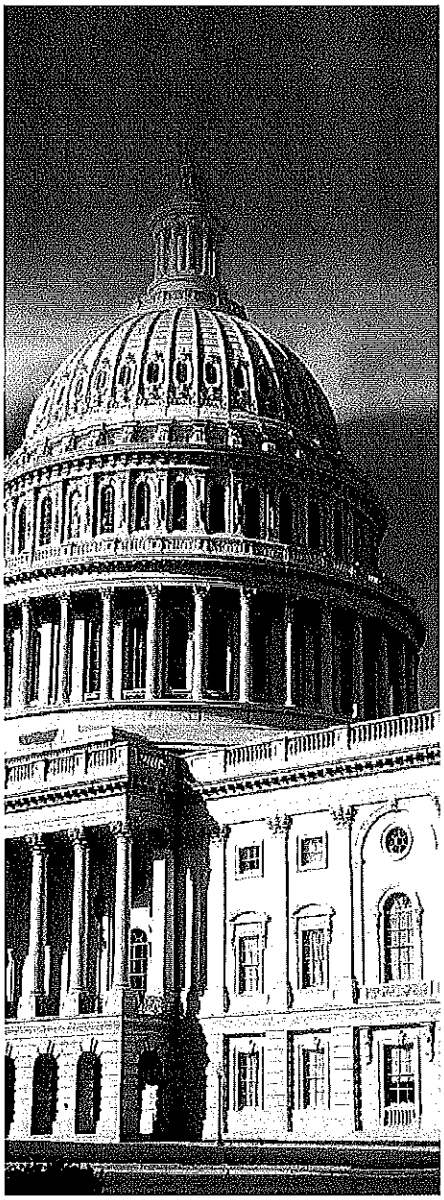
Report No. DODIG-2013-141

FOR OFFICIAL USE ONLY

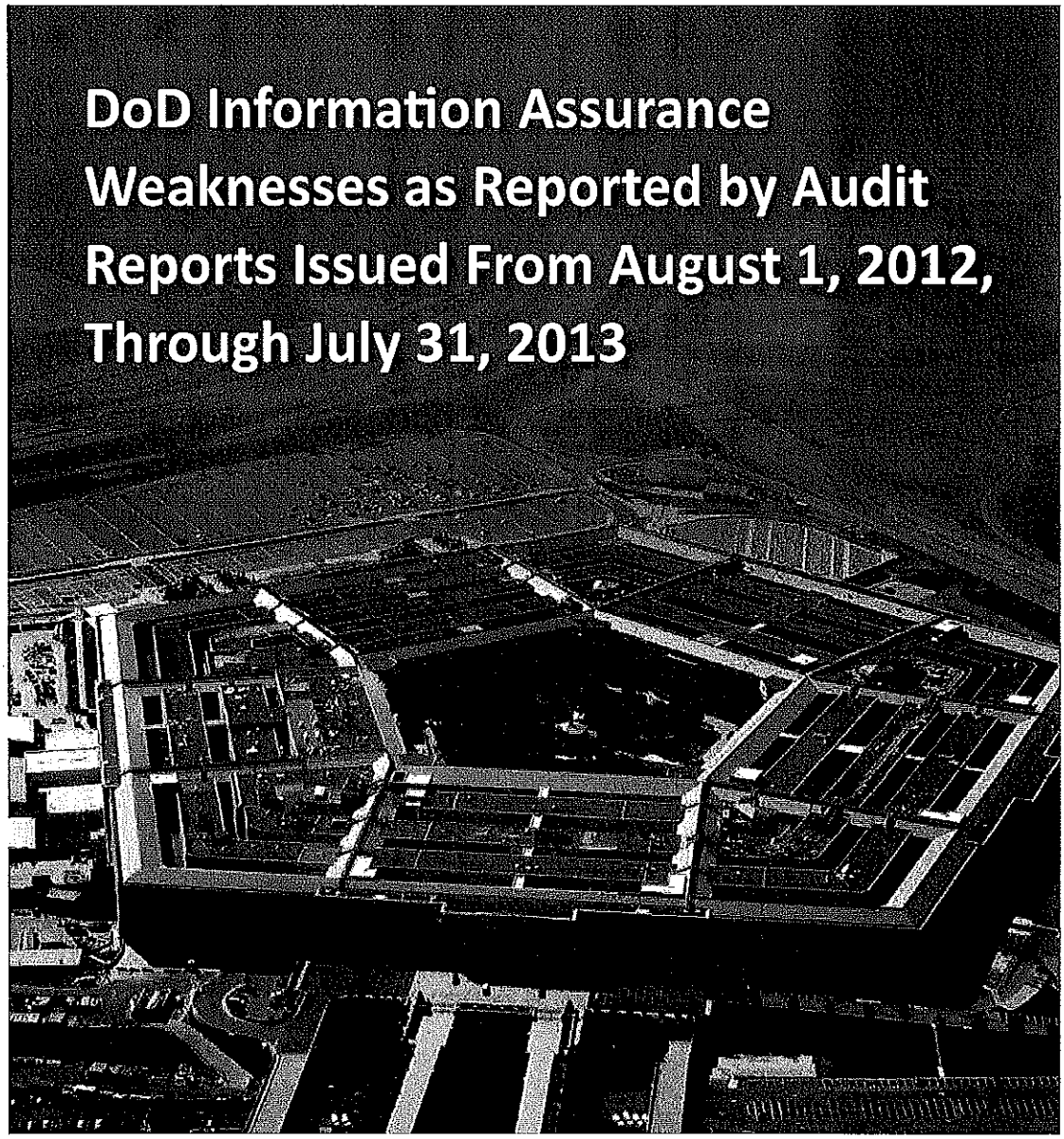
INSPECTOR GENERAL

U.S. Department of Defense

SEPTEMBER 30, 2013



DoD Information Assurance Weaknesses as Reported by Audit Reports Issued From August 1, 2012, Through July 31, 2013



INTEGRITY ★ EFFICIENCY ★ ACCOUNTABILITY ★ EXCELLENCE

FOR OFFICIAL USE ONLY

INTEGRITY ★ EFFICIENCY ★ ACCOUNTABILITY ★ EXCELLENCE

Mission

Our mission is to provide independent, relevant, and timely oversight of the Department of Defense that: supports the warfighter; promotes accountability, integrity, and efficiency; advises the Secretary of Defense and Congress; and informs the public.

Vision

Our vision is to be a model oversight organization in the federal government by leading change, speaking truth, and promoting excellence; a diverse organization, working together as one professional team, recognized as leaders in our field.

Fraud, Waste and Abuse

HOTLINE

1.800.424.9098 • www.dodig.mil/hotline

For more information about whistleblower protection, please see the inside back cover.

