July 19, 2002

Information System Security

DoD Web Site Administration, Policies, and Practices
(D-2002-129)

Department of Defense
Office of the Inspector General

Quality *Integrity* *Accountability*

Report Documentation Page

Report Date	Report Type	Dates Covered (from... to)
19 Jul 2002	N/A	-

Title and Subtitle Information System Security: DoD Web Site Administration, Polices, and Practices	**Contract Number**
	Grant Number
	Program Element Number
Author(s)	**Project Number**
	Task Number
	Work Unit Number
Performing Organization Name(s) and Address(es) OAIG-AUD(ATTN: AFTS Audit Suggestions) Inspector General Department of Defense 400 Army Navy Drive Arlington, VA 22202-2884	**Performing Organization Report Number** D-2002-129
Sponsoring/Monitoring Agency Name(s) and Address(es)	**Sponsor/Monitor's Acronym(s)**
	Sponsor/Monitor's Report Number(s)
Distribution/Availability Statement Approved for public release, distribution unlimited	
Supplementary Notes	
Abstract	
Subject Terms	
Report Classification unclassified	**Classification of this page** unclassified
Classification of Abstract unclassified	**Limitation of Abstract** UU
Number of Pages 27	

Additional Copies

To obtain additional copies of this report, visit the Web site of the Inspector General of the Department of Defense at www.dodig.osd.mil/audit/reports or contact the Secondary Reports Distribution Unit of the Audit Followup and Technical Support Directorate at (703) 604-8937 (DSN 664-8937) or fax (703) 604-8932.

Suggestions for Future Audits

To suggest ideas for or to request future audits, contact the Audit Followup and Technical Support Directorate at (703) 604-8940 (DSN 664-8940) or fax (703) 604-8932. Ideas and requests can also be mailed to:

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

Defense Hotline

To report fraud, waste, or abuse, contact the Defense Hotline by calling (800) 424-9098; by sending an electronic message to Hotline@dodig.osd.mil; or by writing to the Defense Hotline, The Pentagon, Washington, DC 20301-1900. The identity of each writer and caller is fully protected.

Acronyms

JWRAC	Joint Web Risk Assessment Cell
CERT	Computer Emergency Response Team

INSPECTOR GENERAL
DEPARTMENT OF DEFENSE
400 ARMY NAVY DRIVE
ARLINGTON, VIRGINIA 22202-2884

July 19, 2002

MEMORANDUM FOR ASSISTANT SECRETARY OF DEFENSE (COMMAND, CONTROL, COMMUNICATIONS, AND INTELLIGENCE)
DIRECTOR, DEFENSE INFORMATION SYSTEMS AGENCY

SUBJECT: Report on DoD Web Site Administration, Policies, and Practices (Report No. D-2002-129)

We are providing this report for review and comment. We considered management comments on the draft of this report when preparing the final report.

We request that management provide comments that conform to the requirements of DoD Directive 7650.3. If possible, please provide management comments in electronic format (Adobe Acrobat file only). Send electronic transmission to the e-mail addresses cited in the last paragraph of this memorandum. Copies of the management comments must contain the actual signature of the authorizing official. We cannot accept the / Signed / symbol in place of the actual signature. If you arrange to send classified comments electronically, they must be sent over the SECRET Internet Protocol Router Network (SIPRNET).

DoD Directive 7650.3 requires that all recommendations be resolved promptly. The Defense Information Systems Agency's comments to the draft report were responsive. However, the Deputy Assistant Secretary of Defense (Security and Information Operations), who responded for the Assistant Secretary of Defense (Command, Control, Communications, and Intelligence), nonconcurred with Recommendation 1.a. As a result, we request that the Deputy Assistant Secretary of Defense (Security and Information Operations) provide additional comments on Recommendation 1.a. to the final report by September 19, 2002.

We appreciate the courtesies extended to the staff. Questions should be directed to Mr. Bruce A. Burton at (703) 604-9071 (DSN 664-9071) (bburton@dodig.osd.mil) or Mr. Thomas S. Bartoszek at (703) 604-9014 (DSN 664-9014) (tbartoszek@dodig.osd.mil). See Appendix C for the report distribution. The audit team members are listed inside the back cover.

Thomas F. Gimble
Acting
Deputy Assistant Inspector General
for Auditing

Office of the Inspector General of the Department of Defense

Report No. D-2002-129 **July 19, 2002**
(Project No. D2001AB-0116.002)

DoD Web Site Administration, Policies, and Practices

Executive Summary

Who Should Read This Report and Why? Web site developers and administrators, public affairs officers, managers responsible for Web site content, and Web site users should read the reports in this series. Those involved with any aspect of a Web site will want to make sure that the content in their sites is up to date, accessible, tamper-proof, and yet user friendly. The content must also be a true reflection of the policies of the parent organization.

