June 5, 2002

Information System Security

Army Web Site Administration, Policies, and Practices
(D-2002-098)

Department of Defense
Office of the Inspector General

Quality *Integrity* *Accountability*

Report Documentation Page

Report Date	Report Type	Dates Covered (from... to)
05 Jun 2002	N/A	-

Title and Subtitle Information System Security: Army Web Site Administration, Policies, 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 (Room 801) Arlington, VA 22202-2884	**Performing Organization Report Number** D-2002-098
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 29	

Copies

To obtain additional copies of this audit 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.

Acronym

GILS	Government Information Locator Service

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

June 5 2002

MEMORANDUM FOR AUDITOR GENERAL, DEPARTMENT OF THE ARMY

SUBJECT: Audit Report on Army Web Site Administration, Policies, and Practices (Report No. D-2002-098)

We are providing this report for information and use. We considered management comments on a draft of this report in preparing the final report.

The Army comments conformed to the requirements of DoD Directive 7650.3; therefore, additional comments are not required.

We appreciate the courtesies extended to the audit staff. For additional information on this report, please contact Mr. Thomas S. Bartoszek at (703) 604-9014 (DSN 664-9014) (tbartoszek@dodig.osd.mil) or Mr. Bruce A. Burton (703) 604-9071 (DSN 664-9071) (bburton@dodig.osd.mil). See Appendix B for the report distribution. 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-2002-098 **June 5, 2002**
(Project No. D2001AB-0116.001)

Army Web Site Administration, Policies, and Practices

Executive Summary

Who Should Read This Report and Why? Web site developers and administrators, operational security officers, public affairs officers, managers responsible for Web site content, and Web site users should read the reports in this series. Those involved with administering or overseeing Web sites will want to make sure that their content is appropriate.

Background. This report is the second in a series that addresses DoD Internet administration, policies, and practices. The first report addressed the Web site administration, policies, and practices of the Air Force. A subsequent report will cover Web site administration within the DoD. The Naval Audit Service issued a separate audit report on Web site administration within the Navy and the Marine Corps. The "DoD Web site Administration Policy and Procedures," (the Policy) November 25, 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 review all information placed on publicly accessible Web sites for security levels of sensitivity before the information is released. The Policy requires Components to establish procedures for management oversight and review of Web sites and to provide necessary resources to support Web site operations. The Policy also requires an annual security assessment of Web sites.

Results. The Army's publicly accessible Web sites contained inappropriate information, which was in contravention of Army Web Policy. As a result, potentially sensitive matters and information were not adequately protected. The Army needs to revise its policy for documenting and reporting review results, establish a system to resolve discrepancies, reconcile and verify its Web site inventory, establish a way to monitor the consistency of the Army Web site review and approval process, establish an Army Web Risk Assessment Cell, establish annual operational security reviews of Web sites, and establish a training requirement and curriculum for Army Web administration personnel.

Management Comments. The Army concurred with the recommendations. Its actions to establish the Army worldwide Intranet, consolidate Army National Guard and Army Reserve servers, update its Web site administration policy, and determine the training requirement for Web site administration personnel meet the intent of the recommendations; therefore, no further comments are required.

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 Components to establish a process to identify appropriate information for posting to Web sites and to review all information placed on publicly accessible Web sites for security levels of sensitivity before the information is released.

In addition, the Policy requires Components to establish procedures for management oversight and review 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 to ensure that information that could have a negative effect on U.S. military operations or personnel is not available on publicly accessible Web sites.

Moreover, Components must register each publicly accessible Web site with the Government Information Locator Service (GILS). The GILS helps citizens identify, locate, and retrieve information about the Government. The GILS resides on the Defense Link, which is the official Web site for DoD and the starting point for finding military information online for defense policy, organizations, functions, and operations.

The Policy defines a Web site as a collection of information that is organized into a number of Web documents. The information is related to a common subject or set of subjects 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. An official DoD Web site is developed and maintained with command sponsorship, approval, and editorial supervision over content.

DoD Oversight of Web Content. On February 25, 1999, the Secretary of Defense approved the Joint Web Risk Assessment Cell plan to use Reserve assets to conduct ongoing security and threat assessments of Components' publicly accessible Web sites. The Joint Web Risk Assessment Cell is responsible for analyzing data on DoD Web sites for information that poses potential or real threats to ongoing operations and DoD personnel. Inappropriate data include For Official Use Only, sensitive and classified information, and other information at one or more sites that, when combined, would be sensitive or classified and should not be released to the general public.