Results in Brief

Results in Brief: DoD Information Assurance Weaknesses as Reported by Audit Reports Issued From August 1, 2012, Through July 31, 2013

September 30, 2013

Objective

We summarized unclassified audit reports, issued by the DoD audit community and Government Accountability Office between August 1, 2012, and July 31, 2013, that contained findings on information assurance (IA) weaknesses in DoD. This summary report provides a reference document that identifies audit reports that contained findings outlining IA weaknesses in DoD and supports the Department of Defense Office of Inspector General's (DoD OIG) response to the requirements of Public Law 107-347, section 3545, Title III, "Federal Information Security Management Act (FISMA) of 2002," December 17, 2002.

This report is the 15th IA summary report issued by the DoD OIG since January 1999. To remain consistent with the Department of Homeland Security FY 2013 FISMA reporting metrics, the IA weakness categories used in this year's report have been updated from the previous summary reports. The updated IA weakness categories support a more efficient and effective DoD OIG response to the FISMA reporting metrics.

Results

During the reporting period, the DoD audit community and Government Accountability Office issued 28 unclassified reports and 1 testimony addressing a wide range of IA

Results Continued

weaknesses within DoD systems and networks. Reports issued during the reporting period most frequently cited weaknesses in the IA categories of risk management, identity and access management, and contingency planning.

Additionally, as of August 1, 2012, unclassified audit reports identified in the previously issued IA summary reports contained 294 unresolved IA-related recommendations. From August 1, 2012, through July 31, 2013, DoD management resolved 181 recommendations, leaving 113 IA-related unresolved recommendations that required management action.

Recommendations

In this summary report, we identified recommendations from previous reports. 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 is required.

Visit us on the web at www.dodig.mil

INSPECTOR GENERAL
DEPARTMENT OF DEFENSE
4800 MARK CENTER DRIVE
ALEXANDRIA, VIRGINIA 22350-1500

September 30, 2013

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

SUBJECT: DoD Information Assurance Weaknesses as Reported by Audit Reports Issued From August 1, 2012, Through July 31, 2013 (Report No. DODIG-2013-141)

We are providing this summary report for your information and use. The overall objective is to summarize the information assurance (IA) weaknesses identified in unclassified audit reports issued by the DoD audit community and the Government Accountability Office (GAO) between August 1, 2012, and July 31, 2013. During the reporting period, the DoD audit community and GAO issued 28 unclassified reports and 1 testimony addressing information assurance weaknesses within DoD systems and networks. 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 the DoD information technology environment.

The report contains no recommendations for action; however, it does identify previously issued audit reports that contain open recommendations. 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-(b) (6) (DSN 664-(b) (6)).

Daniel R. Blair
Deputy Inspector General
for Auditing

Contents


INSPECTOR GENERAL
DEPARTMENT OF DEFENSE

Introduction

Objective

The overall objective was to summarize the information assurance (IA) weaknesses identified in unclassified reports and testimonies issued by the DoD audit community and the Government Accountability Office (GAO) between August 1, 2012, and July 31, 2013. 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 15th annual IA summary that the Department of Defense Office of Inspector General (DoD OIG) has issued since January 1999. This report will provide a reference document to identify audit reports that contained findings outlining IA weaknesses in DoD as related to Public Law 107-347, section 3545, Title III, "Federal Information Security Management Act (FISMA) of 2002," December 17, 2002.

FISMA Requires Security Controls Over Federal Information

The Federal Government has a duty to secure Federal information and information systems. This responsibility is promulgated in FISMA, which 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 agencywide information security program to provide security for the information and information systems that support the operations and assets of the agency. Each agency must comply with FISMA and related policies, procedures, standards, and guidelines, including the information security standards issued under section 11331, title 40, United States Code (40 U.S.C. 11331), "Responsibilities for Federal Information Systems Standards."

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. Due to the size and number of DoD organizations, a yearly evaluation that addresses all the FISMA metrics is not practical. Instead, the DoD OIG uses this summary of unclassified audit reports issued by the DoD audit community and GAO that address IA weaknesses related to the FISMA metrics to support the DoD OIG's annual requirement for FISMA.

Current IA Weakness Categories

In 2010, the Office of Management and Budget (OMB) mandated the Department of Homeland Security (DHS) provide guidance and operational oversight for Federal agency FISMA reporting. Specifically, DHS must develop and issue FISMA reporting metrics for Federal agencies. Federal agencies are required to submit an annual FISMA assessment based on metrics related to information security management. The Inspector General, Chief Information Office, and Privacy Office of each agency submit a single FISMA assessment report to OMB. The annual reports are submitted electronically in CyberScope, an automated, streamlined platform used for secure FISMA reporting for the collection of agency cybersecurity information.

To further empower Inspectors General to focus on how agencies are evaluating risk and prioritizing security issues, the DHS issued, "FY 2013 Inspector General Federal Information Security Management Act Reporting Metrics," November 30, 2012. The FY 2013 FISMA metrics include Administrative Priorities that focus on continuous monitoring, Trusted Internet Connection capabilities and traffic consolidation, and implementation of Homeland Security Presidential Directive-12. To provide a more efficient and effective DoD OIG response to the FISMA requirements, this year's IA weakness categories are consistent with the DHS FY 2013 FISMA Inspectors General reporting metrics. See the Glossary for definitions of each IA weakness category. This year's categories include:

- Configuration Management,
- Contingency Planning,
- Continuous Monitoring,
- Contractor Systems,
- Identity and Access Management,
- Incident Response & Reporting,
- Plan of Action and Milestones,
- Remote Access Management,
- Risk Management,
- Security Capital Planning, and
- Security Training.

DoD-Issued IA Guidance

DoD issued policy covering the requirements of FISMA through the following IA guidance:

- DoD Directive 5400.11, "DoD Privacy Program," May 8, 2007, Incorporating Change 1, September 1, 2011, establishes policy for the respect and protection of an individual's personal information and fundamental right to privacy.
- 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 the DoD 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 Directive 8000.01, "Management of the Department of Defense Information Enterprise," February 10, 2009, establishes that DoD investments in information solutions be mandated through a capital planning process that (1) is performance and results based, (2) provides for analyzing, selecting, controlling, and evaluating investments, as well as assessing and managing associated risks, (3) interfaces with DoD key decision support systems, and (4) requires the review of information technology investments for compliance with architectures, information technology standards, and related policy requirements.
- DoD Instruction 8582.01, "Security of Unclassified DoD Information on Non-DoD Information Systems," June 6, 2012, establishes policy for securing unclassified information on non-DoD information systems.

Results

DoD Audit Community and GAO Identified IA Weaknesses Throughout DoD

Between August 1, 2012, and July 31, 2013, the DoD audit community and GAO issued 28 unclassified reports and 1 testimony that identified a wide range of IA weaknesses within DoD systems and networks. The DoD audit community and GAO continued to provide recommendations to correct identified IA weaknesses and work with DoD Components to implement the recommendations.

