. F2010-0006-FB2000, "Air National Guard Reserve Writing System Controls," April 30, 2010

Air Force Audit Agency Report No. F2010-0003-FB4000, "Contractor Circuit Security," January 13, 2010

Air Force Audit Agency Report No. F2009-0010-FB2000, "Follow-Up Audit, Air Force Equipment Management Systems Controls," August 14, 2009

Air Force Audit Agency Report No. F2009-0007-FD4000, "Personnel Security Clearances," May 8, 2009

Air Force Audit Agency Report No. F2009-0003-FB4000, "Follow-Up Audit, Controls Over Access to Air Force Networks and Systems," April 30, 2009

Air Force Audit Agency Report No. F2009-0004-FB2000, “Defense Enterprise Accounting and Management System Controls,” February 20, 2009

Air Force Audit Agency Report No. F2009-0002-FB4000, “Plan of Action and Milestone Program Management,” November 5, 2008 **(FOUO)**

Air Force Audit Agency Report No. F2009-0001-FB2000, “Mechanization of Contract Administration Service Controls,” October 3, 2008

Air Force Audit Agency Report No. F2009-0001-FB4000, “Combat Information Transport System Technical Order Compliance Process,” October 3, 2008

Air Force Audit Agency Report No. F2008-0007-FB4000, “Federal Information Security Management Act Security Control Testing,” September 15, 2008 **(FOUO)**

Air Force Audit Agency Report No. F2008-0006-FB4000, “Mission Assurance Category YI Systems Certification and Accreditation,” August 22, 2008

Air Force Audit Agency Report No. F2008-0005-FB2000, “Comprehensive Cost and Requirements System Controls,” July 23, 2008

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. F2007-0004-FB4000, “Security of Remote Computer Devices,” March 13, 2007 **(FOUO)**

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

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. F2006-0006-FB2000, “Controls for the Wholesale and Retail Receiving and Shipping System,” May 19, 2006

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 enables the reconstruction and examination of the sequence of events or changes in an event.

IA Certification and Accreditation – Certification and accreditation is the standard DoD approach for identifying information security requirements, providing security solutions, and managing the security of DoD information systems.

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.

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.

Continuous Monitoring Management – The process implemented to maintain a current security status for one or more information systems or for the entire suite of information systems on which the operational mission of the enterprise depends. The process includes: 1) The development of a strategy to regularly evaluate selected IA controls/metrics, 2) Recording and evaluating IA relevant events and the effectiveness of the enterprise in dealing with those events, 3) Recording changes to IA controls, or changes that affect IA risks, and 4) Publishing the current security status to enable information sharing decisions involving the enterprise.

Contractor Systems – Agency systems operated on its behalf by contractors or other entities, including Agency systems and services residing in the cloud external to the Agency.

Cyber Security – Prevention of damage to, protection of, and restoration of computers, electronic communications systems, electronic communications services, wire communication, and electronic communications, including information contained therein, to ensure its availability, integrity, authentication, confidentially and non-repudiation.

Identity and Access Management – the processes, technologies and policies for managing digital identities and controlling how identities can be used to access resources.

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.

Interoperability – 1. The ability to operate in synergy in the execution of assigned tasks. 2. **(DoD only)** The condition achieved among communications-electronics systems or items of communications-electronics equipment when information or services can be exchanged directly and satisfactorily between them or their users.

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 that 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 and Environmental 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 regulations.

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 SSN; age; military rank; civilian grade; marital status; race; salary; home or office phone number; and other demographic, biometric, personal, medical, and financial information. This information is also referred to as PII, or that which can be used to distinguish or trace an individual's identity.

Remote Access Management – Access to an organizational information system by a user (or a process acting on behalf of a user) communicating through an external network (e.g., the Internet).

Risk Assessment – Risk assessment is an analysis of threats to and vulnerabilities of information systems and the potential impact of 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 Capital Planning – Synonym for capital programming and is a decision-making process for ensuring that IT investments integrate strategic planning, budgeting, procurement, and the management of IT in support of agency missions and business needs.

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, multidisciplinary 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.

Inspector General
Department of Defense