Audit Report No. D-2011-020 November 29, 2010

Inspector General

United States Department of Defense

DOD Controls Over Information Placed on Publicly Accessible Web Sites Require Better Execution

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

AFIS	American Forces Information Service
DEPSECDEF	Deputy Secretary of Defense
FOUO	For Official Use Only
IOSS	Interagency Operations Security Support
JWRAC	Joint Web Risk Assessment Cell
OPSEC	Operations Security
PII	Personally Identifiable Information

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

November 29, 2010

MEMORANDUM FOR ASSISTANT SECRETARY OF DEFENSE FOR NETWORKS AND INFORMATION INTEGRATION/DOD CHIEF INFORMATION OFFICER
ASSISTANT SECRETARY OF DEFENSE FOR PUBLIC AFFAIRS
ASSISTANT SECRETARY OF THE AIR FORCE FOR FINANCIAL MANAGEMENT AND COMPTROLLER

SUBJECT: DOD Controls Over Information Placed on Publicly Accessible Web Sites Require Better Execution (Report No. D-2011-020)

We are providing this report for your review and comment. We considered management comments on a draft of this report when preparing the final report. When sensitive information on DOD publicly accessible Web sites is retrieved by adversaries, it places DOD personnel and missions at risk. We evaluated management of 436 public Web sites for their compliance with mandatory content and approval procedures and training requirements. We determined that DOD Web site administrators are not properly managing their Web sites.

DOD Directive 7650.3 requires that all recommendations be resolved promptly. Comments from the Assistant Secretary of Defense for Networks and Information Integration/DOD Chief Information Officer, the Assistant Secretary of Defense for Public Affairs, Air Force Director Network Services Office of Information Dominance and Chief Information Officer, and the Vice Director Defense Information Systems Agency were generally responsive. As a result of management comments and suggestions on the draft report, we revised Recommendation A.2 to better align with the impending Instruction. We request that the Assistant Secretary of Defense for Networks and Information Integration/DOD Chief Information Officer provide additional comments on the final report by December 22, 2010. See Recommendations Table on page ii of this report.

If possible, send a .pdf file containing management comments to audros@dodig.mil. Copies of management comments must have the actual signature of the authorizing official. We are unable to accept the /Signed/ symbol in place of the actual signature. If you arrange to send classified comments electronically, you must send them over the SECRET Internet Protocol Router Network (SIPRNET).

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: DOD Controls Over Information Placed on Publicly Accessible Web Sites Require Better Execution

What We Did

We performed the audit in response to a September 25, 2008, request by the then Deputy Secretary of Defense for the DOD OIG to address concerns that sensitive information continues to be found on DOD public Web sites. We evaluated the management of 436 public Web sites for their compliance with mandatory content and approval procedures and training requirements. We also reviewed 3,211 DOD-identified Web sites for public accessibility.

What We Found

DOD 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, sensitive information continues to be posted to DOD public Web sites, putting DOD missions and personnel at risk. We found:

- 43 of 73 DOD organizations failed to respond to the Deputy Secretary of Defense requirement to certify their Web sites.
- Web site administrators for 207 out of 436 public Web sites of DOD Components failed to implement proper content review and approval procedures.
- 452 of 470 DOD Web site administrators reviewed did not receive the required Web operations security training.

DOD is not maintaining a Department-wide inventory of all its public Web sites as required by law. DOD stopped funding and discontinued its central Web site inventory system in 2006. A total of 791 Web sites identified by DOD in their inventories as publicly accessible were actually password-protected or nonexistent. Furthermore, individual organizations are not maintaining accurate inventories of Web sites and cannot ensure that all information posted on public Web sites has received proper review.

What We Recommend

Among other recommendations, we recommend the Assistant Secretary of Defense for Public Affairs [ASD (PA)] within 120 days develop and maintain a DOD inventory of all publicly accessible Web sites. We recommend the Assistant Secretary of Defense for Networks and Information Integration/DOD Chief Information Officer [ASD (NII)/DOD CIO] within 120 days:

- Require heads of DOD Components to certify annually that a documented Web review and approval process has been developed and implemented.
- Require all Web administrators to receive the proper Web operations security training.
- Require Military Services to maintain an integrated registration system within the DOD's central registration system.

Management Comments and Our Response

Comments from the ASD (NII)/DOD CIO, ASD (PA), Air Force Director Networks Services Office, and Vice Director, Defense Information Systems Agency (DISA) generally agreed with and responded to our recommendations. However, the ASD (NII)/DOD CIO's comment was only partially responsive to Recommendation A.2. We partially agreed with the ASD (NII)/DOD CIO and revised Recommendation A.2 to better align with the impending Instruction. We request that the ASD (NII)/DOD CIO provide additional comments on Recommendation A.2. We request management provide comments by December 22, 2010. Please see the recommendations table on the back of this page.

Recommendations Table

Management	Recommendations Requiring Comment	No Additional Comments Required
Assistant Secretary of Defense for Networks and Information Integration/DOD Chief Information Officer	A.2.a, A.2.b, A.2.c, A.2.d, A.2.e ,	A.1, A.3, B.2.a, B.2.b, B.2.c, B.2.d
Assistant Secretary of Defense for Public Affairs		B.1
Secretary of the Air Force		A.5
Director, Joint Web Risk Assessment Cell		A.4

Please provide comments by December 22, 2010.

Table of Contents

Results in Brief i

Introduction 1

Objectives 1
Background 1
Review of Internal Controls 2

Finding A. Weaknesses in DOD's Web Site Review and Approval Process 3

DOD Organizations' Certification of Publicly Accessible Web Sites Needs Improvement 4
Inconsistent Web Site Content Review and Approval Process 5
Web Site Administrators Lack Web Operations Security Training 8
Availability of Operations Security Training Courses 10
Management Oversight 10
Web Risk Assessment Cell Continues to Find Sensitive Information on DOD Publicly Accessible Web Sites 10
Management Comments on the Finding and Our Response 11
Recommendations, Management Comments, and Our Response 12

Finding B. DOD Lacks a Complete Inventory for Publicly Accessible Web Sites 15

DOD Did Not Maintain a Central Web Site Inventory of All Publicly Accessible Web Sites 16
Inventories of DOD Organizations' Public Web Sites 16
Management Actions 19
Recommendations, Management Comments, and Our Response 20

Appendices

A. Scope and Methodology 23
B. Public Web Site Certification Compliance 26
C. Interagency Operations Security Support Staff FY 2010 Training Schedule for Courses OPSE-1500 and OPSE-3500 32
D. Management Comments on the Finding and Our Response 33
E. Criteria for DOD Web Site Inventory 36
F. Deputy Secretary of Defense Memorandum for Office of the Inspector General 38

Management Comments

Assistant Secretary of Defense for Networks and Information Integration/ DOD Chief Information Officer 39
Assistant Secretary of Defense for Public Affairs 43
Secretary of the Air Force 45
Defense Information Systems Agency (Joint Web Risk Assessment Cell) 47

Introduction

Objectives

In a September 25, 2008, memorandum to the DOD Office of the Inspector General, the then Deputy Secretary of Defense (DEPSECDEF), outlined his concerns that, "sensitive information frequently can still be found on publicly accessible Web sites." To address these concerns, the then DEPSECDEF requested the Inspector General to include this matter when executing his oversight responsibility.

As a result, the DOD Office of the Inspector General announced an audit of controls over information contained on DOD publicly accessible Web sites. The overall objective was to determine whether DOD Components are in compliance with Web site security policy. Specifically, we determined whether DOD Components have controls and processes in place to ensure review and approval of all information posted to publicly accessible Web sites before posting. We also determined whether personnel responsible for review of information for Web posting have received Web operations security (OPSEC) training. See Appendix A for a discussion of the scope and methodology and prior audit coverage.

Background

DOD publicly accessible Web sites are unrestricted by password or public key infrastructure user authorization and can be accessed directly from the Internet by members of the public. Due to extensive use of Web archiving tools, once information is posted to publicly accessible Web sites, it is captured and distributed throughout the World Wide Web. Preventing the disclosure of sensitive information requires proper review of that information prior to posting.

On January 14, 2003, the then Secretary of Defense issued a memorandum to DOD Components concerning discrepancies in Web site OPSEC. The memorandum directed heads of DOD Components to ensure Web site owners take responsibility for all content posted to their organizations' Web sites. It directed Web site owners to redouble their efforts to ensure that only the information necessary to accomplish their missions be posted to publicly accessible Web sites. This is especially critical in light of the Al Qaeda training manual recovered in Afghanistan that, when translated, states, "Using public sources openly and without resorting to illegal means, it is possible to gather at least 80 percent of information about the enemy."

Joint Web Risk Assessment Cell

The Joint Web Risk Assessment Cell (JWRAC), a DEPSECDEF-chartered cell within the Defense Information Systems Agency, is responsible for conducting OPSEC assessments and trend analyses of content and data on DOD publicly accessible Web sites. JWRAC reviews Web sites for compliance with existing DOD Web policy and directs remediation actions to bring Web sites into compliance. The JWRAC performs analyses of the data to determine any existing OPSEC risks that may pose an immediate or potential threat to

warfighters. According to officials, JWRAC conducts analyses of organization Web sites on an annual schedule and by request from DOD organizations.

Review of Internal Controls

We determined that internal control weaknesses existed in DOD as defined by DOD Instruction 5010.40, "Managers' Internal Control (MIC) Program Procedures," January 4, 2006. DOD Components lacked processes for ensuring:

- administrators of DOD public Web sites implement proper content review procedures;
- administrators of public Web Site[1] receive the required Web OPSEC training; and
- an accurate inventory of DOD publicly accessible Web sites as required by public law, the Office of Management and Budget, and DOD policy.

Therefore, DOD does not have reasonable assurance that all DOD Components are implementing controls for the review and approval of content prior to posting to DOD publicly accessible Web sites. Also, DOD did not ensure Components were preventing the posting of sensitive and/or Personally Identifiable Information (PII) on DOD publicly accessible Web sites.

We also determined that some Army activities failed to include the management of Army publicly accessible Web sites as a part of their internal control reviews. We further determined that internal control guidance in the Navy, Air Force, and Marine Corps did not mandate review of each Service's public Web sites. Implementing the recommendations in this report will correct DOD organizations' failure to properly review and approve information placed on publicly accessible Web sites and correct the site registration deficiencies for DOD Services, agencies, and combatant commands. We will provide a copy of the report to the senior officials responsible for internal controls at the Army, Navy, Air Force, Marine Corps, and DOD agencies and other offices listed in Appendix A.

[1] DOD Web site administrators include: OPSEC managers, Web Managers, webmasters, public affairs specialists, and anyone who reviews information prior to posting on publicly accessible Web sites.

Finding A. Weaknesses in DOD's Web Site Review and Approval Process

Many DOD organizations did not comply with DOD Web Site policy and procedures for publicly accessible Web site content review and approval. Specifically:

- Of 73 DOD organizations identified, 43 (59 percent) did not certify, as required, that they have mandatory content review and approval procedures in place for information posted to publicly accessible Web sites.
- Of 436 publicly accessible Web sites reviewed, 207 (47 percent) did not have documented review and approval procedures, or existing procedures did not fully comply with requirements.
- Of 470 Web site administrators reviewed, 452 (96 percent) had not received required OPSEC 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 cannot ensure that all information posted to DOD publicly accessible Web sites has been properly reviewed and approved. In fact, over the past 3 years, DOD's JWRAC has identified For Official Use Only (FOUO) information, PII, and limited-distribution information posted on DOD publicly accessible Web sites. Improper postings increase the risk of potentially harmful disclosure of information related to DOD personnel and missions.

Criteria for Web Site Administration

DOD's "Web Site Administration Policies and Procedures," November 25, 1998, updated January 11, 2002 (Web site administrative guidance), prescribes the process for content review and approval of information to be placed on DOD publicly accessible Web sites. This guidance requires heads of DOD Components and other organizations to establish a content review and approval process for all information prior to posting on publicly accessible Web sites.