Reports on IA Weaknesses

This report summarizes the IA weaknesses reported in the DoD audit community and GAO reports as they relate to FY 2013 FISMA reporting metrics. Table 1 shows the number of IA weaknesses reported in the 28 unclassified reports and 1 testimony. See the Glossary for specialized terms.

Table 1. IA Weaknesses Reported From August 1, 2012, Through July 31, 2013

IA Weakness Categories	GAO	DoD OIG	Military Departments	Total
Risk Management	4	3	7	14
Identity and Access Management	0	2	7	9
Contingency Planning	1	2	4	7
Configuration Management	0	3	3	6
Security Training	1	0	4	5
Incident Response and Reporting	2	0	2	4
Continuous Monitoring	0	3	0	3
Plan of Action and Milestones	1	1	1	3
Security Capital Planning	2	0	0	2
Remote Access Management	0	1	0	1
Contractor Systems	0	0	0	0

Types of IA Weaknesses

Reports issued during the reporting period most frequently cited weaknesses in the IA categories of risk management, identity and access management, and contingency planning. 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.

Risk Management

Risk management is the process of managing threats to organizational operations, organizational assets, other organizations, individuals, and the United States that result from operating an information system. Risk management includes:

- performance of a risk assessment,
- implementation of a risk mitigation strategy, and
- employment of techniques and procedures for the continuous monitoring of the information system's security.

The DoD audit community and GAO reported weaknesses related to risk management in 14 reports. Examples of the risk management IA weakness category were identified in the following reports.

Air Force Did Not Properly Establish Information Protection Offices

Air Force Audit Agency Report No. F2013-0005-O10000, "Enterprise Information Protection Capability," October 26, 2012, found that Air Force Major Commands, direct reporting units, and installation-level commanders did not properly establish information protection offices (IPOs) and did not ensure critical IPO management positions were created and filled. Within the Air Force, information protection refers to the policies, processes, and use of risk management and mitigation actions to prevent compromise, loss, or unauthorized access of Air Force information. However, the report found that of the 17 organizations reviewed, 4 did not establish IPOs and 16 did not align manpower to fulfill IPO management positions. This occurred because the Information Protection Directorate, Office of the Administrative Assistant to the Air Force (SAF/AAP), did not provide Air Force Major Commands, direct reporting units, and installation-level commanders with the documents needed to facilitate hiring; did not establish guidance to inform the Air Force of IPO implementation; and did not establish processes to monitor and evaluate IPO implementation within the Air Force. As a result, the Air Force was unable to reduce the risk of unauthorized disclosure, compromise, or loss of Air Force operational and critical information.

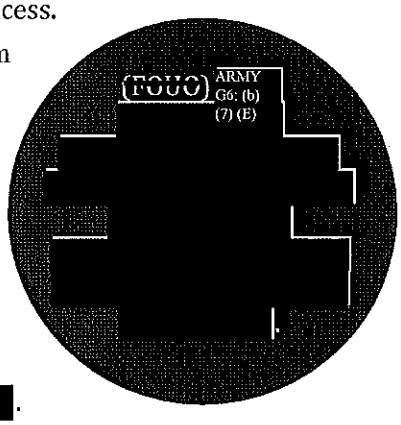
The report recommended the Administrative Assistant to the Air Force to direct the SAF/AAP to provide Air Force organizations with approved, classified, and published civilian positions description documents to facilitate filling information protection positions; establish an Air Force instruction regarding the revised information protection program requirements; and establish IPO governance processes to monitor and assess organizations in establishing and staffing IPOs. According to the report, the Administrative Assistant to the Air Force agreed with the recommendations and stated the SAF/AAP would perform all the recommended actions.

DoD Automated Information Systems Operated Without Proper Security Controls

~~(FOUO)~~ DoD Inspector General (DoD IG) Report No. DODIG-2013-068, "Maintaining Authorization Accreditation for Select DoD Information Systems Needed Improvement," April 15, 2013, found 2 of 10 automated information system applications operated without the proper security controls in place to continue their authorization agreements.

~~(FOUO)~~ Specifically, ARMY G6: (b) (7) (E) [redacted].

This occurred because the Army application IA manager did not have proper guidance for the Tenant Security Plan process. Additionally, the Air Force Container Design System operated on the DoD network with an unsupported system server operating system, a Category I weakness, and operated without an accreditation decision for 14 months. This occurred because the Air Force program manager did not properly plan for upgrading the unsupported system. As a result, DoD networks were vulnerable to cyber-attacks ARMY G6: (b) (7) (E) [redacted].



~~(FOUO)~~ The report recommended the Director, Army Chief Information Officer/G-6 Cybersecurity Directorate, develop instructions for the Tenant Security Plan process and develop and implement training for Army Chief Information Officer certification and accreditation officials to define procedures for performing arbitration during a disagreement regarding correcting system weaknesses. According to the report, the Director agreed with the recommendations and stated officials will update their Best Business Practices and document contacts for arbitration when there are disagreements on correcting IA system weaknesses. The report also recommended the Program

(~~FOUO~~) Manager, Air Force for the Container Design Retrieval System, ensure Category I weaknesses are corrected in accordance with DoD and Air Force requirements and ensure reviews of all security IA controls are completed annually. According to the report, Air Force management agreed with the recommendations, stating the Air Force Container Design System received an authorization to operate in November 2012 after the Category I weaknesses were corrected. Further, management stated the system is scheduled to undergo its annual security review in November 2013, which will be documented.

Identity and Access Management

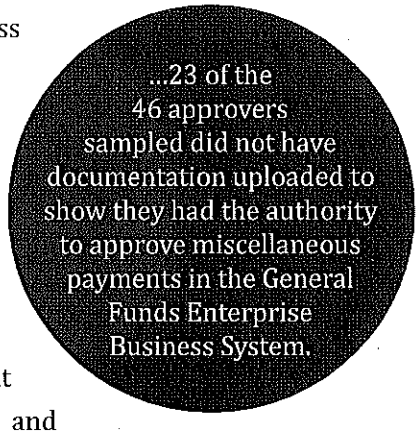
Identity and access management includes the processes, technologies, and policies for managing digital identities and controlling how identities can be used to access resources. The DoD audit community reported weaknesses related to identity and access management in 9 reports. Examples of the identity and access management IA weakness category were identified in the following reports.