Background. This report is the third in a series that addresses Internet access, practices, and policies. Previous reports covered Web site administration at the Air Force and the Army. The Naval Audit Service issued a separate report based on the audit of Web-site administration at the Navy and the Marine Corps. The "DoD Web Site Administration Policy and Procedures," implemented December 7, 1998, and updated April 26, 2001, describes procedures for establishing, operating, and maintaining DoD unclassified Web sites. The Policy requires heads of DoD Components to establish a process to identify appropriate information for posting to Web sites and to ensure the review of all information placed on publicly accessible Web sites for security levels of sensitivity and other concerns before release. In addition, it requires the Assistant Secretary of Defense for Command, Control, Communications, and Intelligence to ensure that DoD agencies and the Services comply with the Policy.

On February 12, 1999, the Deputy Secretary of Defense approved the Joint Web Risk Assessment Cell's Concept of Operations, a plan to use Reserve Components' assets to conduct ongoing security and threat assessments of Components' Web sites for inappropriate information. The Concept of Operations identifies the Defense Information Systems Agency as the executive agent for the Joint Web Risk Assessment Cell and requires the executive agent to develop an implementation plan, operating procedures, and a reporting mechanism.

Results. As of May 2002, 30 of the 200 disclosures on publicly accessible DoD Web sites that the JWRAC previously identified between April and September 2001 as inappropriate were still available for public viewing. As a result, DoD Web-site owners are not providing consistent levels of assurance that only appropriate information is posted on their publicly accessible Web sites. DoD must require DoD agencies and the Services to remove from public view Web pages that contain information identified as potentially inappropriate in the Joint Web Risk Assessment Cell reports. In addition, DoD must establish a mechanism that adjudicates disagreements between the Joint Web Risk Assessment Cell and Web-site owners on potentially inappropriate disclosures at Web sites. Further, DoD must publish and comply with the standard operating procedures of the Joint Web Risk Assessment Cell for discrepancy reporting and tracking, and maintain an up-to-date database of reported violations.

Management Comments. The Deputy Assistant Secretary of Defense (Security and Information Operations), who responded for the Assistant Secretary of Defense (Command, Control, Communications, and Intelligence), nonconcurred with the recommendation to suspend Web pages that contain potentially inappropriate information until resolution. She stated that Web site postings are based on operational security evaluations at the local commander level and, unless overturned by a higher authority, their decision is final. The Deputy Assistant Secretary partially concurred to establish a timely adjudication process. The Defense Information Systems Agency concurred with the recommendation to publish the Joint Web Risk Assessment Cell's Standard Operating Procedures for Discrepancy Reporting and Tracking and to establish a database system to track Web risk-assessment activities.

Audit Response. Of the 200 instances of information deemed inappropriate at DoD Web sites, 30 were still available to the general public in May 2002, almost 8 months after the Joint Web Risk Assessment Cell issued its September 2001 report that identified the information. It is evident by the number of occurrences that the review process for determining the appropriateness of data on Web pages has not been fully successful, and that the existing process and procedures for local commanders to address the content of information placed on their Web site are inadequate. Accordingly, information that may place DoD at an increased risk must be suspended until resolved through an adjudication process.

Table of Contents

Background

DoD Web Page Policy. The "DoD Web Site Administration Policy and Procedures," (the Policy) December 7, 1998, and updated April 26, 2001, describes procedures for establishing, operating, and maintaining DoD unclassified Web sites. The Policy requires heads of DoD agencies and the Services (DoD Components) to establish a process to identify information that is appropriate for posting to Web sites. The Policy requires that all information placed on publicly accessible Web sites is reviewed for security levels of sensitivity and other concerns before the information is released. Inappropriate data include data labeled "For Official Use Only," "sensitive," classified, and other information at one or more sites, which, when combined, would be sensitive or classified, and should not be released to the general public.

The Policy requires DoD Components to establish procedures for management oversight and regular functional reviews of Web sites and to provide necessary resources to support Web site operations, including funding, staffing, and training. The Policy also requires an annual security assessment of Web sites. Moreover, Components must register each publicly accessible Web site with the Government Information Locator Service, which helps citizens identify, locate, and retrieve information about the Government. The Government Information Locator Service resides on the Defense Link, which is the official Web site for DoD and the starting point for finding military information about defense policy, organizations, functions, and operations online. In addition, the Policy requires the Assistant Secretary of Defense for Command, Control, Communications, and Intelligence to ensure that DoD Components comply with the Policy.

The Policy defines a DoD Web site as a collection of information organized into a number of Web documents. The information is related to a common subject or set of subjects, including a Home Page, and is linked to subordinate information that is included on a Web page. A Home Page is the index or introductory document for a Web site. A Web site is developed and maintained with command sponsorship, approval, and editorial supervision over content.

DoD Oversight of Web Content. On February 12, 1999, the Deputy Secretary of Defense approved the Joint Web Risk Assessment Cell (JWRAC) Concept of Operations, a plan to use Reserve Components' assets to conduct ongoing security and threat assessments of Components' Web sites. The JWRAC is responsible for analyzing data on DoD Web sites for information that poses potential or real threats to ongoing operations and DoD personnel.