DEPSECDEF Memorandum, "DOD Web Site Security Policy Compliance," September 25, 2008, states that DOD organizations must ensure information placed on DOD publicly accessible Web sites is compliant with the DOD Web site administrative guidance. Additionally, personnel trained in Web OPSEC must review information placed on DOD publicly accessible Web sites for security concerns. The DEPSECDEF Memorandum also requires DOD organizations to either certify an established process for content review and approval or submit a plan of actions and milestones for implementing a content review and approval process, and to certify that individuals involved in the process have received Web OPSEC training. On August 6, 2006, the Vice Chairman of the Joint Chiefs and the DEPSECDEF issued a joint message, "Information Security/Web Sites Alert," that required all command OPSEC managers,

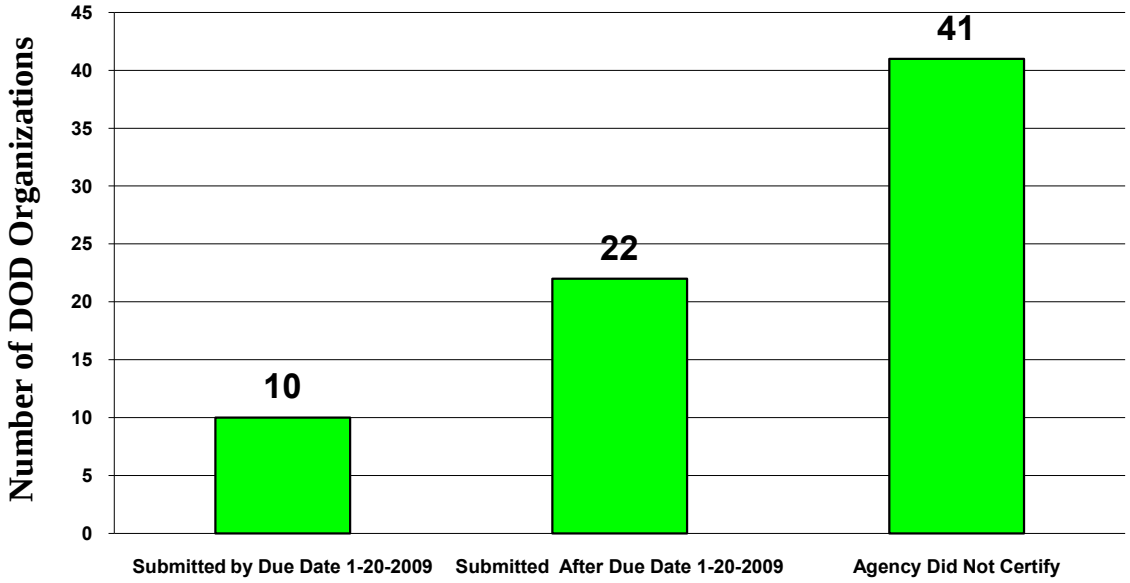
webmasters, and public affairs specialists who review information for Web posting to receive Web OPSEC training.

The Under Secretary of Defense for Intelligence is responsible for overseeing the DOD OPSEC program. OPSEC reviews are central to identifying and safeguarding critical information. Therefore, critical information available on publicly accessible Web sites is an OPSEC concern. Duties of OPSEC managers are consistent with Web site administrator responsibilities, which include identifying and protecting unclassified information that may individually or in the aggregate lead to compromise of classified information and sensitive activities.

DOD Organizations' Certification of Publicly Accessible Web Sites Needs Improvement

The September 25, 2008, DEPSECDEF Memorandum required DOD organizations to certify the implementation of public Web sites content review and approval procedures or provide a plan of actions and milestones. We identified 73 DOD organizations that operate DOD publicly accessible Web sites. Of the 73 organizations, 41 failed to certify or submit a plan of actions and milestones as required by the DEPSECDEF Memorandum. Of the 32 organizations that submitted a response, 10 submitted on or before the revised January 20, 2009, due date, and 22 submitted after. Nine of 22 DOD organizations submitted Web site certifications or provided a plan of actions and milestones after being contacted by the audit team. See Figure 1 below[2] and Appendix B.

Figure 1. Public Web Site Certification Compliance



[2] Figure 1 and Appendix B include organizations submitted prior to August 30, 2010.

Eleven of the 32 DOD organizations submitted responses that did not contain all the required information. Some heads of DOD Components failed to certify review and approval procedures and training for their subordinate organizations; other heads of DOD Components failed to specify to which subordinate organizations (agencies and organizations) the certification pertained. The remaining 21 organizations submitted responses that included all the required information for review and approval, training, and plan of actions and milestones when necessary.

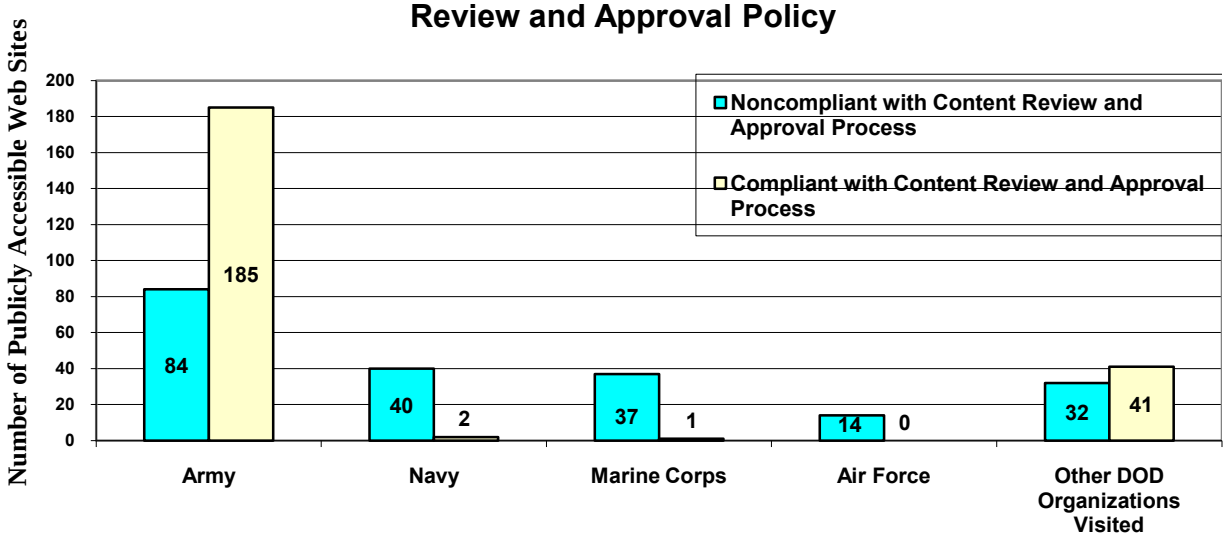
Personnel from the Office of the Assistant Secretary of Defense Networks and Information Integration/DOD Chief Information Officer stated their intention is to revise the DOD Web site administrative guidance and reissue it as a DOD instruction to clarify and provide more detailed procedures for Web site review and approval. On November 9, 2009, they provided a draft copy of the revision to the audit team. The draft contains necessary Internet-based controls that should assist with preventing dissemination of inappropriate information over DOD Web-based applications.

Inconsistent Web Site Content Review and Approval Process

DOD organizations that administer publicly accessible Web sites were not adequately implementing content review and approval procedures before posting information. Specifically, 207 of 436 publicly accessible Web sites reviewed were noncompliant with the DOD Web site administrative guidance and the DEPSECDEF Memorandum sent to all DOD Components. (See Figure 2.) These policies require organizations to maintain consistent processes ensuring the review and approval of all information posted to publicly accessible Web sites. Although several organizations established local policies incorporating DOD Web site administrative guidance and the DEPSECDEF Memorandum, they did not effectively enforce compliance with the policies.

These policies require organizations to maintain consistent processes ensuring the review and approval of all information posted to publicly accessible Web sites.

Figure 2. DOD Organizations' Compliance With Content Review and Approval Policy



Below are the specific findings regarding management of publicly accessible Web sites for Military Services and other DOD organizations.

Army Site Visit Results

We interviewed 148 Army Web administrators responsible for managing 269 Army public Web sites and determined that Army Medical Command public Web site managers complied with DOD Web site administrative guidance for the 185 public Web sites they managed. Conversely, Web site managers for 84 other Army public Web sites were noncompliant. Specifically, managers for 50 of the 84 Web sites lacked documented review and approval procedures. Managers for the remaining 34 Web sites had content review and approval procedures, but the procedures were inconsistent with the DOD policy and failed to fully address:

- review of sensitive information to include data labeled FOUO;
- review of information in the aggregate; and
- review of PII for members of deployable units.

Army Regulation 25-1, "Army Knowledge Management and Information Technology," December 4, 2008, requires public affairs officers and other appropriate designees to review and approve Web content before posting to the Internet for the general public and ensure content meets requirements set forth in DOD Web site administrative guidance. Although we found no PII on any of the Army public Web sites we reviewed, Army Web administrators responsible for 84 Web sites did not comply with DOD and Army policies and procedures for managing their Web sites.

Navy and Marine Corps Site Visit Results

Secretary of the Navy Instruction 5720.47B, "Department of the Navy Policy for Content of Publicly Accessible World Wide Web Sites," December 28, 2005, requires Navy and Marine Corps activities to maintain publicly accessible Web sites that (1) implement and administer a comprehensive Web site management program; (2) develop local procedures

for the approval of information posted on publicly accessible Web sites; and (3) ensure posted information meets requirements set forth in DOD Web site administrative guidance.

Navy

We interviewed 75 Navy Web site managers responsible for managing 42 public Web sites and determined content review and approval processes for 40 public Web sites were noncompliant with DOD Web site administrative guidance. The 40 public Web sites we reviewed had content review and approval procedures, but the procedures did not fully address requirements for reviewing:

- sensitive information, to include data labeled FOUO as required by DOD policy;
- information in the aggregate; and
- PII such as family member information, date and place of birth, and duty location.

We found PII on seven Navy public Web sites. For example, one Web site contained individuals' dates and places of birth, spouses' names, residences, and dependents' names. After we notified the managers of the noncompliance, they removed the PII from the seven public Web sites we identified.

Marine Corps

We interviewed 17 Marine Corps Web site managers responsible for managing 38 public Web sites. The content review and approval process for Web site managers of 37 public Web sites did not comply with DOD Web site administrative guidance. Thirty-seven public Web sites we reviewed provided content review and approval procedures, but the procedures did not fully address requirements for reviewing:

- sensitive information, to include data labeled FOUO as required by DOD policy;
- information in the aggregate; and
- PII.

We found PII on 12 Marine Corps public Web sites. For example, the Web sites contained individuals' dates and places of birth, spouses' names, residences, dependents' names, and other PII. After we notified the Marine Corps public Web site managers of the noncompliance, they removed PII from 11 of the 12 public Web sites. The Web manager for the remaining Web site continues to evaluate the occurrence of PII on that Web site.

Air Force Site Visit Results

All 14 Air Force public Web sites we reviewed were managed and operated under the Air Force Public Information Management System. Air Force public Web site managers must sign a memorandum of understanding to access the Air Force Public Information Management System and register their public Web sites with the Air Force Public Affairs Agency. Only 1 of the 14 public Air Force Web sites we reviewed had established local plans, policies, and procedures for management of their Web sites as required by the memorandum of understanding. The operating instructions for the Web site with

documented content management procedures were outdated and failed to fully address DOD Policy requirements for reviewing:

- sensitive information, to include data labeled FOUO as required by DOD policy;
- information in the aggregate; and
- PII.

Although we found no PII on any of the 14 Air Force public Web sites, content managers for the 13 public Web sites without documented local procedures provided inconsistent approaches to Web site content management. Web site managers stated that the same individual could create, review, and approve content for public release, but some managers separated the duties. Separation of duties is a fundamental principle of various regulatory mandates, such as Sarbanes-Oxley and the Gramn-Leach-Biliey Act.

Air Force Instruction 33-129, "Web Management and Internet Use," February 3, 2005, defines the roles and responsibilities of personnel maintaining Air Force public Web sites. It designates the Secretary of the Air Force Office of Public Affairs to develop a review process for posting information on publicly accessible Web sites. Further, Air Force Instruction 35-101, "Public Affairs Policies and Procedures," November 29, 2005, mandates a security and policy review to ensure the material proposed for public release through Web sites is accurate, contains no classified material, and does not conflict with established Air Force, DOD, or U.S. Government policy. Near the completion of our audit, the Air Force issued Air Force Instruction 35-107, "Public Web Communications," October 21, 2009, and is currently working to refine its guidance.