Navy Electronic Leave System Administrators Had Unauthorized Access

(~~FOUO~~) Naval Audit Service Report No. N2013-0024, "Internal Controls over Navy's Electronic Leave System," April 26, 2013, found that access controls were not properly used for the Navy's Electronic Leave (e-Leave), a self-service application that allows electronic processing of leave transactions. For example, 10 of 88 Command Leave Administrators (CLAs) sampled had unauthorized access to e-Leave because the CLAs did not have their access removed when they transitioned out of the position. Of these 10 CLAs with unauthorized access, 8 accessed the accounts during the time they were not authorized access. This occurred because there was an oversight within the Personnel Support Detachments (PSDs)/commands. According to the PSD personnel, it is up to the command to notify PSD when an individual's access should be removed if they are no longer performing the role of a CLA. As a result, the Navy's ability to achieve auditable financial statements could be negatively affected because DoD guidance states that strong internal controls are important to achieve audit readiness. The report recommended the Deputy Chief of Naval Personnel implement controls, such as periodic reviews of CLA authorizations, to ensure CLAs can only access e-Leave as authorized and as required by their current position. According to the report, the Deputy Chief agreed with the recommendation and stated the Navy plans to validate the authorization of e-Leave CLAs.

Army Miscellaneous Payment Approval Process Was Ineffective

Army Audit Agency Report No. A-2013-0130-FMR, "Miscellaneous Pay Process General Fund Enterprise Business System," July 31, 2013, found that the Army was reliant on miscellaneous pay approvers to verify that miscellaneous payments were valid, accurate, and supported before they are approved for payment. However, the miscellaneous pay approvers were not an effective manual control because 23 of the 46 approvers sampled did not have documentation uploaded to show they had the authority to approve miscellaneous payments in the General Funds Enterprise Business System (GFEBS). Specifically, 17 of the 23 approvers did not have any form uploaded and the remaining 6 approvers had forms uploaded, but these forms did not state that the individual had the authority to approve miscellaneous payments in GFEBS. This occurred because the Army had not developed functional guidance or training to identify the responsibilities of ensuring that miscellaneous payments were valid, accurate, and supported to sustain a financial audit.



Additionally, the Army lacked management oversight of this process and did not ensure that an approver's authority to approve miscellaneous payments in the GFEBS was uploaded in the module. For the miscellaneous pay approvers to be an effective control, functional guidance needs to be established, the approvers need training, management needs to provide oversight, and evidence that approvers are authorized to approve miscellaneous payments in the GFEBS needs to be uploaded in the module.

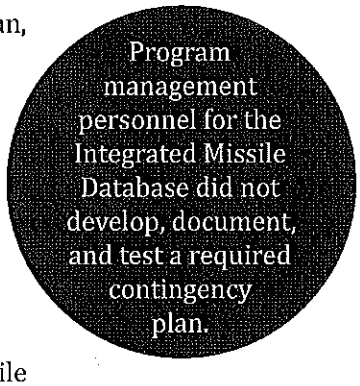
The report recommended the Deputy Assistant Secretary of the Army (Financial Operations) develop guidance for miscellaneous pay approvers, develop and provide functional training for miscellaneous pay approvers, and require verification that miscellaneous pay approvers have written authority to approve payments in the GFEBS. According to the report, the Deputy Assistant agreed with the recommendations. The Deputy Assistant stated he drafted standing operating procedures and redistributed guidance on miscellaneous payments, increased functional training on miscellaneous pay approvers, and verified documentation of pay approver authority.

Contingency Planning

Contingency planning is the process of preparing 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. The DoD audit community and GAO reported weaknesses related to contingency planning in 7 reports. The following reports identified examples of the contingency planning IA weakness category.

Air Force Integrated Missile Database System Program Personnel Did Not Develop, Document, and Test Required Contingency Plan

Air Force Audit Agency Memorandum Report of Audit F2013-0011-O10000, "Integrated Missile Database System Application Controls," January 15, 2013, found system application controls for the Integrated Missile Database system needed improvement, including the contingency plan. Program management personnel for the Integrated Missile Database did not develop, document, and test a required contingency plan. Specifically, personnel did not identify the roles and responsibilities of persons required to implement the plan, test the plan periodically, and store backup software in a secure offsite location, and management did not approve and sign the plan, as required. This occurred because program management office personnel followed Air Force guidance that did not align with the current Federal standards. As a result, strengthening system controls will enhance operational and financial data integrity for approximately 3,360 missile motors valued at $2.2 billion.



The report recommended that the Air Force Materiel Command, direct the Integrated Missile Database program management office to fully align their procedures with current Federal regulations, as required by FISMA. Specifically, the report recommended the Commander establish and implement a comprehensive contingency plan that is based on the categorization of the system's risk level, includes identification of roles and responsibilities, and is approved and signed by the Air Force Nuclear Weapons Center Intercontinental Ballistic Missile Systems Directorate Commander. According to the memorandum report, management agreed with the recommendation and stated Air Force guidance will be updated and Air Force management will direct Integrated Missile Database personnel to establish and implement a contingency plan.

Navy Lacked Contingency Plan for Safeguarding and Disposing Personally Identifiable Information

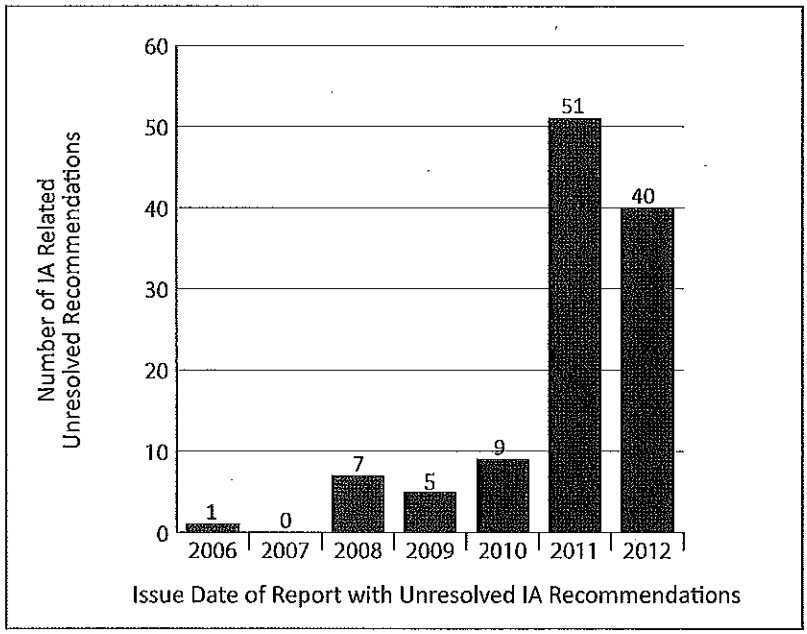
~~(FOUO)~~ Naval Audit Service Report No. N2013-0034, "Department of the Navy Contract Requirements–Personally Identifiable Information and Sensitive Data," June 27, 2013, found the Bureau of Naval Personnel and Naval Health Clinic Annapolis did not have an approved and implemented contingency plan in place to handle an unexpected event that would interrupt operations. For example, the Bureau of Naval Personnel and Naval Health Clinic Annapolis did not have a contingency plan in the event Department of the Navy personally identifiable information or sensitive data were compromised, because there was a lack of management oversight. While both entities had a contingency plan in draft status, neither contingency of operations plan had been approved or signed by management. As a result, sensitive information and information systems may not be protected in accordance with Federal, DoD, and Department of the Navy requirements.