The Concepts of Operations identifies the Defense Information Systems Agency as the executive agent for JWRAC. As executive agent, the Defense Information Systems Agency exercises operational control over the JWRAC and provides it with legal support, facilities, and other administrative support. The Concept of Operations also requires the executive agent to develop an implementation plan and standard operating procedures for the JWRAC. The standard operating procedures should include procedures for identifying Web sites that contain potentially inappropriate information and define that information as a discrepancy. An implementation plan should also include a process to report the discrepancy to

the DoD Computer Emergency Response Team (DoD CERT) and the responsible Service or command entity. The standard operating procedures plan would also outline a process to track, verify, and resolve the discrepancy. DoD established the CERT in April 1999 to manage, control, monitor, and protect computer networks and their infrastructure so that they would be available to support the needs of DoD.

Draft Reporting and Tracking Procedures for the JWRAC. The Defense Information Systems Agency prepared a draft "JWRAC Standard Operating Procedures for Discrepancy Reporting and Tracking." The procedures were undated, but the DoD CERT verbally approved them for use in May 2001. The procedures describe the process for recording and reporting the results of the JWRAC. The procedures state that after the JWRAC analyzes data on DoD Web sites for information that poses potential or real threats to ongoing operations and DoD personnel, it must prepare an End of Tour Report and send it to the Chief, DoD CERT.

The End of Tour Report contains a description of the discrepancies, actions required, and a summary of findings. DoD CERT officials then record the JWRAC information in its database, which is used to report, monitor, and verify removal of inappropriate information. The JWRAC Team Chief also prepares the Initial Notification Message (Message) from the information in the database and sends it to the Chief, DoD CERT for review. The Chief, DoD CERT in turn reviews the Message and sends it to the Joint Task Force-Computer Network Operations who sends it to the organization whose Web site contains the inappropriate information.

The Message contains the Web address of the discrepancy, a description of the inappropriate information, an assessment of the risk, and a request to the Web-site owner to remove or block the data from public access. The JWRAC Message requires a response time of 12 hours for a critical violation, 48 hours for a major violation, and 14 days for a minor violation. Violations are determined to be critical if they consist of either classified or sensitive information or, when combined with other sensitive information, they may have a significant operational impact. Major violations consist of information that is "For Official Use Only," and minor violations consist of other information that may not be posted on official Web sites that are available to the general public. The DoD CERT, through a designated discrepancy tracking coordinator, monitors the responses to the JWRAC, determines whether the discrepancies have been resolved and, if so, closes out the tracking database. If the discrepancies have not been resolved, the discrepancy tracking coordinator would bring the response to the Chief, DoD CERT for escalation to closure. Escalating the discrepancy to closure requires the Chief, DoD CERT to contact the Web-site owner and request immediate removal of the inappropriate information.

Objectives

Our objective was to evaluate policies and practices for Web site administration and oversight at selected DoD agencies. Specifically, we reviewed how the Defense Logistics Agency; the General Counsel, Office of the Secretary of Defense; and the U. S. Space Command host official Web sites, and how the DoD agencies register the Web sites, monitor compliance with policy, and safeguard information displayed. In addition, we reviewed the DoD process for identifying and removing inappropriate information from publicly accessible DoD Web sites. We also evaluated the management control program as it relates to the overall objective.

The results of our review on how selected DoD agencies register and monitor Web sites are included in Appendix B. The process for identification, removal, and oversight of inappropriate information on publicly accessible DoD Web sites warrants management attention and is discussed in the Finding section of this report. See Appendix A for a discussion of the audit scope and methodology, the management control program, and prior audit coverage.

Inappropriate Information on Publicly Accessible DoD Web Sites

As of May 2002, 30 of 200 disclosures on publicly accessible DoD Web sites that the JWRAC previously identified as inappropriate were still available for public viewing because the Assistant Secretary of Defense (Command, Control, Communications, and Intelligence) did not establish:

- a mechanism to remove potentially inappropriate information from Web sites, and
- an adjudication process to resolve differences between the Joint Web Risk Assessment Cell and Web-site owners on whether disclosures were inappropriate.

In addition, the Defense Information Systems Agency had not completed the "JWRAC Standard Operating Procedures for Discrepancy Reporting and Tracking" in a timely manner. As a result, DoD Web-site owners were not providing consistent levels of assurance that only appropriate information is posted on their publicly accessible Web sites.

Information Reported on DoD Public Web Sites

Results of the Joint Web Risk Assessment Cell. In November 2001, the JWRAC Team Chief provided us with eight End of Tour Reports, issued between April and September 2001, which contained 200 violations. We summarized the reports and identified the descriptions and the number of violations by Service and DoD agency as shown in Table 1.