Other DOD Organization Site Visit Results

We interviewed public Web site managers from 12 Defense Agencies, 5 Office of the Secretary of Defense offices, and 1 combatant command, which in combination, are responsible for managing 73 DOD public Web sites. Of the 73 public Web sites reviewed, 41 were compliant, and 32 were noncompliant with DOD Web site administrative guidance. Managers for 17 of the 32 Web sites lacked documented review and approval procedures. Web site managers for the remaining 15 Web sites provided content review and approval procedures that failed to fully address the following process requirements for:

- overall review before posting unmarked (FOUO) content;
- clearance review;
- review of content for sensitivity and distribution/release controls;
- sensitivity of information in the aggregate; and
- required training and knowledge of personnel.

Web Site Administrators Lack Web Operations Security Training

DOD organizations failed to ensure all DOD Web site administrators received the required training, and they implemented inconsistent procedures that omitted requirements for Web OPSEC training. On August 6, 2006, the Vice Chairman of the Joint Chiefs and the Deputy Secretary of Defense issued a joint message, "Information

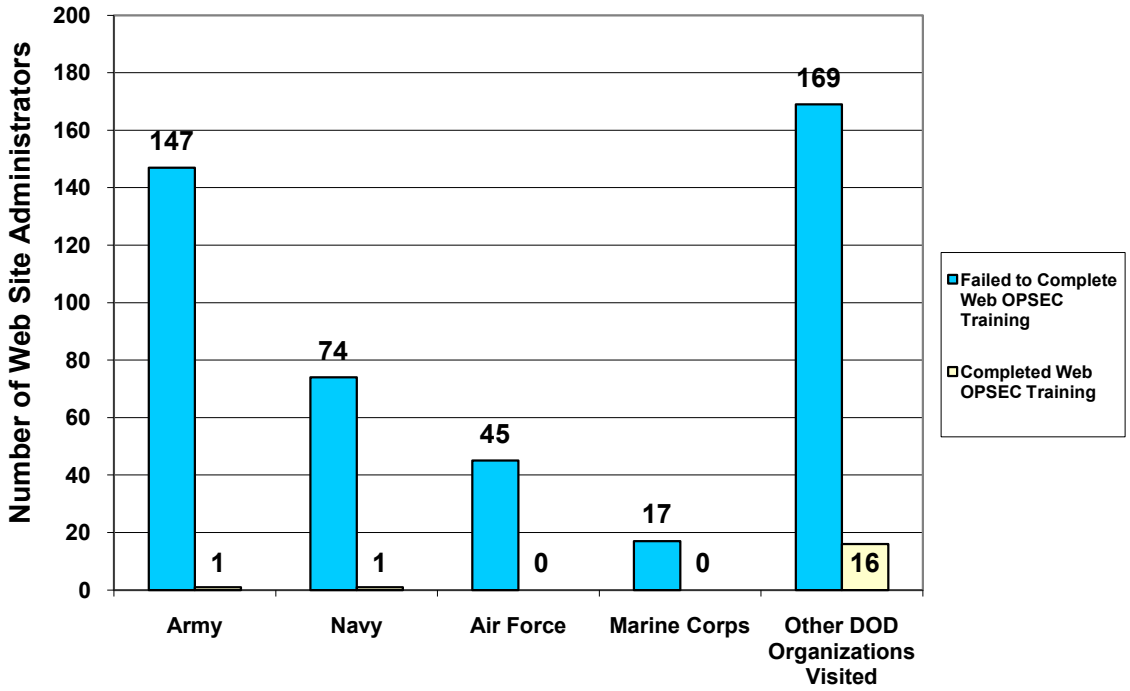
Security/Web Sites Alert." The joint message requires all command OPSEC managers, webmasters, and public affairs specialists who review information for Web posting to receive Web OPSEC training. The message does not specify the frequency of the training. Web OPSEC training is critical to ensuring the identification, proper control, and proper posting of sensitive information to DOD public Web sites. Appropriate Web OPSEC training enhances the ability of content review participants to perform essential Web site administration tasks and manage the information in a responsible and secure manner.

We found 452 of 470 DOD public Web site administrators did not complete required Web OPSEC training: broken down by Service, 147 of 148 Army, 74 of 75 Navy, 45 of 45 Air Force, 17 of 17 Marine Corps, and 169 of 185 other DOD organizations' Web site administrators did not meet DOD OPSEC training requirements.

DOD public Web site administrators stated they were unaware of the Web OPSEC training requirement.

Web site administrators responsible for content review and approval duties cited on-the-job training and knowledge acquired over the years as adequate preparation for executing the required review and approval procedures. Web site administrators stated they were unaware of the Web OPSEC training requirement. Other Web site administrators pointed to the lack of available Web OPSEC training classes and funding shortfalls that precluded travel to obtain required OPSEC training. See Figure 3.

Figure 3: Web Operational Security Training Compliance for DOD Organizations



Availability of Operations Security Training Courses

The Interagency OPSEC Support Staff (IOSS) sponsors Web OPSEC training through both classroom and e-learning courses. Since April 2007, the IOSS has offered an adjunct faculty option allowing Federal organizations to certify personnel to teach Web OPSEC courses at the local command level. As of December 2009, no DOD organizations had taken advantage of the opportunity to certify adjunct personnel to teach Web OPSEC courses at their respective DOD organizations. The IOSS reports that they have sufficient resources to accommodate the demand for the Web OPSEC training for all agencies. Appendix C provides a schedule of available Web OPSEC courses.

Management Oversight

Incentive to Comply With DOD Policy

Ultimately, DOD Web site administrators lack the incentive to ensure the implementation of proper Web site management procedures and internal controls. For instance, there were no penalties for noncompliance with public Web site guidance. Management took no action to determine if sensitive information was posted to DOD public Web sites. In fact, few Web site administrators were aware of the need for a documented process for accountability and authorization prior to posting. Most of the organizations did not maintain records for tracking the posting of sensitive or personal information over the last 5 years. If such incidents should occur, organizations can withdraw the information from a Web site; however, Web archiving tools can still retrieve the information.

Dissemination of Guidance

DOD Web administrators stated that the DEPSECDEF Memorandum was not disseminated to their offices. A total of 168 Web administrators responsible for managing 116 Web sites reported that they received neither the DEPSECDEF Memorandum nor other Web site guidance and were unaware of the Web OPSEC training certification requirement contained in the guidance. Inadequately trained DOD Web site administrators had insufficient knowledge for assessing the nature of security risks associated with reviewing and approving information before posting.

DOD Organization Internal Reviews

DOD organizations failed to conduct internal reviews to ensure that DOD Web site administrators were implementing content review and approval procedures as required. Organizations' management control plans did not include controls for the review of Web site content review and approval procedures. The absence of internal reviews increases the potential for posting inappropriate content.

Web Risk Assessment Cell Continues to Find Sensitive Information on DOD Publicly Accessible Web Sites

DOD approved the establishment of the JWRAC on February 12, 1999. Its mission is to provide analyses of Web site risk and operations security. From 2007 through 2009,

JWRAC identified sensitive information posted to multiple DOD publicly accessible Web sites. For example, improper posting of sensitive information related to 702 FOUO documents, 241 occurrences of PII including social security numbers, and 1,124 postings of information designated as "for limited distribution."

All DOD Components that have established publicly accessible Web sites are responsible for ensuring that the information published on these sites does not compromise national security or place DOD personnel at risk. DOD Component heads are required to enforce the application of comprehensive risk management procedures ensuring that mission benefits gained by using the Web are balanced against the potential security and privacy risks created when aggregated DOD information is more readily accessible over the World Wide Web.

Service Web Risk Assessment Cells

The Army, Navy, and Marine Corps established Web risk assessment cells to conduct assessments of their publicly accessible Web sites, notify commands of Web site violations, and ensure compliance with DOD policy requirements. The Air Force is discussing establishing a Web risk assessment cell, but has not set a firm date by which to make a decision. Given the continued findings of sensitive information posted to DOD public Web sites and the current inaccuracies of Services' Web site inventories, the Air Force should move forward without further delay and establish a Web risk assessment cell to assess risk and compliance with DOD OPSEC and privacy requirements for its public Web sites.

Upon establishment of a DOD central Web site registration system, personnel working in Service Web risk assessment cells should routinely search for unregistered DOD Web sites. This practice would identify unregistered sites that should be blocked until they are registered.

Conclusion

Many DOD organizations failed to implement the proper public Web site content review and approval procedures for reducing the risk of posting sensitive information on DOD public Web sites. DOD Web site administrators often maintained inconsistent levels of information content review, were unaware of DOD Web site policies, and received little or no proper training. DOD organizations failed to submit and submitted incomplete Web site certifications. DOD failed to implement a followup process to verify Components compliance with the Web site certification reporting requirement. Proper implementation and strengthening of Web site policies will reduce the risk of posting sensitive information to DOD public Web sites and detrimental impacts to DOD missions and personnel.

Management Comments on the Finding and Our Response

Please see Appendix D for complete management comments and audit responses on the finding.

Recommendations, Management Comments, and Our Response

Revised Recommendation

Recommendation A.2 has been revised in response to comments from the Assistant Secretary of Defense for Networks and Information Integration/DOD Chief Information Officer's and Vice Director, Defense Information Systems Agency, to better align with the impending issuance of DOD Instruction 8430.aa.

A.1. We recommend the Assistant Secretary of Defense for Networks and Information Integration/DOD Chief Information Officer re-emphasize to all DOD Components the DOD Web Site Administration Policy and Procedures requirements to develop review and approval procedures for information posted to publicly accessible Web sites.

Assistant Secretary of Defense for Networks and Information Integration/DOD Chief Information Officer Comments

The Deputy Chief Information Officer, responding for the Assistant Secretary of Defense for Networks and Information Integration/DOD Chief Information Officer agreed, stating the Assistant Secretary of Defense for Networks and Information Integration/DOD Chief Information Officer will, in coordination with the offices of primary responsibility for information release to the public and operations security, the Director of Administration & Management, and the Under Secretary of Defense for Intelligence, respectively, reemphasize and fully describe current review, clearance, and authorization policies and procedures in the forthcoming DOD Instruction 8430.aa, "DoD Internet Services and Internet-Based Capabilities."

Our Response

The Deputy Chief Information Officer's comments are responsive and meet the intent of our recommendations. No further comments are required.

A.2. We recommend the Assistant Secretary of Defense for Networks and Information Integration/DOD Chief Information Officer, within 120 days, develop and issue a DOD Instruction that requires heads of DOD Components to annually assess and document, with signature, DOD Internet services and use of Internet-based capabilities for compliance with applicable policies and procedures to include, at minimum, that:

a. Documented review and approval processes are implemented for all public Web sites and copies of the documentation are filed with the DOD Component CIOs,

b. All Web site administrators have received the proper Web OPSEC training,

c. All Web site administrators submit a plan of actions and milestones to the responsible head of DOD Component for all public Web sites that have not implemented a documented content review and approval process, and for those personnel who have not received the proper Web OPSEC training;

d. Web sites and associated processes not brought into compliance with the instruction are shut down or disconnected; and

e. Joint and Service Web risk assessment cells conduct routine searches for unregistered DOD Web sites.

Assistant Secretary of Defense for Networks and Information Integration/DOD Chief Information Officer Comments

The Deputy Chief Information Officer, responding for the Assistant Secretary of Defense for Networks and Information Integration/DOD Chief Information Officer, agreed with the original recommendation stating that the annual policy compliance assessment and corrective action will be mandated in the impending DOD Instruction 8430.aa. In addition, the Deputy Chief Information Officer suggested that the recommendation be revised to better align with the Instruction and provide a more efficient process.

Our Response

The Deputy Chief Information Officer's comments are partially responsive. Due to the revisions, we revised recommendation A.2 to include suggestions from the Deputy Chief Information Officer and the Vice Director, Defense Information Systems Agency. We request the Assistant Secretary of Defense for Networks and Information Integration/DOD Chief Information Officer provide comments for recommendations A.2.a, A.2.b, A.2.c, A.2.d and A.2.e

A.3. We recommend the Assistant Secretary of Defense for Networks and Information Integration/DOD Chief Information Officer develop enforcement procedures for noncompliance with the annual certification requirements.

Assistant Secretary of Defense for Networks and Information Integration/DOD Chief Information Officer Comments

The Deputy Chief Information Officer, responding for the Assistant Secretary of Defense for Networks and Information Integration/DOD Chief Information Officer, agreed. The forthcoming DOD Instruction 8430.aa mandates that Web sites and associated processes comply with the instruction.