~~(FOUO)~~ The report recommended the Office of the Chief of Naval Personnel and the Bureau of Medicine and Surgery require Naval Health Clinic Annapolis to approve and implement a contingency plan to support and/or perform Department of the Navy mission essential functions and facilitate business continuity during recovery from a disruptive event. According to the report, management agreed with the recommendations. The Office of the Chief of Naval Personnel provided a target completion date for the implementation of the draft continuity of operations plan by the end of FY 2013. Further, the Bureau of Medicine and Surgery advised that the continuity of operations plan was revised and the memorandum to implement was signed in June 2013. The report also recommended the Bureau of Medicine and Surgery determine if other Health Clinics have unimplemented contingency plans and, if so, require these plans to be approved and implemented. According to the report, management agreed with the recommendation and stated they are currently requesting verification of their subordinate's continuity of operations plans.

DoD's Progress to Implement Recommendations Reported in Previously Issued IA Summary Reports

As of August 1, 2012, audit reports identified in the previously issued IA summary reports contained 294 unresolved IA-related recommendations. From August 1, 2012, through July 31, 2013, DoD management resolved 181 recommendations, leaving 113 IA related unresolved recommendations that required management action. Of the remaining 113 unresolved recommendations, more than 80 percent were made in 2011 and 2012. See the figure on page 11 for a breakout of the issue date of reports that contains the remaining 113 unresolved recommendations. See Appendix E for a listing of the reports with unresolved recommendations relating to IA weaknesses.

Figure. Issue Date of Reports Containing Unresolved Recommendations Related to IA Weaknesses



IA Weaknesses Identified in Unresolved Recommendations

The most common IA weaknesses identified in the remaining unresolved recommendations are related to the IA categories of risk management and configuration management. See Table 2 below for a breakout of IA weakness categories as they relate to these unresolved recommendations.

Table 2. IA Weaknesses Identified in Unresolved Recommendations

IA Weakness Categories	GAO	DoD OIG	Military Departments	Total
Risk Management	4	9	51	64
Configuration Management	0	13	8	21
Identity and Access Management	0	6	13	19
Plan of Action and Milestones	8	5	1	14
Continuous Monitoring	1	0	6	7
Contingency Planning	0	0	5	5
Incident Response and Reporting	1	2	2	5
Security Training	1	0	5	6
Contractor Systems	1	0	2	3
Security Capital Planning	3	0	0	3
Remote Access Management	0	0	1	1

Note: Totals do not equal the number of unresolved recommendations identified because one recommendation may cover several IA weaknesses.

Summary

The DoD audit community and GAO issued 28 unclassified reports and 1 testimony from August 1, 2012, through July 31, 2013, that identified IA weaknesses related to the FY 2013 FISMA Inspectors General reporting metrics. Within the reports and testimony, risk management, identity and access management, and contingency planning were the most frequently cited IA weaknesses. The DoD audit community and GAO continue to review and report on IA weaknesses found within DoD information technology systems and networks. Further, the DoD audit community and GAO provided recommendations to correct the identified IA weaknesses, and DoD continues to make progress in addressing those recommendations.

Appendix A.

Scope and Methodology

We conducted this summary work from May 2013 through September 2013. We followed generally accepted government auditing standards, except for the standards of planning and evidence because this report summarizes previously released reports. This summary report supports the DoD OIG response to the requirements of Public Law 107-347, section 3545, Title III, "Federal Information Security Management Act (FISMA) of 2002," December 17, 2002.

Also, this report summarizes the DoD IA weaknesses identified in 28 unclassified reports and 1 testimony that GAO and the DoD audit community issued from August 1, 2012, through July 31, 2013. To prepare this summary, the DoD OIG audit team reviewed the websites 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 followup organizations, summarized reports with unresolved recommendations on IA weaknesses. We did not review the supporting documentation for any of the reports. This summary report does not make recommendations because recommendations have already been made in the summarized reports.

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 5 years, DoD OIG issued 5 summary reports summarizing IA weaknesses identified in 195 audit reports issued by the DoD audit community and the Government Accountability Office. Unrestricted DoD IG reports can be accessed at http://www.dodig.mil/pubs/index.cfm?office=Audit. The remainder of the reports are For Official Use Only and can be obtained through the Freedom of Information Act Requester Service Center website at http://www.dodig.mil/foia/submitfoia.html.

DoD IG Report No. DODIG-2012-145, "DoD Information Assurance Weaknesses as Reported by Audit Reports Issued From August 1, 2011, Through July 31, 2012," September 27, 2012 (Report is FOUO)

DoD IG Report No. D-2011-114, "Summary of Information Assurance Weaknesses as Reported by Audit Reports Issued From August 1, 2010, Through July 31, 2011," September 30, 2011

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 (Report is 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 (Report is 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

Appendix C.

Matrix of IA Weaknesses Reported From August 1, 2012, Through July 31, 2013

Agency Report No.	Configuration Management	Contingency Planning	Continuous Monitoring	Contractor Systems	Identity and Access Management	Incident Response and Reporting	Plan of Action and Milestones	Remote Access Management	Risk Management	Security Capital Planning	Security Training
Government Accountability Office											
GAO-12-956									X		
GAO-12-992											X
GAO-13-87										X	
GAO-13-98									X		
GAO-13-128		X				X					
GAO-13-157									X		
GAO-13-311									X		
GAO-13-557							X			X	
GAO-13-462T						X					
DoD Inspector General											
DODIG-2012-122 (FOUO)					X						
DODIG-2013-036 (FOUO)		X	X								
DODIG-2013-055 (FOUO)	X							X	X		
DODIG-2013-060	X										
DODIG-2013-068 (FOUO)									X		
DODIG-2013-072 (FOUO)		X	X		X						
DODIG-2013-107 (FOUO)			X				X				
DODIG-2013-109 (FOUO)	X								X		