Table 1. JWRAC-Verified Web Site Violations

Description of Violations	Army	Navy	Air Force	Marine Corps	DoD Agencies	Total
Operation plans	19	6	16	6	2	49
For Official Use Only	11	7	12	4	26	60
Military personnel information such as social security numbers	4	7	1	0	0	12
Reserve Officer Training Corps fax numbers	39	0	0	0	0	39
Other	2	2	3	0	8	15
Details of radio frequencies	0	0	7	0	0	7
Internal policies and procedures	2	2	0	0	9	13
Root internet protocol addresses	0	0	0	0	5	5
Total	77	24	39	10	50	200

Inappropriate Disclosures Remaining on Web Sites. In May 2002, we accessed the 200 Web site locations to determine whether the information reported by the JWRAC was still present. Of the 200 disclosures that were cited in the 8 JWRAC reports, 30 (15 percent) still contained the inappropriate data. We summarized the results in Table 2 by description of the violation, the number of occurrences, the Service, and DoD agency.

Table 2. JWRAC-Verified Web Sites With Violations Remaining

Description of Violations	Army	Navy	Air Force	DoD Agencies	Total
Operation plans	0	0	2	0	2
For Official Use Only	3	0	2	7	12
Other	0	2	0	4	6
Internal policies and procedures	2	0	0	4	6
Root internet protocol addresses	0	0	0	4	4
Total	**5**	**2**	**4**	**19**	**30**

There were 30 inappropriate disclosures of information remaining on DoD Web sites that were still available to the general public in May 2002, almost 8 months after the JWRAC issued the September 2001 report. We determined that 14 of the 30 (46 percent) Web sites contained potentially major violations because they showed operation plans and "For Official Use Only" data.

Authority for Suspension or Removal of Inappropriate Information. The JWRAC analyzed data on DoD Web sites and verified that Web-site violations had occurred. The Team Chief, JWRAC reported the verified violations in an End of Tour Report to the Chief, DoD CERT. The Team Chief informed us that he then prepared the Messages for the violations, which the Chief, DoD CERT reviewed and forwarded to the Joint Task Force-Computer Network Operations who forwards it to the organizations whose Web sites contained the inappropriate information.

The previously described process is contained in the draft "JWRAC Standard Operating Procedures for Discrepancy Reporting and Tracking." Officials stated that, beginning in October 2001, the procedures would be used as a working document while they were being refined and improved; however, the procedures contained an underlying assumption that the Web-site owner would concur or that resolution would occur within a short time frame, and that the Web-site owner would remove the inappropriate information.

When differences arise between the Web-site owner and the JWRAC Team Chief on whether a violation has occurred, the current practice is for the discrepancy tracking coordinator to bring the Web-site owner's response to the Chief, DoD CERT for escalation to closure. However, a mechanism is needed to remove the Web page containing the potentially inappropriate information from public view until an adjudication authority makes a decision. Additionally, disagreements on the appropriateness of the information require an adjudication authority to make a timely decision.

Discrepancy Reporting and Tracking

Of the eight End of Tour Reports issued by the JWRAC, only one included all three categories of critical, major, and minor violations. Two of the reports included only major violations when they should also have included minor violations, two included critical violations when they should also have addressed major and minor violations, one addressed critical and major violations when they should also have addressed minor violations, and two reports did not categorize violations.

The reports must address the type of violation because that is how the urgency of resolution and the suspense time frame for a response by the Web-site owner are determined. The JWRAC Team Chief could not explain this condition except to indicate that the reporting process was still evolving.

In addition, officials stated that they were unable to provide us with the Messages sent to the Web-site owners for violations recorded in the eight End of Tour Reports because the CERT did not retain them. Also, the database maintained by the Chief, DoD CERT was not updated to show whether notifications were delayed, whether follow-up actions were required or taken on nonresponses, and whether the inappropriate information was still on the Web site. Officials informed us that the CERT planned to migrate the information to a new database but migration had not occurred because of funding constraints. They believed that many of the problems we identified were a result of the still-evolving reporting and recording process. The Chief, DoD CERT verbally approved the draft "JWRAC Standard Operating Procedures for Discrepancy Reporting and Tracking" for incident reporting for use in May 2001. Officials agreed that the draft would be used as a working document while the reporting procedures continued to be refined and improved. The present procedures, dated October 18, 2001, were being updated.

The JWRAC reports must be consistent in identifying the category of inappropriate disclosures to allow the DoD CERT to track Messages of potential violations and identify the response time required by Web-site owners. Also, the database must be kept current on the status of each finding, the timeliness of responses, and whether the issues were resolved and the inappropriate information was removed. A consistent and up-to-date database will provide an accurate assessment of Web site information and will allow DoD to take appropriate action to remove information that poses potential or real threats to ongoing operations and DoD personnel. In addition, the draft reporting procedures should be completed, published, and complied with because they provide DoD officials with a reporting and recording mechanism for inappropriate disclosures identified by the JWRAC.