Our Response

The Deputy Chief Information Officer's comments are partially responsive. Management comments do not address the development of enforcement actions for non-compliance with annual assessment requirements. However, management comments and suggestions for Recommendation A.2 establish an annual Web site assessment

requirement that, if not complied with, will result in DOD Web sites being shut down or disconnected. No further comments are required.

A.4. We recommend the Director Joint Web Risk Assessment Cell expand distribution of its annual OPSEC and threat assessment reports on DOD public Web sites to the Assistant Secretary of Defense for Networks and Information Integration/DOD Chief Information Officer and the Office of the Under Secretary of Defense for Intelligence.

Defense Information Systems Agency Comments

The Vice Director, Defense Information Systems Agency agreed. The Vice Director stated that the Joint Web Risk Assessment Cell will expand the distribution of its annual OPSEC and threat assessments report on DOD public Web sites to the Assistant Secretary of Defense for Networks and Information Integration/DOD Chief Information Officer and the Office of the Under Secretary of Defense for Intelligence.

Our Response

The Vice Director's comments are responsive and meet the intent of our recommendations. No further comments are required.

A.5. We recommend the Secretary of the Air Force within 90 days develop a process to review OPSEC threat and vulnerability risks for all its public Web sites.

Secretary of the Air Force Comments

The Director of Network Services Office of Information Dominance and Chief Information Officer, responding for the Secretary of the Air Force, agreed. The Director stated the Air Force Telecommunications Monitoring Assessment Program will be utilized to conduct OPSEC vulnerability assessments for release of information to the public via Internet-base Capabilities. Additionally, policy is being developed within AFI 10-701, Operations Security (OPSEC), to address the lack of Air Force directive regarding OPSEC reviews conducted prior to releasing information, as well as training for personnel reviewing information.

Our Response

The Director of Network Services Office of Information Dominance and Chief Information Officer's comments are responsive and meet the intent of our recommendations. No further comments are required.

Finding B. DOD Lacks a Complete Inventory for Publicly Accessible Web Sites

DOD did not comply with requirements to maintain a central Web site registration system. This occurred because, after the disestablishment of the office of primary responsibility under the 2005 Base Realignment and Closure process, the responsibility to operate and maintain a central registration system was not reassigned. In addition, although the Military Services and other DOD organizations had Web site inventory systems, the systems were not accurate or current. Without an accurate inventory system, DOD organizations cannot account for the proper management of all DOD's publicly accessible Web sites or reduce the risk of posting personally identifiable, FOUO, and other sensitive information to DOD publicly accessible Web sites.

Criteria for DOD Web Site Inventory

Public Law 104-13, "Paper Reduction Act of 1995," Chapter 35, Section 3506 requires each agency to maintain a current and complete inventory of its information resources (including Web sites) to fulfill the requirements of the Government Information Locator Service. Further, Section 3511 requires each agency to establish and maintain its own information locator service as a component of, and to support the operation of, the Government Information Locator Service. Public Law 107-347, 107th Congress, "E -Government Act of 2002," December 17, 2002, amended Public Law 104-13 to require heads of Federal agencies to prepare and maintain an inventory of information resources, including public Web sites.

Office of Management and Budget policy requires agencies to establish a public Web site inventory. Office of Management and Budget Circular A-130, "Management of Federal Information Resources," states that agencies must establish and maintain inventories of all agency information dissemination products[3] by implementing a management system. Also, Office of Management and Budget M-05-04, "Policies for Federal Agency Public Web Sites," December 17, 2004, requires agencies to establish and maintain inventories for information dissemination products, including public Web sites.

DOD Web site administrative guidance requires the Assistant Secretary of Defense for Public Affairs to provide and maintain a central Web site registration system. Military Services must establish and maintain their own registration systems and integrate their systems within the DOD's central system. To that end, the Army, Navy, Air Force, and Marine Corps each have an individual policy and individual instructions requiring Web site registration.

---

[3] Under Office of Management and Budget Circular A-130, the term "information dissemination product" means any book, paper, map, machine-readable material, audiovisual production, or other documentary material, regardless of physical form or characteristic, disseminated by an agency to the public.

DOD Web site administrative guidance requires the Assistant Secretary of Defense for Networks and Information Integration/DOD Chief Information Officer to approve and publish DOD instructions to guide, direct, or help Web site activities; and coordinate training guidance for requirements addressing information security on the Web.

DOD Did Not Maintain a Central Web Site Inventory of All Publicly Accessible Web Sites

The DOD did not comply with requirements to maintain an inventory of all DOD public Web sites. Office of Management and Budget policies that implement the provisions of Public Laws 104-13 and 107-347 require agencies to prepare and maintain an inventory of information resources to include publicly accessible Web sites. DOD implemented these OMB policies through its DOD Web site administrative guidance.

In 1998, DOD issued the Web site administrative guidance requiring the Assistant Secretary of Defense for Public Affairs to establish and maintain a DOD central Web site registration system. In November 2000, the American Forces Information Service (AFIS), under the authority of the Assistant Secretary of Defense for Public Affairs, received the responsibility to maintain the DOD central Web site registration system. In FY 2000, AFIS began funding the Defense Technical Information Center to operate the DOD central Web site registration system. In 2005, when the Defense Technical Information Center needed to update and redesign the system, AFIS discontinued its funding. As a result, the Defense Technical Information Center terminated the operation of the central Web site registration system.

In 2006, after the registration system was shut down, AFIS began a review of the Web site registration system requirements with the intention of issuing a plan of action by mid- to late April 2006. However, AFIS never completed the review. In October 2008, AFIS was disestablished under the 2005 Base Realignment and Closure process. In January 2008, the Defense Media Activity was established under the authority of the Assistant Secretary of Defense for Public Affairs. AFIS functions, personnel, funding, and associated resources were transferred to the Defense Media Activity. However, responsibility for the requirement to operate a central Web site registration system was not reassigned.

Inventories of DOD Organizations' Public Web Sites

Military Services and other DOD organizations' Web site inventories were inaccurate and unreliable. Without an accurate and reliable inventory, the risk of posting personally identifiable, FOUO, and other sensitive information on publicly accessible Web sites will continue to be a concern.

The Military Services and other DOD organizations (see Appendix A) provided lists totaling 3,211 publicly accessible Web sites; however, after testing the list of Web sites for public accessibility, we determined that 791 (25 percent) were not publicly accessible. Specifically, the lists contained password-protected and non-operational Web sites. When we tested the contact information associated with the public Web sites, we found

many of the points of contact were outdated. After contacting Web site managers, we found an additional 51 publicly accessible Web sites which were not included in Components' inventory list. See Table 1.

Table 1. Number of Public Web Sites Reported and Verified

DOD Component	Reported In Inventory Listings	Verified	Password-Protected/ Non-Operational	Not Reported in Inventory Listings
Army	1,111	791	320	20
Navy	710	647	63	17
Air Force	311	285	26	0
Marine Corps	502	336	166	14
Other Defense	577	361	216	0
Total	**3,211**	**2,420**	**791**	**51**

Army Site Visit Results

A September 2007 Army Audit Agency Report found that since 2005, the Army did not have a central Web site registration repository for its public Web sites, even though it had anticipated establishing a central Web site registration system for all Army Web sites by November 2007. We confirmed that the Army had not established an inventory system for public Web sites. In order to respond to the DEPSECDEF Memorandum issued to DOD Components on September 25, 2008, the Office of the Army Chief Information Officer/G6 issued an All Army Action data call, dated December 8, 2008, for Army public Web sites. The data call required Army commands and agencies to submit a list of their public Web sites and Web site personnel information by February 4, 2009.

We requested a list of Army public Web sites, and on March 31, 2009, the Office of the Army Chief Information Officer/G-6 provided an inventory list of 1,111 public Web sites that was derived from the All Army Action data call. We tested all 1,111 Web sites for public accessibility and found 320 (29 percent) that were not publicly accessible. The inventory listing included password-protected and non-operational Web sites. We also tested Web site inventory point-of-contact information and found much of it was outdated because Web site administrators did not update Web site contact information when personnel changes occurred.

For the Army sites we visited, the inventory list showed 249 Web sites. During our site visits, we verified that all 249 Web sites were publicly accessible. However, we found an additional 20 Web sites not listed by the Army sites we visited.

The Asset and Vulnerability Tracking Resource System, designated on March 12, 2009, as the registration system for all Army public Web sites, was not designed to provide an accurate inventory of Army public Web sites. We received a Web site inventory list

based on an Asset and Vulnerability Tracking Resource system report dated June 15, 2009; the system inventory report listed 1,938 public and private Web sites. We requested a separate list of publicly accessible Web sites only, and were told that because Web sites, both public and private, were not properly labeled when entered into the system, an accurate report listing for public Web sites only was unavailable. For the Asset and Vulnerability Tracking Resource System list of public Web sites to be integrated with a DOD central registration system, the Army system must be able to distinguish between public and all other Web sites, which it does not do.

Results of Navy, Air Force, and Marine Corps Site Visits

Navy, Air Force, and Marine Corps policies require all publicly accessible Web sites to be registered in their respective registration systems. Secretary of the Navy Instruction 5720.47B, "Department of The Navy Policy For Content of Publicly Accessible World Wide Web Sites," December 28, 2005, mandates registration of Navy Web sites in the Naval Web Site Registration System and Marine Corps Web sites in the Marine Corps Web Site Registration Database. The Air Force Policy Memorandum "Public Web Site Registration," May 2, 2007, requires registration of Air Force public Web sites in the Air Force Public Information Management System.

We tested the Navy, Air Force, and Marine Corps Web site registration system inventories for accuracy and currency. We requested a list of public Web sites and were provided Web site inventory lists derived from each of the three Services' registration systems:

- For the listing of 710 Navy-provided Web sites, we found 63 sites (9 percent) were not publicly accessible.
- For the listing of 311 Air Force-provided Web sites, we found 26 sites (8 percent) were not publicly accessible.
- For the listing of 502 Marine Corps-provided Web sites, we found 166 sites (33 percent) were not publicly accessible.

The Navy, Air Force, and Marine Corps Web site lists included password-protected and non-operational Web sites. Point-of-contact information was outdated because Web site administrators did not update contact information when personnel changes occurred.

In addition, for the Navy sites we visited, the inventory list showed 25 Web sites. During our site visits, we verified that all 25 Web sites were publicly accessible, and we found an additional 17 Web sites not listed on the Navy inventory. For the Marine Corps sites we visited, the inventory list showed 24 Web sites. During our site visits, we verified that all 24 Web sites were publicly accessible; however, we found an additional 14 Web sites not listed on the Marine Corps inventory. One possible explanation for some of the inaccuracies in the Marine Corp listing may be attributed to the current effort to migrate all Marine Corps public Web sites to the new Web site, www.marines.mil. Internal control guidance for the Navy, Air Force, and Marine Corps did not mandate review of each Service's public Web sites.

Other DOD Organization Site Visit Results

We reviewed Web site registration practices and requirements for 12 DOD agencies, 5 offices of the Office of the Secretary of Defense, and 1 combatant command. We requested public Web site inventory lists from these DOD organizations which provided lists containing 577 Web sites. We tested all 577 Web sites for public accessibility and determined that 216 (37 percent) were not publicly accessible. The 216 Web sites included password-protected and non-operational Web sites.

Although DOD Web site administrative guidance requires the Military Services to establish and maintain a Web site registration system, the requirement does not extend to DOD agencies and the offices of the Secretary of Defense. However, the Web site registration requirement should extend to DOD organizations such as the Defense Logistics Agency and the Defense Information Systems Agency which operate multiple public Web sites. DOD should establish a threshold requirement for non-Service DOD organizations such as the Defense Information Systems Agency and Defense Logistics Agency to establish and maintain a public Web site registration system based on the number of public Web sites they operate. Web site administrators reported they were unaware of any Federal or DOD policy requiring them to register their public Web sites outside of their offices.

Management Actions

However, the registration application does not completely fulfill the requirements of public law and Federal policy to maintain a current and complete inventory of information dissemination products.

According to the Defense Media Activity Director of Public Web sites, the Defense Media Activity established a new Web site registration capability at the Defense.gov Web site in August 2009. The activity had not issued a DOD-wide notification of the new registration capability as of August 30, 2010. Implementation of the Web site registration application provides a capability for DOD Web site managers to register their public Web sites. However, completion of the registration application does not completely fulfill the requirements of public law and Federal policy to maintain a current and complete inventory of information dissemination products. Additionally, the application does not fully comply with DOD policy which requires all Service registration systems to integrate with the DOD registration system.