Army Policy on Web Sites. The Director of Information Systems for Command, Control, Communications, and Computers serves as the Chief Information Officer of the Army. Army Regulation 25-1, "Army Information Management," February 15, 2000, states that Army organizations will assign a Web master who will have technical control over updating each Web site's content and approving information for public release. Prohibited information, which includes information that is classified, For Official Use Only, protected under the Privacy Act, exempted under the Freedom of Information Act, and draft policy

publications must not be made available to the general public. In addition, Regulation 25-1 requires Army organizations that maintain Web sites to register with the Army Home Page. The Army Home Page is used by Army organizations and personnel to share information with Web users. Registration requires the submission of official record information such as Web site title, Internet address, major command, base location, point of contact, and other pertinent Web site data. Regulation 25-1 also states that the Training and Doctrine Command will formulate information management and information technology doctrine for the Army, and in coordination with the Director of Information Systems for Command, Control, Communications and Computers identify and analyze information management training requirements, and update existing courseware.

The Office of the Director of Information Systems for Command, Control, Communications, and Computers provided detailed guidance on Web site administration in "Guidance for Management of Publicly Accessible U.S. Army Web Sites," November 30, 1998, which defines the responsibilities of Army personnel in the establishment, and operation of Army Web sites. The guidance provides that officials who operate Army Web sites must control the Web sites' contents so that they comply with policies, and must periodically reevaluate each Web site under their control. Officials must ensure information posted on Web sites is accurate, timely, represents the official Army position and is properly cleared for public release. Additional prohibited information includes copyrighted trademarks, logos, and links to inappropriate commercial Web sites. Moreover, Army organizations that maintain Web sites must register with GILS and also notify the Army Web site when changes occur to the registration information.

Army Regulation on Public Affairs. Army Regulation 360-1, "The Army Public Affairs Program," September 15, 2000, states that public affair offices and security offices must review and approve DoD official information for public release.

Army Regulation on Operations Security. Army Regulation 530-1 "Operations Security," March 3, 1995, prescribes policy and procedures for operational security. Operations security is a process to protect and prevent the disclosure of any information that may jeopardize U.S. Forces performing their mission. Regulation 530-1 requires each Army organization to develop an Operations Security Program to protect critical information. The program should include a process to identify critical information, analyze threats and vulnerabilities, and assess risks and countermeasures. In addition, each year, major commands must submit a report on their programs to the Deputy Chief of Staff for Operations and Plans, who is the Army proponent for operations security.

Objectives

Our objective was to evaluate Army policies and practices for Web site administration and oversight. Specifically, we reviewed how the Army hosts official Web sites, how the Army registers and monitors Web sites for compliance

with policy, and how the Army safeguards sensitive information. We also evaluated the management control program as it related to the overall objective. See Appendix A for a discussion of the audit scope and methodology, the management control program, and prior audit coverage.

Army Internet Administration, Policies, and Practices

The Army had publicly accessible Web sites that contained inappropriate information, which was in contravention of Army Web Policy. This condition occurred because:

- Army organizations did not employ consistent approval processes for reviewing information displayed on publicly accessible Web sites, and did not conduct periodic policy compliance and annual security reviews of publicly accessible Web sites;
- the Director of Information Systems for Command, Control, Communications and Computers did not coordinate with the Training and Doctrine Command to identify and implement training and curriculum requirements for Web administration personnel; and
- the Director of Information Systems for Command, Control, Communications and Computers did not provide oversight and was not aware of all publicly accessible Army Web sites.

As a result, potentially sensitive matters and information were not adequately protected.

Information on Army Public Web Sites

Joint Web Risk Assessment Cell Review of Army Web Sites. The Joint Web Risk Assessment Cell conducts ongoing security and threat assessments of DoD Components' publicly accessible Web sites. The Joint Web Risk Assessment Cell is responsible for analyzing data for information that poses threats to ongoing DoD operations or personnel and that should not be released to the general public. From June 2001 through August 2001, the Joint Web Risk Assessment Cell identified 77 publicly accessible Web sites that contained inappropriate information. The types of information identified on the Web sites were operational plans, personal information, policies and procedures on military operations, and documents marked For Official Use Only.