Summary

Publicly accessible DoD Web sites must be informative and contain only information that is appropriate for public release. The JWRAC is responsible for analyzing data on DoD Web sites and informing the Chief, DoD CERT of potential or real threats to ongoing operations and DoD personnel. The DoD CERT Tracking Coordinator notifies the offending Web-site owner, monitors the owner's responses, determines whether discrepancies have been resolved, follows up on nonresponses within the stated time frame, and maintains the tracking database. However, inappropriate information is not always removed. Additionally, disagreements on the inappropriateness of the information require a timely decision from an adjudication authority.

Management Comments on the Finding

Although not required to comment, the Director of Information Operations, Chief Information Officer, Defense Logistics Agency provided comments to the draft audit report. She concurred with the finding and recommendations and suggested several editorial changes.

Recommendations, Management Comments, And Audit Response

1. We recommend that the Assistant Secretary of Defense (Command, Control, Communications, and Intelligence):

a. Suspend Web pages that contain potentially inappropriate information identified in the Joint Web Risk Assessment Cell reports as part of the adjudication process until resolution is achieved.

Management Comments. The Deputy Assistant Secretary of Defense (Security and Information Operations) provided comments for the Assistant Secretary of Defense (Command, Control, Communications, and Intelligence). She non-concurred with the recommendation and stated that the Web site posting review process is part of Operations Security, which is governed by DoD Directive 5205.2, "DoD Operations Security Program." The Directive recognizes that decisions regarding operational security are made by those responsible for mission accomplishment. Consequently, the Web posting responsibility is within the scope of the local commander's authority unless a higher adjudicating authority overturns the decision on appropriateness of page content. The Deputy Assistant Secretary stated that because the information in dispute is not classified, there is no reason to preempt the decision of command authority pending resolution of any disagreement.

Audit Response. Management comments were not responsive. Although the Deputy Assistant Secretary nonconcurred with the recommendation, it is evident that existing procedures used by local commanders are not adequate. Inappropriate information on 30 of 200 DoD Web site locations was still available to the general public in May 2002, almost 8 months after the JWRAC issued the September 2001 report. Of the 30 disclosures 14 (46 percent) contained

potentially major violations because they showed operation plans and "For Official Use Only" data. Additionally, unclassified data may through compilation also pose security risk. Accordingly, information that may place DoD at increased risk must be suspended until resolved through an adjudication process.

b. Establish a corresponding mechanism in the "Joint Web Risk Assessment Cell's Standard Operating Procedures for Discrepancy Reporting and Tracking," that adjudicates disagreements on inappropriate information between the Joint Web Risk Assessment Cell and Web-site owner.

Management Comments. The Deputy Assistant Secretary partially concurred with the recommendation. She agreed that a timely adjudication process is required to resolve questions or disagreements on the appropriateness of information posted on public Web sites. However, she stated that the Joint Web Risk Assessment Cell's Concepts of Operations gives the Director of the Defense Information Systems Agency the responsibility and authority to establish operating procedures. The Deputy Assistant Secretary agreed to work with Defense Information Systems Agency to define a mechanism for adjudicating disagreements over findings. Once it is defined, she agreed to include the mechanism in the Joint Web Risk Assessment Cell's Standard Operating Procedures for Discrepancy Reporting and Tracking.

Audit Response. Although the Deputy Secretary partially concurred, her proposed actions will meet the intent of the recommendation.

2. We recommend that the Director, Defense Information Systems Agency complete, publish, and comply with the "Joint Web Risk Assessment Cell Standard Operating Procedures for Discrepancy Reporting and Tracking," and maintain an up-to-date database of reported violations.

Management Comments. The Defense Information Systems Agency concurred with the recommendation. Management stated that the Joint Web Risk Assessment Cell's Standard Operating Procedures for Discrepancy Reporting and Tracking is under final review and expected to be published by June 2002. Officials informed us that it was published July 1, 2002. Also, a database system to track the Web risk-assessment activities is expected to be online in the first quarter of 2003.

Appendix A. Scope and Methodology

Scope and Methodology

We visited the Defense Logistics Agency; the Defense Supply Center-Richmond; the General Counsel, Office of the Secretary of Defense; and the U.S. Space Command. We selected the Defense Logistics Agency because of the number of publicly accessible Web sites that were registered in the Defense Link. We selected the Defense Supply Center-Richmond because it is one the Defense Logistics Agency's publicly accessible Web sites. We selected the General Counsel, Office of the Secretary of Defense and the U. S. Space Command because of the number of potential violations identified in the August 2001 report of the Office of the Deputy Assistant Secretary of Defense (Intelligence). We reviewed and evaluated the Web site policies and conducted discussions with officials in the Office of the Assistant Secretary of Defense (Command, Control, Communications, and Intelligence); the Defense Logistics Agency; the Defense Supply Center-Richmond; General Counsel, Office of the Secretary of Defense; and the U.S. Space Command to evaluate whether policies and practices for publicly accessible DoD Web sites were adequate. We reviewed records and documents dated from December 1998 through May 2002.