Agency Report No.	Configuration Management	Contingency Planning	Continuous Monitoring	Contractor Systems	Identity and Access Management	Incident Response and Reporting	Plan of Action and Milestones	Remote Access Management	Risk Management	Security Capital Planning	Security Training
Army Audit Agency											
A-2012-0200-FMT						X					
A-2013-0130-FMR					X						X
Naval Audit Service											
N2012-0063 (FOUO)					X				X		X
N2012-0070 (FOUO)							X		X		
N2013-0024 (FOUO)					X				X		
N2013-0034 (FOUO)		X									
Air Force Audit Agency											
F2013-0003-O10000		X			X				X		
F2013-0005-O10000									X		X
F2013-0007-O10000					X	X					X
F2013-0009-O10000	X	X			X				X		
F2013-0011- O10000	X	X			X				X		
F2013-0003-L20000	X										
Total	**6**	**7**	**3**	**0**	**9**	**4**	**3**	**1**	**14**	**2**	**5**

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, 2012, Through July 31, 2013

Unrestricted GAO reports can be accessed over the Internet at http://www.gao.gov/. Unrestricted Army reports can be accessed from .mil and gao.gov domains over the Internet at https://www.aaa.army.mil/. Naval Audit Service and Air Force Audit Agency reports are unavailable over the Internet. Unrestricted DoD IG reports can be accessed at http://www.dodig.mil/pubs/index.cfm?office=Audit.

GAO

GAO Report No. GAO-12-956, "Navy Implementing Revised Approach, but Improvement Needed in Mitigating Risks," September 2012

GAO Report No. GAO-12-992, "Department-Level Actions Needed to Assess Collaboration Performance, Address Barriers, and Identify Opportunities," September 2012

GAO Report No. GAO-13-87, "Agencies Need to Strengthen Oversight of Billions of Dollars in Operations and Maintenance Investments," October 2012

GAO Report No. GAO-13-98, "Opportunities Exist to Improve Transparency and Oversight of Investment Risk at Select Agencies," October 2012

GAO Report No. GAO-13-128, "DoD Needs to Address Gaps in Homeland Defense and Civil Support Guidance," October 2012

GAO Report No. GAO-13-157, "DoD Assessment Needed to Determine Requirement for Critical Technologies List," January 2013

GAO Report No. GAO-13-311, "Selected Defense Programs Need to Implement Key Acquisition Practices," March 2013

GAO Report No. GAO-13-557, "Further Actions Needed to Address Challenges and Improve Accountability," May 2013

DoD IG

DoD IG Report No. DODIG-2012-122, "DoD Should Procure Compliant Physical Access Control Systems to Reduce the Risk of Unauthorized Access," August 29, 2012 (Report is FOUO)

DoD IG Report No. DODIG-2013-036, "Improvements Are Needed to Strengthen the Security Posture of USACE, Civil Works, Critical Infrastructure and Industrial Control Systems in the Northwestern Division," January 14, 2013 (Report is FOUO)

DoD IG Report No. DODIG-2013-055, "Improvements Needed With Wireless Intrusion Detection Systems at the Defense Logistics Agency," March 13, 2013 (Report is FOUO)

DoD IG Report No. DODIG-2013-060, "Improvements Needed With Tracking and Configuring Army Commercial Mobile Devices," March 26, 2013

DoD IG Report No. DODIG-2013-068, "Maintaining Authorization Accreditation for Select DoD Information Systems Needed Improvement," April 15, 2013 (Report is FOUO)

DoD IG Report No. DODIG-2013-072, "Data Loss Prevention Strategy Needed for the Case Adjudication Tracking System," April 24, 2013 (Report is FOUO)

DoD IG Report No. DODIG-2013-107, "Defense Information Systems Agency Needs to Improve Its Information Assurance Vulnerability Management Program," July 26, 2013 (Report is FOUO)

DoD IG Report No. DODIG-2013-109, "Improved Security Needed to Protect Infrastructure and Systems in the Great Lakes and Ohio River Division," July 29, 2013 (Report is FOUO)

Army Audit Agency

Army Audit Agency Report No. A-2012-0200-FMT, "Audit of Army Materiel Command Cyber Program (A-2012-FMT-0230.000) and the Audit of the Army's Reporting of Cyber Events/Incidents for Army Materiel Command Systems (A-2012-FMT-0307.000)," September 28, 2012

Army Audit Agency Report No. A-2013-0130-FMR, "Miscellaneous Pay Process General Fund Enterprise Business System," July 31, 2013

Naval Audit Service

Naval Audit Service Report No. N2012-0063, "Managing Personally Identifiable Information at Navy Operational Support Centers," August 28, 2012 (Report is FOUO)

Naval Audit Service Report No. N2012-0070, "Navy Compliance with Department of Defense Information Assurance Certification and Accreditation Process," September 28, 2012 (Report is FOUO)

Naval Audit Service Report No. N2013-0024, "Internal Controls over Navy's Electronic Leave System," April 26, 2013 (Report is FOUO)

Naval Audit Service Report No. N2013-0034, "Department of the Navy Contract Requirements Personally Identifiable Information and Sensitive Data," June 27, 2013 (Report is FOUO)

Air Force Audit Agency

Air Force Audit Agency Report No. F2013-0003-O10000, "Memorandum Report of Audit F2013-0003-O10000, Reliability and Maintainability Information System Application Controls," October 22, 2012

Air Force Audit Agency Report No. F2013-0005-O10000, "Enterprise Information Protection Capability," October 26, 2012

Air Force Audit Agency Report No. F2013-0007-O10000, "Memorandum Report of Audit F2013-0007-O10000, Financial Inventory Accounting and Billing System Application Controls," November 20, 2012

Air Force Audit Agency Report No. F2013-0009-O10000, "Memorandum Report of Audit F2013-0009-O10000, Reliability, Availability, Maintainability Support System for Electronic Combat Pods - Application Controls," January 3, 2013

Air Force Audit Agency Report No. F2013-0011-O10000, "Memorandum Report of Audit F2013-0011-O10000, Integrated Missile Database System Application Controls," January 15, 2013

Air Force Audit Agency Report No. F2013-0003-L20000, "Serialized Parts Configuration Management," April 1, 2013

GAO Testimony

GAO Report No. GAO-13-462T, "A Better Defined and Implemented National Strategy Is Needed to Address Persistent Challenges," March 7, 2013

Appendix E.

Audit Reports From Prior IA Summary Reports With Unresolved Recommendations

IA weaknesses continue to exist throughout DoD. As of August 1, 2012, previously identified audit reports contained 294 unresolved recommendations. During the reporting period, management resolved 181 recommendations, leaving 113 IA-related unresolved recommendations; management had not corrected agreed-upon IA weaknesses within 12 months of the report issue date. These 113 unresolved recommendations are identified within the 41 audit reports listed below. The list of reports with unresolved recommendations was compiled based on information GAO and the DoD audit community provided in August 2013 and may be incomplete because of the extent of information maintained in their respective followup systems.