Conclusion

DOD did not maintain an agency-wide inventory of its public Web sites as required by law and DOD policy. Military Services were not maintaining Web site inventory systems that reflect an accurate accounting of their publicly accessible Web sites. Twenty-five percent of the Web sites listed in the public Web site inventories for the Military Services and DOD organizations were not publicly accessible. Without an accurate inventory, DOD organizations cannot account for the proper management of all of its publicly

accessible Web sites to reduce the risk of posting personally identifiable, FOUO, and other sensitive information to DOD publicly accessible Web sites.

Recommendations, Management Comments, and Our Response

B.1. We recommend the Assistant Secretary of Defense for Public Affairs identify the system that will maintain the inventory of all DOD publicly accessible Web sites and notify all Components of their requirements to register publicly accessible Web sites within 120 days.

Assistant Secretary of Defense for Public Affairs Comments

The Deputy Assistant Secretary of Defense for Outreach and Social Media, responding for the Assistant Secretary of Defense for Public Affairs, agreed. The Deputy Assistant Secretary of Defense for Outreach and Social Media stated that the registration requirements are published in the existing "Web Site Administration Policies and Procedures," and these requirements will be reissued in the impending DOD Instruction 8430.aa, "DOD Internet Services and Internet-Based Capabilities."

Our Response

The Deputy Assistant Secretary of Defense for Outreach and Social Media comments are responsive and meet the intent of the recommendation. No further comments are required.

B.2. We recommend the Assistant Secretary of Defense for Networks and Information Integration/DOD Chief Information Officer:

a. Require all DOD organizations to register their publicly accessible Web sites with the re-established registration system implemented in Recommendation B.1.

Assistant Secretary of Defense for Networks and Information Integration/DOD Chief Information Officer Comments

The Deputy Chief Information Officer, responding for the Assistant Secretary of Defense for Networks and Information Integration/DOD Chief Information Officer, agreed. The Deputy Chief Information Officer stated the impending DOD Instruction 8430.aa will mandate procedures to register Internet addresses and contact information for all DOD Internet services, external official presence, [4] and other official uses in the registration and inventory system(s) hosted by Assistant Secretary of Defense for Public Affairs on Defense.gov.

---

[4] External official presence is defined by draft DOD Instruction 8430.aa as official public affairs activities, as defined in DOD Instruction 5400.13, conducted on Internet-based capabilities (e.g., Combatant Commands on Facebook, Chairman of the Joint Chiefs of Staff on Twitter).

b. Develop and implement policies to enforce the registration of all DOD publicly accessible Web sites.

Assistant Secretary of Defense for Networks and Information Integration/DOD Chief Information Officer Comments

The Deputy Chief Information Officer, responding for the Assistant Secretary of Defense for Networks and Information Integration/DOD Chief Information Officer, agreed. The impending DOD Instruction 8430.aa mandates that Web sites be registered. Additionally comments for Recommendations A.2, establishes that Web sites not brought into compliance with the instruction will be shut down or disconnected.

c. Require DOD Component Chief Information Officers to maintain accurate inventories of publicly accessible Web sites and ensure their inventories are integrated with the re-established DOD-wide public Web site registration system.

Assistant Secretary of Defense for Networks and Information Integration/DOD Chief Information Officer Comments

The Deputy Chief Information Officer, responding for the Assistant Secretary of Defense for Networks and Information Integration/DOD Chief Information Officer, agreed. The Deputy Chief Information Officer stated the impending DOD Instruction 8430.aa assigns DOD Component Chief Information Officers the responsibility to advise the Assistant Secretary of Defense for Networks and Information Integration/DOD Chief Information Officer and ensure that the policies for the use of DOD Internet services and Internet-based capabilities issued by Assistant Secretary of Defense for Networks and Information Integration/DOD Chief Information Officer are implemented within the Component. The instruction will also establish the requirement to register the Internet addresses and contact information for all DOD Internet services external official presence and other official uses in the registration and inventory system(s) hosted by Assistant Secretary of Defense for Public Affairs on Defense.gov.

d. Establish a minimum threshold based on the number of publicly accessible Web sites managed by non-Service DOD organizations requiring the organizations to establish and maintain an integrated Web site registration system.

Assistant Secretary of Defense for Networks and Information Integration/DOD Chief Information Officer Comments

The Deputy Chief Information Officer, responding for the Assistant Secretary of Defense for Networks and Information Integration/DOD Chief Information Officer, partially agreed. The Assistant Secretary of Defense for Public Affairs will host and operate a registration and inventory system(s) capable of serving the inventory needs of all DOD Components. DOD Components may optionally operate organizational inventory systems to meet their specific needs, but policy should not require the establishment of potentially redundant systems. The impending DOD Instruction 8430.aa has been modified to require the Assistant Secretary of Defense for Public Affairs to host and

operate a registration system(s) for the addresses of public DOD Web sites and external official presence that is capable of producing individual Component inventories. The instruction also requires that the CIOs ensure that the Component's inventory of public Web sites and external official presence is maintained on the registration and inventory system(s) hosted and operated by the Assistant Secretary of Defense for Public Affairs.

Our Response

The Deputy Chief Information Officer's comments are responsive and meet the intent of recommendations B.2.a, B.2.b., B.2.c. and B.2.d. We agree that the creation of potentially redundant systems should be avoided and that the implementation of a fully functional central DOD Web site inventory system is essential to serving the inventory needs of all DOD Components. We confirmed that the draft DOD Instruction 8430.aa contains the requirement for inventory capability and requires the Assistant Secretary of Defense for Public Affairs to host and operate a registration system(s) for the addresses of public DOD Web sites and external official presence that is capable of producing individual Component inventories. No further comments are required.

Appendix A. Scope and Methodology

We conducted this performance audit from February 2009 through August 2010 in accordance with generally accepted government auditing standards. The standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

We evaluated the implementation of the DOD Web Site Administration Policies and Procedures; Deputy Secretary of Defense Memorandum; and Information Security/Web site Alert. We interviewed personnel and obtained information from the Military Services, 12 Defense Agencies, 5 Secretary of Defense offices, and 1 Combatant Command; to include the Defense Logistics Agency, Defense Information Systems Agency, Defense Technical Information Center, Defense Contract Audit Agency, Defense Threat Reduction Agency, Defense Media Activity, TRICARE Management Activity, Defense Finance and Accounting Service, Defense Prisoner of War/Missing Personnel Office, National Geospatial-Intelligence Agency, Defense Advanced Research Project Agency, National Security Agency; Office of the General Counsel, Assistant Secretary of Defense for Public Affairs, Assistant Secretary of Defense for Network and Information Integration/DOD Chief Information Officer, Under Secretary of Defense for Acquisitions, Technology, and Logistics, Secretary of Defense Chief Information Officer; and U.S. Strategic Command, and Public Affairs Officers and Web administrators with the Departments of the Army, Navy, Air Force, and Marine Corps.

We non-statistically selected military installations with publicly accessible Web sites to determine compliance with DOD Web site administrative guidance. Our review included the following 41 military installations selected because of a concentrated number of publicly accessible Web sites in a particular location.

- Army Medical Department Center and School, Fort Sam Houston, Texas
- Army Medical Command, Fort Sam Houston, Texas
- U.S. Army Garrison, Fort Sam Houston, Texas
- U.S. Army North, Fort Sam Houston, Texas
- U.S. Army South, Fort Sam Houston, Texas
- Navy Region Southwest Morale, Welfare, and Recreation, San Diego, California
- Commander Navy Region Southwest, San Diego, California
- Helicopter Maritime Strike Squadron Four One, Naval Air Station North Island, San Diego, California
- Helicopter Anti-Submarine Squadron Light Four Five, Naval Air Station North Island, San Diego, California
- Commander Helicopter Maritime Strike Wing, U.S. Pacific Fleet, Naval Air Station North Island, San Diego, California
- Helicopter Sea Combat Squadron Two One, Naval Air Station North Island, San Diego, California

- Commander, Naval Beach Group One, Naval Amphibious Base Coronado, San Diego, California
- Command, Naval Surface Forces, Naval Amphibious Base Coronado, San Diego, California
- Space and Naval Warfare Systems Command, San Diego, California
- Commander Explosive Ordnance Disposal Group One, Naval Amphibious Base Coronado, San Diego, California
- Tactical Air Control Squadron Twelve, Naval Amphibious Base Coronado, San Diego, California
- Navy Medical Center, San Diego, California
- Commander, Submarine Forces, U.S. Pacific Fleet, Pearl Harbor, Hawaii
- Patrol Squadron 47, Kaneohe Bay Marine Corps Base, Kaneohe, Hawaii
- Patrol Squadron 9, Kaneohe Bay Marine Corps Base, Kaneohe, Hawaii
- Personnel Support Detachment Activity Pearl Harbor, Honolulu, Hawaii
- Commander U.S. Pacific Fleet, Honolulu, Hawaii
- Pearl Harbor Naval Shipyard, Pearl Harbor, Hawaii
- Joint Pacific Command, Hickam Air Force Base, Hawaii
- Mobile Diving and Salvage Unit One, Hickam Air Force Base, Hawaii
- Commander Navy Region Hawaii Fleet and Family Readiness Group, Pearl Harbor, Hawaii
- Naval Computer and Telecommunications Area Master Station Pacific, Wahiawa, Hawaii
- Commander Navy Region Hawaii, Pearl Harbor, Hawaii
- Air Education and Training Command/37th Training Wing, Lackland Air Force Base, Texas
- Air Education and Training Command/Wilford Hall Medical Center, Lackland Air Force Base, Texas
- Air Force Reserve Command/433rd Airlift Wing, Lackland Air Force Base, Texas
- Air Force Security Forces Center, Lackland Air Force Base, Texas
- Air National Guard/149th Fighter Wing, Lackland Air Force Base, Texas
- Air Education and Training Command/12th Flying Training Wing, Randolph Air Force Base, Texas
- Air Education and Training Command/Headquarters, Randolph Air Force Base, Texas
- Air Forces Personnel Center, Randolph Air Force Base, Texas
- First Marine Expeditionary Forces, Camp Pendleton, San Diego, California
- Third Marine Aircraft Wing, Marine Corps Air Station Miramar, San Diego, California
- First Marine Division, Camp Pendleton, San Diego, California
- First Marine Logistics Group, Camp Pendleton, San Diego, California
- Marine Corps Base Hawaii , Kaneohe Bay, Hawaii

Use of Computer-Processed Data

We did not use computer-processed data to perform this audit.

Prior Coverage

During the last 9 years, the Department of Defense Inspector General (DOD IG), the Department of the Army, and the Department of the Navy have issued six reports discussing Web site security policy. Unrestricted DOD IG reports can be accessed at http://www.dodig.mil/audit/reports. Unrestricted Army reports can be accessed at https://www.aaa.army.mil/. Navy reports are unavailable over the Internet.