Types Of Inappropriate Information On Army Web Sites

Types of Information	Number of Web Sites Affected
Personal Information	4
For Official Use Only	11
Operational Plans	14
Policies and Procedures on Military Operations	48
Total	**77**

DoD IG Web Site Reviews. We performed in-depth reviews of Web site administration at the Army Forces Command, the Army Training and Doctrine Command, and 11 subordinate organizations. Through the Internet, we identified Web sites under the control of both commands that contained information prohibited by Army Web policy. For example, Forces Command organizations that we reviewed had Web sites that identified birth dates, family information, personal e-mail addresses, new equipment fielded, exercise data, or inappropriate links to commercial sites. The Army Training and Doctrine Command organizations that we reviewed also had Web sites that contained birth dates, family information, or inappropriate language. We provided each organization reviewed with the inappropriate information and were told by the officials that it would be removed.

The Army had publicly accessible Web sites that contained inappropriate information, which contravenes DoD Policy and Army Web policy and guidance and that should not be made available to the public. Web sites must be informative and contain only information that is appropriate for posting. The Army must prevent the disclosure of sensitive movements of military assets or personnel; locations of units, installations, or personnel; personal information protected under the Privacy Act; copyright information; trademarks and logos; and classified information on Army publicly accessible Web sites. In addition, information on Army Web sites must be accurate, timely, represent the official Army position, and must not have a negative effect on Army personnel and operational security.

Approval Process for Releasing Information

Although the November 30, 1998, Army guidance for managing publicly accessible Web sites and Army Regulation 360-1 require that all information posted to a Web site should be reviewed for appropriateness by the security and the public affairs offices, the 2 major commands and 11 subordinate organizations that we visited had inconsistent approval processes for releasing and publishing information on Web sites. The Forces Command requires public affairs offices to control the content of Web sites, and the Training and Doctrine Command provides that public affairs offices and staff judge advocate offices, when requested, will review material prior to posting to publicly accessible Web sites.

Army Forces Command. Forces Command policy, June 18, 2001, "World Wide Web Policy 25-01-2," requires that the public affairs offices review and approve all information posted to the Forces Command and subordinate commands' Web sites. The Office of Public Affairs is the approval authority for the release of information to the general public. The Office of Public Affairs and the Information Management Directorate reviewed and approved the release of information posted on the Forces Command Web site. The three subordinate organizations visited--the Reserve Command, the I Corps, and the Fifth Army--inconsistently followed the Forces Command's policy.

Army Reserve Command. The Office of Public Affairs operated the Reserve Command's Web site and reviewed and approved information posted on its Web site. One of the subordinate organizations, the 94th Regional Support Command, maintained a Web site operated by its Office of Public Affairs. However, the Office of Public Affairs did not review subordinate organizations' Web sites unless the Web page was hosted on the 94th Web site or if the organization requested a review. Another subordinate organization, the 70th Regional Support Command, stated that its Office of Public Affairs reviewed and approved information posted to its Web site and for subordinate units' Web sites when the Web sites were first initiated, but it did not review and approve subsequent information posted.

I Corps. At I Corps, the Office of Public Affairs, the Office of the Staff Judge Advocate, and the Directorate of Information Management reviewed and approved information posted on the I Corps and subordinate units' Web sites when the Web sites were first initiated but did not review and approve subsequent information posted.

Fifth Army. The Fifth Army Office of Public Affairs is the approval authority for the release of information and operates the Fifth Army Web site. However, the Office of Public Affairs did not review and approve information on subordinate units' Web sites at initiation and did not review and approve updates unless the Web page was hosted on the Fifth Army Web site.

Training and Doctrine Command. Training and Doctrine Command Regulation 25-70, July 7, 2000, "Network Services," provides that public affairs offices and staff judge advocate offices, when requested, will review material before it is posted to publicly accessible Web sites.