Unrestricted GAO reports can be accessed over the Internet at http://www.gao.gov/. Unrestricted Army reports can be accessed from .mil and gao.gov domains over the Internet at https://www.aaa.army.mil/. Naval Audit Service and Air Force Audit Agency reports are unavailable over the Internet. Unrestricted DoD IG reports can be accessed at http://www.dodig.mil/pubs/index.cfm?office=Audit.

GAO

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-11-566R, "Defense Logistics: Oversight and a Coordinated Strategy Needed to Implement the Army Workload and Performance System," July 2011

GAO Report No. GAO-12-138, "Warfighter Support: DOD Has Made Progress, but Supply and Distribution Challenges Remain in Afghanistan," October 2011

GAO Report No. GAO-12-83, "Defense Contract Management Agency: Amid Ongoing Efforts to Rebuild Capacity, Several Factors Present Challenges in Meeting Its Missions," November 2011

GAO Report No. GAO-12-241, "Information Technology: Departments of Defense and Energy Need to Address Potentially Duplicative Investments," February 2012

GAO Report No. GAO-12-669, "VA/DOD Federal Health Care Center: Costly Information Technology Delays Continue and Evaluation Plan Lacking," June 2012

DoD IG

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

DoD IG Report No. D-2011-096, "Improvements Are Needed to the DoD Information Assurance Vulnerability Management Program," August 12, 2011 (Report is FOUO)

DoD IG Report No. D-2011-101, "Controls Over Army Deployable Disbursing System Payments Need Improvement," August 17, 2011

DoD IG Report No. DODIG-2012-050, "Improvements Needed With Host-Based Intrusion Detection Systems," February 3, 2012 (Report is FOUO)

DoD IG Report No. DODIG-2012-069, "Action is Needed to Improve the Completeness and Accuracy of DEERS Beneficiary Data," April 2, 2012

DoD IG Report No. DODIG-2012-090, "Improvements Needed to Strengthen the Defense Enrollment Eligibility Reporting System Security Posture," May 22, 2012 (Report is FOUO)

Army Audit Agency

Army Audit Agency Report No. A-2011-0219-ALA, "Configuration Management of Weapon Systems, Program Executive Offices, Ground Combat Systems, and Combat Support and Combat Service Support," September 30, 2011

Army Audit Agency Report No. A-2012-0127-FMT, "Bandwidth Requirements for Connecting Army Installations to the Global Information Grid," July 2, 2012

Naval Audit Service

Naval Audit Service Report No. N2008-0023, "Information Security within the Marine Corps," February 20, 2008 (Report is FOUO)

Naval Audit Service Report No. N2009-0027, "Processing of Computers and Hard Drives During the Navy Marine Corps Intranet (NMCI) Computer Disposal Process," April 28, 2009 (Report is FOUO)

Naval Audit Service Report No. N2010-0005, "Information Security for Research, Development, Test and Evaluation and Education Legacy Networks," January 7, 2010 (Report is 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 (Report is FOUO)

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

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

Naval Audit Service Report No. N2011-0047, "Certification and Accreditation of Information Systems within the Marine Corps," August 2, 2011 (Report is FOUO)

Naval Audit Service Report No. N2012-0010, "Defense Travel System - Marine Corps," December 21, 2011 (Report is FOUO)

Air Force Audit Agency

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. F2009-0001-FB4000, "Combat Information Transport System Technical Order Compliance Process," October 3, 2008

Air Force Audit Agency Report No. F2009-0001-FB2000, "Mechanization of Contract Administration Services System Controls," October 3, 2008

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. F2009-0007-FD4000, "Personnel Security Clearances," May 8, 2009

Air Force Audit Agency Report No. F2010-0003-FB4000, "Contractor Circuit Security," January 13, 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. F2010-0009-FB2000, "Implementation of Chief Financial Officer Compliance Tracking for Financial Systems," July 28, 2010

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

Air Force Audit Agency Report No. F2011-0003-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. F2012-0003-FC4000, "Management of Air Force Nuclear Weapons-Related Materiel Positive Inventory Controls," November 3, 2011

Air Force Audit Agency Report No. F2012-0002-FB4000, "Air National Guard Information Systems Security," January 11, 2012

Air Force Audit Agency Report No. F2012-0003-FB2000, "Defense Enterprise Accounting and Management System Controls," January 17, 2012

Air Force Audit Agency Report No. F2012-0003-FB4000, "Systems Vulnerability Detection and Mitigation," February 16, 2012

Air Force Audit Agency Report No. F2012-0005-FB2000, "Memorandum Report of Audit F2012-0005-FB2000, Automated Funds Management Application Controls," April 4, 2012

Air Force Audit Agency Report No. F2012-0006-FB2000, "Memorandum Report of Audit F2012-0006-FB2000, Positive Inventory Control Fusion - Application Controls," April 12, 2012

Air Force Audit Agency Report No. F2012-0009-FB2000, "Memorandum Report of Audit F2012-0009-FB2000, Automated Funds Management General Controls," June 26, 2012

Glossary

Configuration Management – 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 Planning – the process of preparing 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.

Continuous Monitoring – 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.

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

Incident Response and Reporting – the mitigation of violations of security policies and recommended practices; also referred to as incident handling.

Plan of Action and Milestones – 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.

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, such as the Internet.

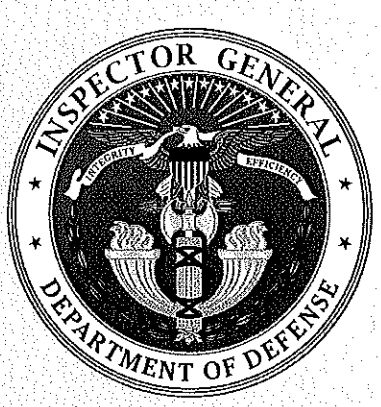
Risk Management – the process of managing risks to organizational operations (including mission, functions, image, reputation), organizational assets, individuals, other organizations, and the Nation, resulting from the operation of an information system, and includes: (1) the conduct of a risk assessment; (2) the implementation of a risk mitigation strategy; and (3) employment of techniques and procedures for the continuous monitoring of the security state of the information system.

Security Capital Planning – a decision making process for ensuring that information technology investments integrate strategic planning, budgeting, procurement, and the management of information technology resources in support of agency missions and business needs; also referred to as capital programming.

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

Acronyms and Abbreviations

CLAs	Command Leave Administrators
DHS	Department of Homeland Security
FISMA	Federal Information Security Management Act
GAO	Government Accountability Office
GFEBS	General Funds Enterprise Business System
IA	Information Assurance
IPOs	Information Protection Offices
OMB	Office of Management and Budget
PSDs	Personnel Support Detachments
SAF/AAP	Information Protection Directorate, Office of the Administrative Assistant to the Air Force


INSPECTOR GENERAL
INTEGRITY
EFFICIENCY
DEPARTMENT OF DEFENSE

Whistleblower Protection

U.S. Department of Defense

The Whistleblower Protection Enhancement Act of 2012 requires the Inspector General to designate a Whistleblower Protection Ombudsman to educate agency employees about prohibitions on retaliation, and rights and remedies against retaliation for protected disclosures. The designated ombudsman is the DoD IG Director for Whistleblowing & Transparency. For more information on your rights and remedies against retaliation, go to the Whistleblower webpage at www.dodig.mil/programs/whistleblower.