DOD IG

DOD IG Report No. D-2002-129, "DOD Web Site Administration, Policies, and Practices," July 19, 2002

DOD IG Report No. D-2002-098, "Army Web Site Administration, Policies, and Practices," June 5, 2002

DOD IG Report No. D-2002-062, "Air Force Web Site Administration, Policies, and Practices," March 13, 2002

DOD IG Report No. D-2001-130, "DOD Internet Practices and Policies," May 31, 2001

Army

U.S. Army Audit Agency Report No. A-2007-0206-FFI, "Army Web Sites: Army Chief Information Officer/G-6," September 7, 2007

Navy

Naval Audit Service Report No. N2002-0034, "Department of the Navy Publicly Accessible Web Sites," March 1, 2002

Appendix B. Public Web Site Certification Compliance

DOD Component	Submitted Certification by Due Date 1-20-09	Submitted Certification After Extended Due Date 1-20-09	Agency Did Not Certify	Submitted After IG Contacted Agency	Certification Contained All Data Required	Certification Missing Required Data
Department of the Army		April 17 09		X	POA&M	
Department of the Navy		Jan 27 09			POA&M	
Department of the Air Force		Jan 29 09				Training POA&M
Marine Corps		Jan 27 09			POA&M	
Business Transformation Agency		Feb 17 09			X	
Defense Advanced Research Projects Agency	Dec 23 08					Review & Approval Training
Defense Contract Management Agency	Dec 04 08					Training
Defense Commissary Agency	Dec 18 08					Training
Defense Security Service		June 23 09		X	X	
Defense Finance Accounting Service			X			
Defense Intelligence Agency	Dec 23 08					Training
Defense Information Systems Agency	Dec 01 08					Training POA&M
Defense Logistics Agency		Feb 25 09			POA&M	
Defense Security Cooperation Agency	Oct 29 08				X	

DOD Component	Submitted Certification by Due Date 1-20-09	Submitted Certification After Extended Due Date 1-20-09	Agency Did Not Certify	Submitted After IG Contacted Agency	Certification Contained All Data Required	Certification Missing Required Data
Missile Defense Agency	Dec 24 08				X	
National Geospatial-Intelligence Agency		Jan 23 09				Training
National Security Agency	Jan 20 09				X	
Pentagon Force Protection Agency		Mar 11 09			Training POA&M	
Defense Media Activity			X			
Defense Human Resource Activity			X			
Defense Manpower Data Center			X			
OUSD Personnel and Readiness Information Management			X			
Defense Department Advisory Committee on Women in the Services			X			
Defense Personnel Security Research Center			X			
Employer Support of the Guard and Reserve			X			
Federal Voting Assistance Program			X			
DOD Office of the Actuary			X			

DOD Component	Submitted Certification by Due Date 1-20-09	Submitted Certification After Extended Due Date 1-20-09	Agency Did Not Certify	Submitted After IG Contacted Agency	Certification Contained All Data Required	Certification Missing Required Data
DOD Sexual Assault Prevention and Response Office			X			
Defense Travel Management Office			X			
National Defense University		Aug 07 09		X	POA&M	
DOD Education Activity		Mar 18 09				Training
DOD Prisoner of War/Missing Personnel Office			X			
Defense Technical Information Center		April 14 09		X	X	
DOD Test Resources Management Center			X			
Defense Technology Security Administration			X			
Director of Administration & Management			X			
Office of Economic Adjustment			X			
TRICARE Management Activity/ Health Affairs		Aug 13 09		X		Training
Washington Headquarter Service		Mar 02 09			POA&M	
Acquisition Technology & Logistics		Feb 18 09			POA&M	

DOD Component	Submitted Certification by Due Date 1-20-09	Submitted Certification After Extended Due Date 1-20-09	Agency Did Not Certify	Submitted After IG Contacted Agency	Certification Contained All Data Required	Certification Missing Required Data
Director Defense Research and Engineering			X			
Under Secretary Defense Intelligence			X			
Office Secretary Defense Policy	Dec 24 08				X	
Assistant Secretary of Defense for International Security Affairs			X			
Assistant Secretary of Defense for Asian and Pacific Security Affairs			X			
USD Personnel and Readiness			X			
OSD Comptroller			X			
Defense Contract Audit Agency		Jan 21 09			POA&M	
Director NET ASSESSMENT			X			
Office of General Council		Jun 17 09		X		Training POA&M
OSD Public Affairs			X			
Legislative Affairs			X			
Alternate Joint Communications Center Raven Rock			X			
Director of Operation Test and Evaluation	Dec 19 08				POA&M	

DOD Component	Submitted Certification by Due Date 1-20-09	Submitted Certification After Extended Due Date 1-20-09	Agency Did Not Certify	Submitted After IG Contacted Agency	Certification Contained All Data Required	Certification Missing Required Data
Program Analysis and Evaluation		Jan 29 09			POA&M	
Civilian Personnel Management Service		Apr 20 09			X	
North American Aerospace Defense Command			X			
Assistant Secretary of Defense for Intelligence Oversight			X			
Defense Business Board			X			
Joint Staff			X			
Northern Command			X			
Pacific Command			X			
Southern Command			X			
Central Command			X			
European Command			X			
Special Operations Command			X			
Transportation Command			X			
Joint Forces Command			X			
Strategic Command		Oct 15 09		X	X	

DOD Component	Submitted Certification by Due Date 1-20-09	Submitted Certification After Extended Due Date 1-20-09	Agency Did Not Certify	Submitted After IG Contacted Agency	Certification Contained All Data Required	Certification Missing Required Data
Africa Command			X			
DOD Office of Inspector General		Jan 8, 10		X	X	
Defense Threat Reduction Agency			X [5]			
Networks Information and Integration/Chief Information Officer		Nov 17, 09		X		Training
Totals	**10**	**22**	**41**	**9**	**21**	**11**

[5] DTRA submitted a draft SOP document

Appendix C. Interagency Operations Security Support Staff FY 2010 Training Schedule for Courses OPSE-1500 and OPSE-3500

Course Date	Course Name	NCS Course #	Location
Oct. 20-21	OPSEC & Public Release Decisions	OPSE-1500	IOSS - Greenbelt, MD
Nov. 2-4	OPSEC & Web Risk Assessment	OPSE-3500	IOSS - Greenbelt, MD
Nov. 17-18	OPSEC & Public Release Decisions	OPSE-1500	E-Learning
Jan. 11-13	OPSEC & Web Risk Assessment	OPSE-3500	IOSS - Greenbelt, MD
Jan. 26-27	OPSEC & Public Release Decisions	OPSE-1500	IOSS - Greenbelt, MD
Feb. 23-24	OPSEC & Public Release Decisions	OPSE-1500	E-Learning
Mar. 22-24	OPSEC & Web Risk Assessment	OPSE-3500	IOSS - Greenbelt, MD
Apr. 26-27	OPSEC & Public Release Decisions	OPSE-1500	IOSS - Greenbelt, MD
June 14-16	OPSEC & Web Risk Assessment	OPSE-3500	IOSS - Greenbelt, MD
June 22-23	OPSEC & Public Release Decisions	OPSE-1500	E-Learning
Aug. 3-4	OPSEC & Public Release Decisions	OPSE-1500	IOSS - Greenbelt, MD
Aug. 30-Sep. 1	OPSEC & Web Risk Assessment	OPSE-3500	IOSS - Greenbelt, MD
Sep. 21-22	OPSEC & Public Release Decisions	OPSE-1500	E-Learning

Appendix D. Management Comments on the Findings and Our Response

Defense Information Systems Agency Comments on the Findings

The Vice Director, Defense Information Systems Agency responded for the Director, Joint Web Risk Assessment Cell. Below are excerpts from the draft report, clarifications that Defense Information Systems Agency recommended, and audit responses.

Item 1 (page i, "What We Recommend")
Excerpt: "Require heads of DOD Components to certify annually that a documented Web review and approval process has been developed and implemented. Require all Web administrators to receive the proper Web operations security training. Require Military Services to maintain an integrated registration system with the DOD's registration system."

Management Comments. Add 4th recommendation bullet to read "Upon establishment of a DOD central Web site registration system, personnel working in Joint and Service Web Risk Assessment Cells should routinely search for unregistered DOD Web sites. This practice would identify unregistered sites that should be blocked until they are registered."

Audit Response. Our revised Recommendation A.2 includes the requirement to routinely search for unregistered DOD Web Sites and disconnect Web sites that are not in compliance with the forthcoming DOD Instruction 8430.aa which will require all public Web sites to be registered within a DOD central Web site inventory system.

Item 2 (page ii, "Recommendations Table")
Excerpt: "Recommendations Requiring Comment."

Management Comments. "Suggest that corresponding page numbers be included in the "Recommendations Requiring Comment" entries located in the right-hand column of the Recommendations Table."

Audit Response. We reviewed the management comments and determined that the report revisions were not required. Adding page numbers in the Recommendations Table is contrary to internal DOD OIG policy.

Item 3 (page 1, "Joint Web Risk Assessment Cell")
Excerpt: "The Joint Web Risk Assessment Cell (JWRAC), a DEPSECDEF-chartered cell within the Defense Information Systems Agency, is responsible for conducting analyses of content and data on DOD publicly accessible Web sites. JWRAC reviews Web sites for compliance with existing DOD Web policy and directs remediation actions to bring

Web sites into compliance. JWRAC performs analyses of the aggregate data to determine any existing OPSEC risks that may pose an immediate or potential threat to warfighters."

Management Comments. Suggest editing lines 1 and 2 to read, "The Joint Web Risk Assessment Cell (JWRAC), a DEPSECDEF-chartered cell within the Defense Information Systems Agency, is responsible for conducting operations security (OPSEC) assessments and trend analyses of content and data on DOD publicly accessible Web sites."

Audit Response. We reviewed the management comments and determined that the report revisions were required. We made the revisions as suggested.

Item 4 (page 1, "Joint Web Risk Assessment Cell")
Excerpt: "JWRAC performs analyses of the aggregate data to determine any existing OPSEC risks that may pose an immediate or potential threat to warfighters."

Management Comments. Suggest revising lines 5 and 6 to read "The JWRAC performs analyses of the data to determine any existing OPSEC risks that may pose an immediate or potential threat to warfighters."

Audit Response. We reviewed the management comments and determined that the report revisions were required. We made the revisions as suggested.

Item 5 (page 2, "Joint Web Risk Assessment Cell")
Excerpt: "According to officials, JWRAC conducts analysis of organization Web sites primarily by request from DOD organizations."

Management Comments. Suggest revising lines 1 and 2 to read "According to officials, JWRAC conducts analyses of organization Web sites on an annual schedule and by request from DOD organizations."

Audit Response. We reviewed the management comments and determined that the report revisions were required. We made the revisions as suggested.

Item 6 (page 10, "Incentive to Comply With DOD Policy")
Excerpt: "Management took no action when sensitive information was posted."

Management Comments. Suggest removing sentence 2 which reads "Management took no action when sensitive information was posted." This sentence appears to contradict the information located on page 7, paragraph 3 (lines 3 and 4), which states "After we notified the manager of the noncompliance, they removed the PII from the seven public Web sites we identified."

Audit Response. We reviewed the management comments and determined that the report revisions were required. We revised the sentence to clarify its intent.

Item 7 (page 12, "Service Web Risk Assessment Cells")
Excerpt: "Upon establishment of a DOD central Web site registration system, personnel working in Service Web Risk Assessment Cells should routinely search for unregistered DOD Web sites. This practice would identify unregistered sites that should be blocked until they are registered."

Management Comments. Suggest deleting the paragraph and adding it to page i, paragraph 7, immediately following the 3 other recommendations and add the words "Joint" and "and" to the second line of the paragraph.

Audit Response. Our revised Recommendation A.2 includes the requirement to routinely search for unregistered DOD Web Sites and disconnect Web sites that are not in compliance with the forthcoming DOD Instruction 8430.aa which will require all public Web sites to be registered within a DOD central Web site inventory system.

Item 9 (page 13, "Recommendations")
Excerpt: "We recommend the Secretary of the Air Force within 90 days develop a process to review OPSEC threat and vulnerability risks for all its public Web sites."

Management Comments. Edit Recommendation A.5 to read "We recommend the Secretary of the Air Force within 90 days develop a process to review OPSEC threat and vulnerability risks for all its public Web sites, to include establishing an Air Force Web Risk Assessment Cell." "Each military Component needs to maintain a Web risk assessment cell in order to perform Web OPSEC vulnerability assessments of its respective Service's public Web sites. The Air Force is the only Service Component that does not have an operational Web risk assessment cell."

Audit Response. We reviewed client comments and determined that report revisions were not required. Air Force provided comments to this report designating the Air Force Telecommunications Monitoring Assessment Program to conduct Web OPSEC vulnerability assessments for release of information to the public via Internet-based capabilities.

Appendix E. Criteria for DOD Web Site Inventory

Public Law

- Public Law 104-13, "Paper Reduction Act of 1995," Chapter 35:
    - Section 3506 – Each agency shall maintain a current and complete inventory of the agency's information resources to fulfill the requirements of Section 3511.
    - Section 3511 – The Director of the Office of Management and Budget shall establish and maintain an electronic Government Information Locator Service, which shall identify the major information systems, holdings, and dissemination products (including Web sites) of each agency. Further, the Law requires each agency to establish and maintain its own information locator service as a component of, and to support the operation of, the Government Information Locator Service.
- Public Law 107-347, 107th Congress, "E-Government Act of 2002," December 17, 2002 – Each Federal agency shall develop and establish a public domain directory (inventory) of public Web sites.