The Training and Doctrine Command Web site was reviewed and approved by the public affairs office and the staff judge advocate office only when requested. The Army Chaplain School obtained public affairs approval for all information posted on its Web site. The Army Finance School, the Recruiting and Retention School, and the Soldier Support Institute obtained public affairs review and approval for major updates to their Web sites. The Adjutant General School did not obtain approval because most changes were updates only. The Cadet Command Web site was reviewed and approved by the public affairs office and the staff judge advocate office only when requested.

The approval process for posting information on Web sites is necessary to ensure that only properly cleared information is released to the general public on Army Web sites. Although Web policy is the responsibility of the Director for Information Systems for Command, Control, Communications, and Computers, the release of information is the responsibility of the Chief of Public Affairs. Accordingly, the Chief of Public Affairs, in coordination with the Director of Information Systems for Command, Control, Communications, and Computers, must establish an oversight mechanism to monitor whether Army organizations are using consistent procedures for reviewing and approving all information posted to Web sites.

Periodic Policy Compliance and Annual Security Reviews

The DoD Policy requires annual security reviews of Web sites, but the Army guidance for management of public Web sites requires periodic policy compliance reviews of Web sites to evaluate compliance. In addition, Army Regulation 530-1 requires Army organizations to develop an Operations Security Program to protect critical information, conduct an annual review of the Operations Security Program, and report the results to the Deputy Chief of Staff for Operations and Plans. However, the 2 major commands and 11 subordinate organizations that we visited inconsistently performed security and policy compliance reviews.

Army Forces Command. Officials at the Forces Command stated that they periodically performed policy compliance reviews of their Web site without documenting the results; however, they did not perform an annual security review. In addition, officials stated that they did not perform periodic policy compliance reviews or annual security reviews of subordinate command Web sites, including the Reserve Command, the I Corps, and the Fifth Army because that responsibility rests with each organization that operates an official Web site.

Army Reserve Command. Officials at the Reserve Command periodically reviewed Reserve Command Web sites for compliance with policy and notified Web masters of needed correction. In August 2001, an operational security review performed on 90 Web sites showed that 20 percent of the Web sites were in violation. On July 5, 2001, an operational security review was performed on the Reserve Web site; however, officials stated that they did not perform annual security reviews of their subordinate units' Web sites. Two subordinate organizations, the 70th and 94th Regional Support Commands, did not conduct periodic policy compliance reviews and annual security reviews of their Web sites or their subordinate units' Web sites due to resource constraints.

I Corps and Fifth Army Commands. The I Corps and the Fifth Army Commands did not conduct periodic policy compliance reviews and annual security reviews of their Web sites or their subordinate units' Web sites because of resource constraints.

Training and Doctrine Command. Officials at the Training and Doctrine Command and the subordinate Cadet Command did not conduct periodic policy compliance reviews and annual security reviews of their Web sites or subordinate organizations' Web sites because of resource constraints. The Adjutant General School, the Army Finance School, and the Recruiting and Retention School also did not conduct periodic policy compliance reviews and annual security reviews of their Web sites because of resource constraints. The Soldier Support Institute stated that it performed periodic policy compliance reviews and quarterly operation security reviews but did not document the reviews. Only the Army Chaplain School performed documented annual security reviews in September 1999, 2000, and 2001 using the Army Operational Security Checklist for Publicly Accessible Web sites. The checklist assists reviewers in assessing operational security vulnerabilities and determining whether Web policy is being properly implemented for their publicly accessible Web sites. The 1999 review performed

by the Office of Public Affairs and the Chaplain School Webmaster identified and corrected six instances where inappropriate information was posted or where required information, such as a Privacy statement, was missing from the Web site. The 2000 review identified no deficiencies. The 2001 review identified and corrected four instances of inappropriately posted information.

Security Reviews after September 11, 2001. After the terrorist attacks on September 11, 2001, the Forces Command reviewed its Web site for operational security information and made necessary corrections. Officials stated that they also plan to review subordinate organizations' Web sites for operational security information. The Chief, Army Reserve Command issued a memorandum dated September 20, 2001, that requires all subordinate units to perform an operational security review of their Web sites, make needed changes, and submit the sanitized Web site to the Reserve Command for final review and approval. The Reserve Command Web site was also reviewed for operational security after the attack. The Training and Doctrine Command Emergency Operations Center issued a tasking to review all public communications, including Web pages, to ensure that operational security information is not released in public forums.