For more information about DoD IG reports or activities, please contact us:

Congressional Liaison
Congressional@dodig.mil; 703.604.8324

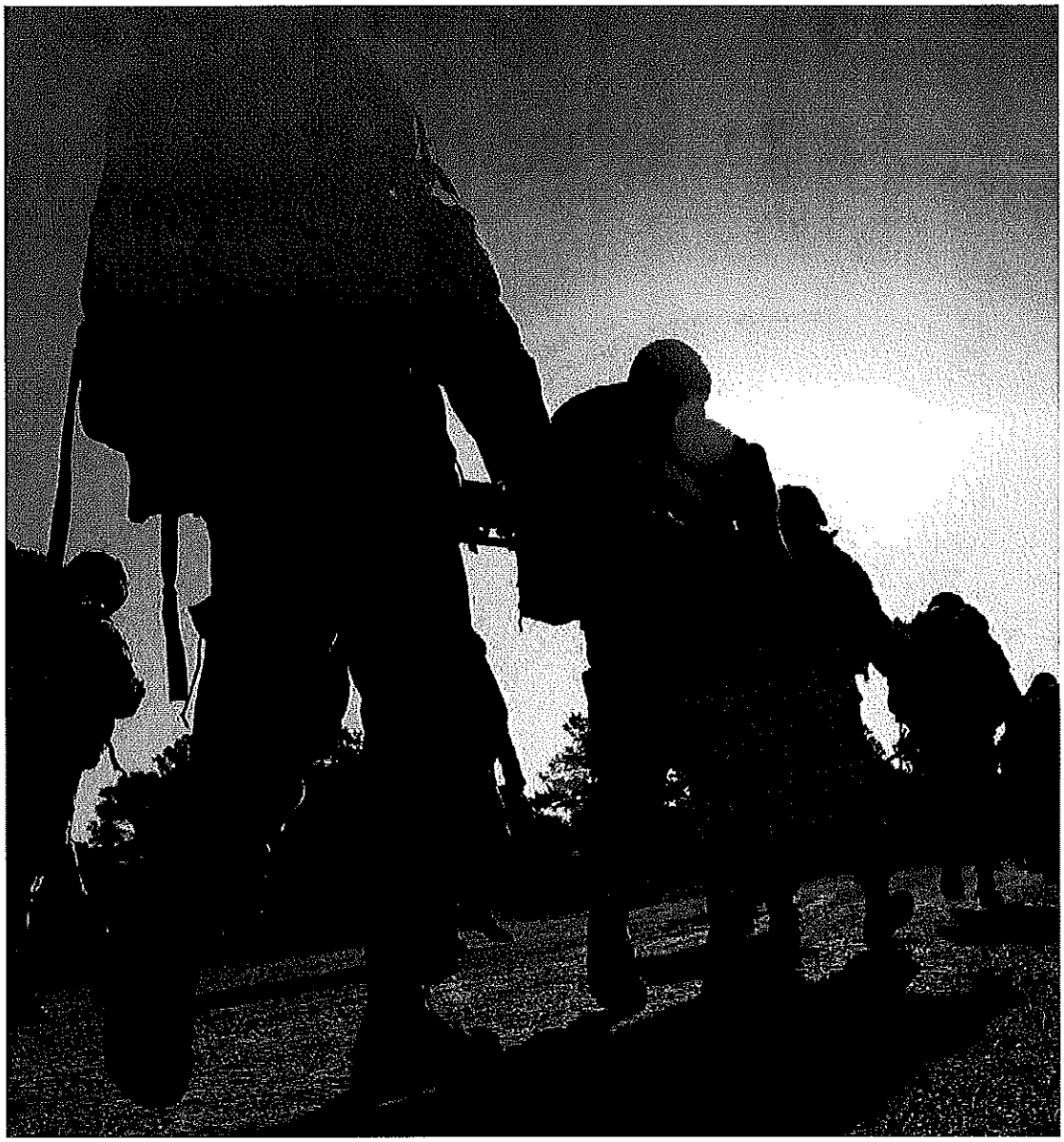
DoD Hotline
1.800.424.9098

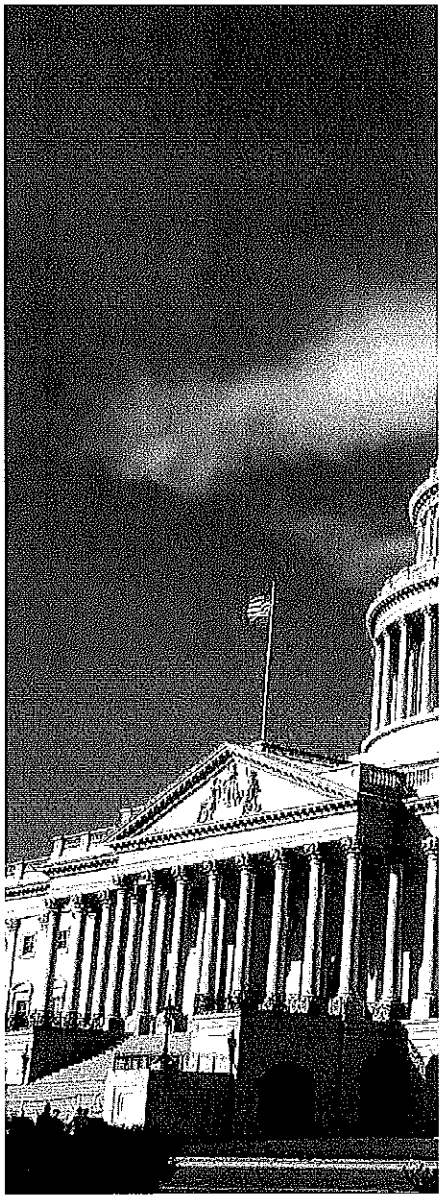
Media Contact
Public.Affairs@dodig.mil; 703.604.8324

Monthly Update
dodigconnect-request@listserve.com

Reports Mailing List
dodig_report-request@listserve.com

Twitter
twitter.com/DoD_IG





DEPARTMENT OF DEFENSE | INSPECTOR GENERAL

4800 Mark Center Drive
Alexandria, VA 22350-1500
www.dodig.mil
Defense Hotline 1.800.424.9098