Office of Management and Budget

- Office of Management and Budget Circular A-130, "Management of Federal Information Resources" – Agencies will maintain and implement a management system for all information dissemination products which must establish and maintain inventories of all agency Web sites. According to the guidance, the term "information dissemination product" means any book, paper, map, machine-readable material, audiovisual production, or other documentary material, regardless of physical form or characteristic, disseminated by an agency to the public.
- Office of Management and Budget M-05-04, "Policies for Federal Agency Public Web Sites," December 17, 2004 – Federal agency public Web sites are information dissemination products as defined in OMB Circular A-130. Agencies are required, under OMB Circular A-130 and Public Law 104-13, to establish and maintain inventories of information dissemination products.

DOD

"Web Site Administration Policies and Procedures," November 25, 1998, updated January 11, 2002.

- The Assistant Secretary of Defense for Public Affairs is responsible for establishing and maintaining a central Web site registration system for DOD that meets the requirements for the Government Information Locator Service and is integrated with each Service-level registration system.

- The Assistant Secretary of Defense for Networks and Information Integration/DOD Chief Information Officer is responsible for:
    - providing DOD procedural guidance for establishing, operating, and maintaining Web sites;
    - developing and maintaining training guidance and requirements addressing information security on the Web; and
    - approving and publishing DOD instructions and publications to guide, direct, or assist Web site activities.

- The Heads of the DOD Components shall register each publicly accessible Web site with the Government Information Locator Service. Further, each Service will establish and maintain Web site registration systems integrated with DOD's central Web site registration system.

Appendix F. Deputy Secretary of Defense Memo for Office of the Inspector General

DEPUTY SECRETARY OF DEFENSE
1010 DEFENSE PENTAGON
WASHINGTON, DC 20301-1010

SEP 25 2008

MEMORANDUM FOR INSPECTOR GENERAL OF THE DEPARTMENT OF DEFENSE

SUBJECT: Department of Defense (DoD) Web Site Security Policy Compliance

On August 6, 2008, the Vice Chairman of the Joint Chiefs of Staff and I issued a joint message to the DoD components asking them to ensure information placed on DoD publicly accessible web sites is reviewed for security concerns and that publicly available content is in accordance with the Department's "Web Site Administration Policies and Procedures," dated November 25, 1998. That message followed other similar communications over the preceding three years. However, sensitive information frequently can still be found on publicly accessible web sites.

We continue to be concerned about the lack of adherence to the DoD web site security policy and ask you to include this matter as one of particular interest in executing your oversight responsibility. Our point of contact is Mr. Carroll Lee at (703) 604-1143 or carroll.lee@osd

Thanks! Gordon England

OSD 12149-08

Assistant Secretary of Defense for Networks and Information Integration/DOD Chief Information Officer Comments

DEPARTMENT OF DEFENSE
6000 DEFENSE PENTAGON
WASHINGTON, D.C. 20301-6000

CHIEF INFORMATION OFFICER

OCT 15 2010

MEMORANDUM FOR INSPECTOR GENERAL OF THE DEPARTMENT OF DEFENSE

SUBJECT: DoD Controls Over Information Placed on Publicly Accessible Web Sites Require Better Execution (Project No. D2009-D00LB-0147.00)

In response to your memorandum on the above subject, dated September 10, 2010, comments on the findings and recommendations are attached as requested.

The point of contact for this matter is Mr. Terry W. Davis at email: terry.w.davis@osd.mil, telephone: 703.699.0107.

David M. Wennergren
Deputy Chief Information Officer

Attachments: As stated.

cc:
Under Secretary of Defense for Intelligence
Assistant Secretary of Defense for Public Affairs
Assistant Secretary of the Air Force for Financial Management and Comptroller

ASD(NII)/DoD CIO Comments on the Findings and Recommendations in DoDIG Project No. D2009-D000LB-0147.00, "DOD Controls Over Information Placed on Publicly Accessible Web Sites Require Better Execution"

INSTRUCTIONS:

- Comment on internal control weaknesses discussed in the report.
- Provide comments and state whether you agree or disagree with the findings and recommendations.
- If you agree, describe actions taken or planned to accomplish the recommendation, with dates.
- If you disagree, specifically explain why and propose alternative action(s).
- Recommendations requiring comment by ASD(NII)/DoD CIO: A.1, A.2.a, A.2.b, A.3, B.2.a-d
- Recommendation requiring comment by ASD(PA): B.1
- Recommendation requiring comment by JWRAC: A.4
- Recommendation requiring comment by USAF: A.5

Internal Control Weaknesses

No disagreement with the internal control weaknesses discussed in the report.

Recommendations and Comments

Recommendation A.1: Recommend the ASD(NII)/DoD CIO re-emphasize to all DoD Components the DoD Web Site Administration Policy and Procedures requirements to develop review and approval procedures for information posted to publicly accessible Web sites.
Comment: Agree. The ASD(NII)/DoD CIO will, in coordination with the offices of primary responsibility (OPRs) for information release to the public and operations security (OPSEC), the Director of Administration & Management (DA&M) and the Under Secretary of Defense for Intelligence (USD(I)) respectively, re-emphasize and fully describe current review, clearance, and authorization policies and procedures in the forthcoming DoD Instruction (DoDI) 8430.aa, "DoD Internet Services and Internet-Based Capabilities."

Final Report Reference

Revised
Added
A.2.d and A.2.e

Recommendation A.2: Recommend the ASD(NII)/DoD CIO within 120 days develop and issue a Deputy Secretary of Defense Directive to require heads of DoD Component to annually certify, with signature, that:

a. All website administrators develop a documented review and approval process for all public websites.

b. All website administrators have received the prober Web OPSEC training; and

c. All website administrators submit a plan of actions and milestones for all public websites that have not implemented a documented content review and approval process and for those personnel who have not received the proper Web OPSEC training.

Comment: Agree. Annual policy compliance assessment and corrective action will be mandated in the forthcoming DoDI 8430.aa. To better align with the Instruction and provide a more efficient process, request recommendation read:

"A.2. Recommend that ASD(NII)/DoD CIO, within 120 days, develop and issue a DoD Instruction that requires heads of DoD Components to annually assess DoD Internet services and use of Internet-based capabilities for compliance with applicable policies and procedures to include, at minimum, that:

a. Documented review and approval processes are implemented for all public websites and copies of the documentation are filed with the DoD Component CIOs.

b. All website administrators have received the proper Web OPSEC training.

c. All website administrators submit a plan of actions and milestones to the responsible head of DoD Component for all public websites that have not implemented a documented content review and approval process, and for those personnel who have not received the proper Web OPSEC training;

d. Websites and associated processes not brought into compliance with the instruction are shut down or disconnected."

Recommendation A.3: Recommend the ASD(NII)/DoD CIO develop enforcement procedures for non-compliance with the annual certification requirements.

Comment: Agree. The forthcoming DoDI 8430.aa mandates that websites and associated processes be in compliance with the instruction.

Recommendation B.2.a: We recommend the Assistant Secretary of Defense for Networks and Information Integration/DOD Chief Information Officer:

a. Require all DOD organizations to register their publicly accessible Web sites with the re-established registration system implemented in Recommendation B.1.

Comment: Agree. The forthcoming DoDI 8430.aa mandates the procedure to "Register the Internet addresses and contact information for all DoD Internet services, EOP, and other official uses in the registration and inventory system(s) hosted by ASD(PA) on Defense.gov."

Recommendation B.2.b: Develop and implement policies to enforce the registration of all DOD publicly accessible Web sites.
Comment: Agree. The forthcoming DoDI8430.aa mandates that websites be registered.

Recommendation B.2.c: Require DOD Component Chief Information Officers to maintain accurate inventories of publicly accessible Web sites and ensure their inventories are integrated with the re-established DOD-wide public Web site registration system.
Comment: Agree. The forthcoming DoDI 8430.aa assigns DoD Component CIOs the responsibility to "Advise the ASD(NII)/DoD CIO and ensure that the policies and guidance for the use of DoD Internet services and IbC issued by ASD(NII)/DoD CIO are implemented within the Component." The instruction also establishes the procedural requirement to "Register the Internet addresses and contact information for all DoD Internet services, EOP, and other official uses in the registration and inventory system(s) hosted by ASD(PA) on Defense.gov."

Recommendation B.2.d: Establish a minimum threshold based on the number of publicly accessible Web sites managed by non-Service DOD organizations requiring the organizations to establish and maintain an integrated Web site registration system.
Comment: Partially agree. The ASD(PA) will host and operate a registration and inventory system(s) capable of serving the inventory needs of all DoD Components. DoD Components may optionally operate organizational inventory systems to meet their specific needs, but policy should not require the establishment of potentially redundant systems. To emphasize the need for inventory capability and maintenance, the forthcoming DoDI8430.aa has been modified as follows: Page 11, Under ASD(PA) responsibilities: b. Host and operate a registration system(s) for the addresses of public DoD websites and EOP that is capable of producing individual Component inventories. Page 14, Under CIOs responsibilities: g. Ensure that the Component's inventory of public websites and EOP is maintained on the registration and inventory system(s) hosted and operated by ASD(PA).

Assistant Secretary of Defense for Public Affairs Comments

OFFICE OF THE ASSISTANT SECRETARY OF DEFENSE
1400 DEFENSE PENTAGON
WASHINGTON, DC 20301-1400

PUBLIC AFFAIRS

MEMORANDUM FOR PROGRAM DIRECTOR, READINESS, OPERATIONS AND SUPPORT, OFFICE OF THE INSPECTOR GENERAL, DEPARTMENT OF DEFENSE

SUBJECT: DoD Controls Over Information Placed on Publicly Accessible Web Sites Require Better Execution (DoDIG Project No. D2009-D000LB-0147.00)

As the Deputy Assistant Secretary of Defense for Public Affairs, I appreciate the opportunity to comment on the subject draft report. The following response has been coordinated with ASD (NII)/DoD CIO.

Finding A. Weaknesses in DOD's Web Site Review and Approval Process
"Many DOD organizations did not comply with DOD Web Site policy and procedures for publicly accessible Web site content review and approval. Specifically:

- Of 73 DOD organizations identified, 43 (59 percent) did not certify as required that they have mandatory content review and approval procedures in place for information posted to publicly accessible Web sites.
- Of 436 publicly accessible Web sites reviewed, 207 (47 percent) did not have documented review and approval procedures or existing procedures did not fully comply with requirements.
- Of 470 Web site administrators reviewed, 452 (96 percent) had not received required OPSEC 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 cannot ensure that all information posted to DOD publicly accessible Web sites has been properly reviewed and approved. In fact, over the past 3 years, DOD's JWRAC has identified For Official Use Only (FOUO) information, PII, and limited distribution information posted on DOD publicly accessible Web sites. Improper postings increase the risk of potentially harmful disclosure of information related to DOD personnel and missions."

Comments Regarding Finding A. Concur. ASD(PA) personnel have completed Web OPSEC training and comply with DoD Web site policies and procedures, which cover publicly accessible Web site content review and approval for sites we manage. We, in general, have no disagreement with the internal control weaknesses discussed in the report.

Recommendation B.1: "We recommend the Assistant Secretary of Defense for Public Affairs identify the system that will maintain the inventory of all DOD publicly accessible Web sites and notify all Components of their requirements to register publicly accessible Web sites within 120 days."

Response for Recommendation B.1. OASD(PA) agrees to identify the system that will maintain the inventory of all DoD publicly accessible websites. Registration requirements are published in the existing "Web Site Administration Policies and Procedures" and these requirements will be reissued in the forthcoming DoD Instruction8430.aa, DoD Internet Services and Internet-Based Capabilities.

We will continue to work on improving our organization by implementing the recommendations, as indicated above, and we will keep your staff apprised of our progress.

Sumit Agarwal
Deputy Assistant Secretary of Defense
for Outreach & Social Media

Secretary of the Air Force Comments

DEPARTMENT OF THE AIR FORCE
WASHINGTON, DC

OFFICE OF THE SECRETARY

OCT 28 2010

MEMORANDUM FOR INSPECTOR GENERAL, AUDITING, READINESS, OPERATIONS AND SUPPORT

FROM: SAF/A6N

SUBJECT: DOD Controls Over Information Placed on Publicly Accessible Web Sites Require Better Execution, Project No. D2009-D000LB-0147.000

1. SAF/CIO A6 has reviewed the aforementioned report and provide the following comments with our planned actions.

a. Air Force Comments to A.5: Concur. The AF has identified that the AF Telecommunications Monitoring Assessment Program (TMAP) will be utilized to conduct OPSEC vulnerability assessments on aggregated information that is released to the public via Internet-base Capabilities. Policy documents have been developed and progress is being made to officially start conducting vulnerability assessment upon the signature of AFI 10-712, Telecommunications Monitoring Assessment Program.

b. In addition, the following policy is being developed within AFI 10-701, Operations Security (OPSEC), to address the lack of AF directive in regards to OPSEC reviews conducted prior to releasing information and training for personnel reviewing information.