General Accounting Office High-Risk Area. The General Accounting Office has identified several high-risk areas in DoD. This report provides coverage of the Information Security high-risk area.

Audit Dates and Standards. We performed this audit from May 2001 through May 2002 in accordance with generally accepted government auditing standards.

Use of Computer-Processed Data. We relied on computer-processed data without performing tests of system general and application controls to confirm the reliability of the database. However, not establishing the reliability of the database will not affect the results of our audit. We relied on judgmental sampling procedures to develop conclusions on this audit.

Contacts During the Audit. We visited or contacted individuals and organizations within DoD. Further details are available on request.

Management Control Program Review

DoD Directive 5010.38, " Management Control Program," August 26, 1996, and DoD Instruction 5010.40, "Management Controls Program Procedures," August 28, 1996, require DoD managers to implement a comprehensive system of management controls that provide reasonable assurance that programs are operating as intended and to evaluate the adequacy of the controls.

Scope of the Review of the Management Control Program. We reviewed the adequacy of DoD management controls over DoD policies and practices for Web site administration and oversight. In assessing those controls, we evaluated

policies and practices on how Government or other servers host official DoD Web sites, and how DoD registers and monitors Web sites for compliance with policy and safeguards sensitive information. We reviewed management's self-evaluation applicable to those controls.

Adequacy of Management Controls. We identified material management control weaknesses for the Assistant Secretary of Defense (Command, Control, Communications, and Intelligence) as defined by DoD Instruction 5010.40. DoD management controls were not adequate to prevent the continued disclosure of inappropriate data on DoD Web sites that were identified by the Joint Web Risk Assessment Cell. In addition, the process for reporting and maintaining a database of inappropriate information contained on publicly accessible Web sites was not being followed.

The recommendations, if implemented, will improve the oversight and Web site administration processes. A copy of the report will be provided to the senior officials responsible for management controls in the Office of the Assistant Secretary of Defense (Command, Control, Communications, and Intelligence).

Adequacy of Management's Self-Evaluation. In FY 2000, the Assistant Secretary of Defense (Command, Control, Communication, and Intelligence) did not identify oversight of DoD and Service Web sites as an assessable unit and, therefore, did not identify or report the material management control weakness identified by the audit.

Prior Coverage

During the last 5 years, GAO has issued two reports, the Inspector General of the Department of Defense has issued three reports, and the Naval Audit Service issued one report on the issue of Internet privacy.

General Accounting Office

GAO Report No. GAO-01-147R, "Internet Privacy: Federal Agency Use of Cookies," October 20, 2000

GAO Report No. GAO/AIMD-00-296R (OSD Case No. 2074), "Internet Privacy: Comparison of Federal Agency Practices With FTC's Fair Information Principles," September 11, 2000

Inspector General of the Department of Defense (IG DoD)

IG DoD Audit Report No. D2001-130, "DoD Internet Practices and Policies," May 31, 2001

IG DoD Audit Report No. D2002-0062, "Air Force Web Site Administration, Policies, and Practices," March 13, 2001

IG DoD Audit Report No. D2002-0098 "Army Web Site Administration, Policies, and Practices, " June 5, 2002

Naval Audit Service

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

Appendix B. Results of Reviews at Selected DoD Organizations

Defense Logistics Agency. The Defense Logistics Agency has 28 publicly accessible Web sites that are registered in the Defense Link. In addition, the Chief Information Officer, Defense Logistics Agency issued "Defense Logistics Agency Internet Guidance," August 28, 2000, that addressed Web sites' administration. The guidance states that the Public Affairs Officer is the release authority for public information. The guidance requires Public Affairs approval in coordination with Internet Council approval before information is first posted on a Web site and also when significant changes occur to previously released information. In addition, the guidance established an Internet Council to periodically review DLA Web sites to ensure that only appropriate information is posted. The guidance also requires Web sites to be registered in the Defense Link.

The Internet Council at the Defense Logistics Agency is responsible for ensuring compliance with Agency guidance and approving Web pages for posting. However, officials at the Defense Logistics Agency did not conduct the required annual reviews, train Web administration officials, and provide oversight to determine that only appropriate information was posted to its Web site. In addition, in August 2001, the Office of the Deputy Assistant Secretary of Defense (Intelligence) identified a Defense Logistics Agency Web site that contained "For Official Use Only" information. When we notified Web administration officials of the inappropriate information, they removed the document from the Web site.

We visited a Web master at the Defense Supply Center-Richmond who maintains a Defense Logistics Agency Web site. The Web site was registered in the Defense Link, officials provided training for Web editors on Web site policy and procedures, and the Web master conducted annual content reviews.

Because only one Web site contained inappropriate information and because officials removed it upon notification, agreed to conduct documented annual reviews, to develop a checklist to conduct the annual reviews, and to develop classes for training Web administrators, we considered those actions responsive and, accordingly, did not make a recommendation in this report. Since the draft report was issued, DLA began the annual review process and documentation by developing the checklist and also began to develop training for Web administrators. (See the Management Comments section for the complete text of management comments.)