1) Draft AFI 10-701, Operations Security (OPSEC) will require that AF organizations conduct vulnerability analysis of content on their organization's public and private web sites for information that is critical to their mission.

2) Commanders/Directors will be required to ensure all personnel such as, Web Site administrators, Webmasters, supervisors, public affairs specialist, OPSEC coordinators, PMs, SMO, etc., who review information for public release complete OPSEC training focused on reviewing information that is intended for posted utilizing Internet-base Capabilities.

3) AF OPSEC Program Managers will be required to work closely with officials who share responsibility for the protection and release of information to ensure critical information is protected.

c. Air Force General Comments: The Air Force Public Affairs Agency (AFPAA) developed and implemented a Quality Assurance program designed to identify, track, and report discrepancies in content on 362 Air Force public websites IAW current DoD and Air Force

instructions, guidance, policies and directives. Among other things, these assessments were designed to identify violations related to OPSEC, Personally Identifiable Information (PII) and other sensitive information and to provide instructions to website managers on how to resolve these issues quickly and effectively. AFPAA will update AFI 35-107, Public Web Communications, in the coming year to better specify relevant policies and procedures related to website content management and oversight with emphasis on security and policy review and OPSEC. In addition, the Agency will develop a template for a local operating instruction that can be tailored by individual Air Force website managers to better manage their local programs.

2. If you have any questions, please contact Mr. Dave Keal at 703-588-6156 or via e-mail at Luther.Keal@pentagon.af.mil.

PAUL F. CAPASSO, Maj Gen, USAF
Director, Network Services
Office of Information Dominance and
Chief Information Officer

Defense Information Systems Agency (Joint Web Risk Assessment Cell) Comments

DEFENSE INFORMATION SYSTEMS AGENCY
P. O. BOX 4502
ARLINGTON, VIRGINIA 22204-4502

IN REPLY REFER TO: Operations (GO)

OCT 1 2 2010

MEMORANDUM FOR THE DEPARTMENT OF DEFENSE INSPECTOR GENERAL (IG)

SUBJECT: Global Information Grid Operations Response to the "DoD Controls Over Information Placed on Publicly Accessible Web Sites Require Better Execution", Project No. D2009-D000LB-0147.000

1. The subject "DoD Controls Over Information Placed on Publicly Accessible Web Sites Require Better Execution" was reviewed and responses are enclosed. The Joint Web Risk Assessment Cell will expand distribution of its annual OPSEC and threat assessments report of DoD public Web sites to the Assistant Secretary of Defense for Networks and Information Integration /DoD Chief Information Officer and the Office of the Under Secretary of Defense for Intelligence.

2. Furthermore, please find enclosed a Joint Web Risk Assessment Cell comments matrix resolution form identifying additional content/administrative recommendations for your consideration.

3. Direct any questions to Lt Col Denise Waggoner, Chief, Joint Web Risk Assessment Cell, 703-697-0332, denise.waggoner@disa.mil or Ms. Lori Collins, Deputy, Joint Staff Support Center (JSSC), 703-693-0111, lori.collins@disa.mil.

RONNIE D. HAWKINS, JR.
Major General, USAF
Vice Director

2 Enclosures:
1 JWRAC Comments Matrix
2 Resolution Form

Final Report Reference

[UNCLASSIFIED]

COMMENTS MATRIX FOR DoD ISSUANCES: DoD IG Report: Project No. D2009-D000LB-0147.000
"DoD Controls Over Information Placed on Publicly Accessible Web Sites Require Better Execution"
(Please read instructions on back before completing form.)

#	CLASS (U)	COMPONENT AND POC NAME, PHONE, AND E-MAIL	PAGE #	PARA #	COMMENT TYPE (C/S)	COMMENTS, JUSTIFICATION, AND ORIGINATOR JUSTIFICATION FOR RESOLUTION	A/R/P
1		DISA/JSSC/ JWRAC, Lt Col Denise Waggoner, 703-697-0332, denise.waggoner @disa.mil	i	7	S	**Coordinator Comment**: Add 4th bullet to read "Upon establishment of a DoD central Web site registration system, personnel working in Joint and Service Web Risk assessment cells should routinely search for unregistered DoD Web sites. This practice would identify unregistered sites that should be blocked until they are registered." **Coordinator Justification**: This bullet is currently located at the top of page 12, first paragraph. Suggest that it be included on p. i., paragraph 7, along with the 3 other recommendations. Also added the words "Joint" and "and" to the second line of the paragraph. As currently written, the Joint Web Risk Assessment Cell is excluded. **Originator Justification for Resolution**:	
2		DISA/JSSC/ JWRAC, Lt Col Denise Waggoner, 703-697-0332, denise.waggoner @disa.mil	ii	1	S	**Coordinator Comment**: Suggest that corresponding page numbers be included in the "Recommendations Requiring Comment" entries located in the right-hand column of the "Recommendations Table". **Coordinator Justification**: For those tasked to comment, this will facilitate locating the applicable section(s) quickly. **Originator Justification for Resolution**:	

SD FORM 818, JAN 09 PREVIOUS EDITION IS OBSOLETE 1

[UNCLASSIFIED]

Revised Added Recommendation A.2.e Page 13

Final Report Reference

[UNCLASSIFIED]

COMMENTS MATRIX FOR DoD ISSUANCES: DoD IG Report: Project No. D2009-D000LB-0147.000
"DoD Controls Over Information Placed on Publicly Accessible Web Sites Require Better Execution"
(Please read instructions on back before completing form.)

#	CLASS (U)	COMPONENT AND POC NAME, PHONE, AND E-MAIL	PAGE #	PARA #	COMMENT TYPE (C/S)	COMMENTS, JUSTIFICATION, AND ORIGINATOR JUSTIFICATION FOR RESOLUTION	A/R/P
3		DISA/JSSC/ JWRAC, Lt Col Denise Waggoner, 703-697-0332, denise.waggoner @disa.mil	1	5	S	**Coordinator Comment**: Suggest editing lines 1 and 2 to read "The Joint Web Risk Assessment Cell (JWRAC), a DEPSECDEF-chartered cell within the Defense Information Systems Agency (DISA), is responsible for conducting operations security (OPSEC) assessments and trend analyses of content and data on DoD publicly accessible Web sites." **Coordinator Justification**: Clarifies the wording describing the JWRAC mission. **Originator Justification for Resolution**:	
4		DISA/JSSC/ JWRAC, Lt Col Denise Waggoner, 703-697-0332, denise.waggoner @disa.mil	1	5	S	**Coordinator Comment**: Suggest editing lines 5 and 6 to read "The JWRAC performs analyses of the data to determine any existing OPSEC risks that may pose an immediate or potential threat to warfighters." **Coordinator Justification**: Removed the word "aggregate" from line 6 as the JWRAC does not perform this function. This falls within the scope of the intelligence arena. **Originator Justification for Resolution**:	

SD FORM 818, JAN 09 PREVIOUS EDITION IS OBSOLETE 2

[UNCLASSIFIED]

Revised Page 1

Revised Page 1

Final Report Reference

[UNCLASSIFIED]

COMMENTS MATRIX FOR DoD ISSUANCES: DoD IG Report: Project No. D2009-D000LB-0147.000
"DoD Controls Over Information Placed on Publicly Accessible Web Sites Require Better Execution"
(Please read instructions on back before completing form.)

#	CLASS (U)	COMPONENT AND POC NAME, PHONE, AND E-MAIL	PAGE #	PARA #	COMMENT TYPE (C/S)	COMMENTS, JUSTIFICATION, AND ORIGINATOR JUSTIFICATION FOR RESOLUTION	A/R/P
5		DISA/JSSC/ JWRAC, Lt Col Denise Waggoner, 703-697-0332, denise.waggoner @disa.mil	2	1	S	**Coordinator Comment**: Suggest editing lines 1 and 2 to read "According to officials, JWRAC conducts analyses of organization Web sites on an annual schedule and by request from DoD organizations." **Coordinator Justification**: The JWRAC conducts analyses two ways; by an annual schedule as well as by ADHOC requests from DoD-level organizations. **Originator Justification for Resolution**:	
6		DISA/JSSC/ JWRAC, Lt Col Denise Waggoner, 703-697-0332, denise.waggoner @disa.mil	10	2	S	**Coordinator Comment**: Suggest deleting sentence 2 which reads "Management took no action when sensitive information was posted." **Coordinator Justification**: This sentence appears to contradict the information located on page 7, paragraph 3 (lines 3 and 4), which states "After we notified the managers of the noncompliance, they removed the PII from the seven public Web sites we identified" (referring to PII found on Navy public Web sites) and also in paragraph 5 (lines 3 and 4), which states "After we notified the Marine Corps public Web site managers of the noncompliance, they removed PII from 11 of the 12 public Web sites." **Originator Justification for Resolution**:	

SD FORM 818, JAN 09 PREVIOUS EDITION IS OBSOLETE 3

[UNCLASSIFIED]

Revised Page 2

Revised Page 10

Final Report Reference

[UNCLASSIFIED]

COMMENTS MATRIX FOR DoD ISSUANCES: DoD IG Report: Project No. D2009-D000LB-0147.000
"DoD Controls Over Information Placed on Publicly Accessible Web Sites Require Better Execution"
(Please read instructions on back before completing form.)

#	Class (U)	Component and POC Name, Phone, and E-mail	Page #	Para #	Comment Type (C/S)	Comments, Justification, and Originator Justification for Resolution	A/R/P
7		DISA/JSSC/ JWRAC, Lt Col Denise Waggoner, 703-697-0332, denise.waggoner @disa.mil	12	1	S	**Coordinator Comment**: Suggest deleting 1st paragraph which reads "Upon establishment of a DoD central Web site registration system, personnel working Service Web Risk assessment cells should routinely search for unregistered DoD Web sites. This practice would identify unregistered sites that should be blocked until they are registered." **Coordinator Justification**: Recommend adding to p. i., paragraph 7, immediately following the 3 other recommendations. Also added the words "Joint" and "and" to the second line of the paragraph. As currently written, the Joint Web Risk Assessment Cell is excluded. **Originator Justification for Resolution**:	
8		DISA/JSSC/ JWRAC, Lt Col Denise Waggoner, 703-697-0332, denise.waggoner @disa.mil	12	6		**Coordinator Comment**: Concur on A.4. **Coordinator Justification**: **Originator Justification for Resolution**:	

SD FORM 818, JAN 09 PREVIOUS EDITION IS OBSOLETE 4

[UNCLASSIFIED]

Revised Added Recommendation A.2.e Page 13

COMMENTS MATRIX FOR DoD ISSUANCES: DoD IG Report: Project No. D2009-D000LB-0147.000
"DoD Controls Over Information Placed on Publicly Accessible Web Sites Require Better Execution"
(Please read instructions on back before completing form.)

#	CLASS (U)	COMPONENT AND POC NAME, PHONE, AND E-MAIL	PAGE #	PARA #	COMMENT TYPE (C/S)	COMMENTS, JUSTIFICATION, AND ORIGINATOR JUSTIFICATION FOR RESOLUTION	A/R/P
9		DISA/JSSC/ JWRAC, Lt Col Denise Waggoner, 703-697-0332, denise.waggoner @disa.mil	13	1	S	**Coordinator Comment**: Recommend editing A.5. to read "We recommend the Secretary of the Air Force within 90 days develop a process to review OPSEC threat and vulnerability risks for all its public Web sites, to include establishing an Air Force Web Risk Assessment Cell." **Coordinator Justification**: Each military component needs to maintain a Web risk assessment cell in order to perform Web OPSEC vulnerability assessments of their respective Service's public Web sites. The Air Force is the only Service component who does not have an operational Web risk assessment cell. **Originator Justification for Resolution**:	

Inspector General
Department of Defense