Office of the General Counsel. The Office of the General Counsel for the Secretary of Defense has four publicly accessible Web sites that are registered in the Defense Link. Although the General Counsel does not have written Web site policy, officials stated that they follow the 1998 DoD Policy; however, they did not conduct the required annual review.

In August 2001, the Office of the Deputy Assistant Secretary of Defense (Intelligence) identified that the General Counsel's Web sites contained

21 postings that included the wording "For Official Use Only, Until Released by…." The postings were statements of DoD officials before Congress. The statements were released for public viewing by the congressional committee. However, General Counsel officials did not delete the restrictive language before posting it to their Web page.

During our review, officials issued written guidance to implement the 1998 DoD Policy establishing a process for the release of information on the General Counsel Web site. The guidance provided examples of information that should not be posted on Web sites that are available to the public. Officials agreed to conduct annual reviews and document the results. In addition, they removed the restrictive language on Web pages that we identified as potentially inappropriate. We viewed the Web pages and verified that the restrictive language had been removed. Accordingly, we considered this a matter of interest and did not make a recommendation.

U.S. Space Command. The U.S. Space Command has two Web sites that are registered in the Defense Link. Officials developed a draft operating instruction addressing the use of Internet and public Home pages. Because the U.S. Space Command is a tenant organization on Peterson Air Force base, it follows Air Force policy for establishing a Web site. This policy includes an initial review of Web site information by the Privacy, Staff Judge Advocate, and Public Affairs offices.

However, Web administrative officials had not conducted the required annual reviews, established a training program for Web officials, or published policy for Web page management. Also, in August 2001, the Office of the Deputy Assistant Secretary of Defense (Intelligence) identified social security numbers at two U.S. Space Command Web sites. The Web sites that contained the potential violations were Canadian Forces Web sites that were linked to the Space Command site. Canadian officials stated that they do not use social security numbers and could not review the site's content because the site had been removed. U.S. Space Command officials deleted the link to the Canadian site because the site contained outdated information and had been removed from public viewing. Officials agreed to conduct annual reviews and document results, update and publish guidance, require training for the Web master, and identify a process to establish and update Web pages. Accordingly, we did not make any recommendations.

Appendix C. Report Distribution

Office of the Secretary of Defense

Under Secretary of Defense (Comptroller)/Chief Financial Officer
    Deputy Chief Financial Officer
    Deputy Comptroller (Program/Budget)
Assistant Secretary of Defense (Command, Control, Communications, and Intelligence)
General Counsel, Secretary of Defense

Unified Command

Commander, U. S. Space Command

Other Defense Organizations

Director, Defense Information Systems Agency
Director, Defense Logistics Agency

Non-Defense Federal Organization

Office of Management and Budget

Congressional Committees and Subcommittees, Chairman and Ranking Minority Member

Senate Committee on Appropriations
Senate Subcommittee on Defense, Committee on Appropriations
Senate Committee on Armed Services
Senate Committee on Governmental Affairs
House Committee on Appropriations
House Subcommittee on Defense, Committee on Appropriations
House Committee on Armed Services
House Committee on Government Reform
House Subcommittee on Government Efficiency, Financial Management, and Intergovernmental Relations, Committee on Government Reform
House Subcommittee on National Security, Veterans Affairs, and International Relations, Committee on Government Reform
House Subcommittee on Technology and Procurement Policy, Committee on Government Reform

Assistant Secretary of Defense for Command, Control, Communications, and Intelligence Comments

COMMAND, CONTROL, COMMUNICATIONS, AND INTELLIGENCE

OFFICE OF THE ASSISTANT SECRETARY OF DEFENSE
6000 DEFENSE PENTAGON
WASHINGTON, DC 20301-6000

June 14, 2002

MEMORANDUM FOR DIRECTOR, ACQUISITION MANAGEMENT,
DEPARTMENT OF DEFENSE INSPECTOR GENERAL

SUBJECT: Draft Audit Report on DoD Web Site Administration, Policies, and Policies (Project No. D2001AB-0116.002), May 9, 2002

This office appreciates the opportunity to comment on the subject report. The Joint Web Risk Assessment Cell (JWRAC) and its service counterparts are making important contributions to the security of the Department's web-based information.

This office non-concurs with the recommendation to suspend web pages that contain potentially inappropriate information until resolution of differences on whether the disclosures were appropriate or not. The basis of the required web site posting review process is Operations Security (OPSEC). DoD Directive 5205.2, "DoD Operations Security (OPSEC) Program," recognizes that decisions regarding OPSEC implementation are made by those with the responsibility for mission accomplishment. Thus, web posting decisions based on OPSEC evaluations are within the scope of authority of the local commander, and until a higher adjudication authority determines differently, the local commander's determination of appropriateness is the overriding one. As the information in dispute is not classified, there is no generally compelling reason to preempt the decision of command authorities pending resolution of such disagreements.

This office partially concurs with the recommendation to establish an adjudication mechanism. We agree that a timely adjudication process is required to resolve questions or disagreements on the appropriateness of information posted to public web sites. However, the Concept of Operations approved by the Deputy Secretary of Defense

assigned the Director, Defense Information Systems Agency (DISA) the responsibility and authority to establish operating procedures. This office will work with DISA, and the JWRAC, to define a mechanism for adjudication of disagreements over findings that can be incorporated by DISA into the JWRAC Standard Operating Procedures.

Carol A. Haave
Deputy Assistant Secretary of Defense
(Security and Information Operations)

Defense Information Systems Agency Comments

DEFENSE INFORMATION SYSTEMS AGENCY
701 S. COURTHOUSE ROAD
ARLINGTON, VIRGINIA 22204-2199

IN REPLY
REFER TO: INSPECTOR GENERAL (IG) 7 June 2002

MEMORANDUM FOR DOD Inspector General,
ATTN: Mr. Burton/Mr. Bartoszek

SUBJECT: Draft Audit Report, DOD Web Site Administration, Policies and Practices (FOUO)
2001AB-0116.002

1. The enclosed document provides the response from the Defense Information Systems Agency on recommendation 2, page 7.

2. If you have any questions, please call Liz Lippmann, Audit Liaison, at 703.607-6306 or Teddie Steiner, Audit Liaison, at 703.607-6316.

FOR THE DIRECTOR:

Enclosure a/s

RICHARD T. RACE
Inspector General

Quality Information for a Strong Defense

DODIG DRAFT AUDIT REPORT
D2001AB-0116.002
DOD WEB SITE ADMINISTRATION, POLICIES AND PRACTICES

RECOMMENDATION 2: Recommend the Director, DISA, complete, publish and comply with the "Joint Web Risk Assessment Cell (JWRAC) Standard Operating Procedures for Discrepancy Reporting and Tracking," and maintain an up-to-date database of reported violations.

DISA RESPONSE: Concur with the recommendation. We are using the SOP referenced in the audit report and have undertaken the development of a database. The SOP is currently undergoing final review and is expected to be final and published on 30 June 2002. The database system is expected to be online in 1Q03. The database is designed to track the web risk assessment activities of the JWRAC and the emerging Service WRACs.

Defense Logistics Agency Comments

DEFENSE LOGISTICS AGENCY
HEADQUARTERS
8725 JOHN J. KINGMAN ROAD, SUITE 2533
FT. BELVOIR, VIRGINIA 22060-6221

IN REPLY
REFER TO

JUN 1 1 2002

J-65

MEMORANDUM FOR DIRECTOR, INVESTMENTS AND ACQUISITION (COMMAND, CONTROL, COMMUNICATIONS, AND INTELLIGENCE)

SUBJECT: Department of Defense Inspector General (DoDIG) Proposed Audit Report, D2001AB-0116.002, "DoD Web Site Administration, Policies, and Practices," May 9, 2002

This is the DLA response to the DoDIG Proposed Audit Report, D2001AB-0116.002, dated May 9, 2002, Web Site Administration, Policies, and Practices.

DLA concurs on the proposed audit report and our comments are attached.

The point of contact for this effort is Ms. Becky Perry who can be reached at (703) 767-2163 or e-mail: becky_perry@hq.dla.mil.

MAE DE VINCENTIS
Director, Information Operations
Chief Information Officer

Attachment

cc:
DUSD (L&MR)
DUSD (ARA)
J-308

Federal Recycling Program Printed on Recycled Paper

Comment Matrix
for
Audit Report: DoD Web Site Administration, Policies, and Practices

Priority Key: 1 – Will nonconcur unless this change is made.
2 – Strongly recommended change.
3 – Suggested change.

No.	Pg.	Para.	Component	Comments and Disposition	Pri.
1.	11	1	DLA	DoD should be changed to *DLA*	2
2.	11	2	DLA	The required annual reviews were not *adequately documented* rather than not conducted at all.	2
3.	11	2	DLA	There was no *official* training rather than no training at all.	2
4.	11	Replace 4th	DLA	Only one web site contained inappropriate information. Because officials removed it upon notification, the process for annual reviews and the documentation of these reviews has begun, a checklist is being used to document the reviews, and DLA is in the process of developing a training plan for the web administrators and content managers. We consider these actions responsive. Accordingly, we did not make a recommendation in this report.	2

Attachment 1

Team Members

The Acquisition Management Directorate, Office of the Assistant Inspector General for Auditing of the Department of Defense prepared this report. Personnel of the Office of the Inspector General of the Department of Defense who contributed to the report are listed below.

Mary L. Ugone
Bruce A. Burton
Thomas S. Bartoszek
Thomas J. Hilliard
Thelma E. Jackson
Carrie J. Gravely
Mandi L. Markwart
Jenshel D. Marshall
Jacqueline N. Pugh