Major commands must evaluate each Web site under their control for compliance with Army policy and to protect operational security. Both periodic policy compliance reviews and annual security reviews are a necessary part of Web site administration to prevent information that could affect operational security from being posted on publicly accessible Army Web sites. Army Web Administration policy requires periodic policy compliance reviews but does not require annual security reviews of Web sites. Also, Army Policy does not require the results to be written or a followup system to resolve identified potential inappropriate postings.

The Director for Information Systems for Command, Control, Communications, and Computers must revise the Army Web administration guidance to require documented periodic policy compliance reviews of publicly accessible Web sites and a followup system to resolve discrepancies concerning operational and other issues identified during the reviews. The Deputy Chief of Staff for Operations and Plans must ensure that major commands' operational security personnel perform independent, annual operational security reviews of Web sites as part of the Operational Security Program and annual Operational Security Report.

Training of Web Administration Personnel

Web Administration Training. Army Regulation 25-1 requires that the Training and Doctrine Command formulate information management and information technology doctrine for the Army, and in coordination with the Director of Information Systems for Command, Control, Communications, and Computers identify and analyze information management training requirements, and update existing courseware. The Training and Doctrine Command officials indicated that they had not developed training requirements and course material for Web administration personnel.

Forces Command. The Forces Command did not have a training requirement and did not provide Web administration personnel with training on Web site administration. However, the Forces Command Web page did provide guidance on Web site issues, including Web procedures. The Army Reserve Command, the Fifth Army and the 94th Reserve Support Command did not offer policy training to their Web administrators. The 70th Reserve Support Command developed a training course on Web site policy that included Web Administrator responsibilities and publishing guidelines. The I Corps developed a Web Administrator policy course that included responsibilities of Web administration personnel and identified types of prohibited information. The I Corps also provided links to Web policy and guidance at its Web site.

Training and Doctrine Command. The Training and Doctrine Command did not provide its organizations with training on Web administration; however, it did provide access to DoD, Army, and Training and Doctrine Command Web policies. Web administrators must receive training in Web site administration policy so that Web administration personnel are cognizant of guidance and requirements for Web site administration. Trained personnel provide an additional assurance that information on publicly accessible Web sites is appropriate for public viewing.

Air Force Lessons Learned. Our review of the Air Force Web administration identified that the Air Force Communications Agency was developing a computer-based training course for Web masters and other Web administration personnel. The course includes a 4-hour session with a 1-hour review, followed by questions that must be answered with a 70-percent correct score for successful completion of the course. Instruction topics include Web administration, roles of personnel, the Web server, system security, Web site establishment, page design, and the collection of information. The training will enable participants to perform essential Internet administration tasks and manage the enterprise in a secure manner.

The Director of Information Systems for Command, Control, Communications, and Computers must coordinate with the Training and Doctrine Command to establish an Army Web administration training requirement and curriculum. All personnel should complete the training before being assigned Web duties. The Director for Information Systems for Command, Control, Communications, and Computers should request the Training and Doctrine Command use the already developed Air Force training as a starting point for an Army training and education program in Web administration.

Army Web Site Inventory

The number of publicly accessible Army Web sites is unknown. Army policy requires registration of publicly accessible Web sites in the GILS and with the Army Home Page. Listings of Army Web sites accessible to the general public as shown on the Army Home Page were different than those registered in GILS. As of December 11, 2001, 459 Army Web sites were listed on the Army Home Page.

The GILS contained 374 Army listings. Only 43 were listed at both sites with the remainder listed either in GILS (331) or on the Army Home Page (416).

Although Web sites are required to be registered in both the Army Home Page and GILS, there is no requirement for both listings to be identical and up-to-date. Annually, major commands should correct the information in both listings and report discrepancies. Command oversight and identical registration will ensure that Army officials have a listing of all publicly accessible Web sites so that when changes to policy occur, the changes can be disseminated to Web officials; when training requirements are established, training can be planned and taken; and when commands perform periodic policy and annual security reviews, they will be able to analyze all publicly accessible sites. The Director for Information Systems for Command, Control, Communications, and Computers should revise Army Web Administration policy to require periodic reviews to reconcile Web site registration between the Army Home Page and GILS.

Monitoring Army Web Sites

The Army had not established a Web Risk Assessment Cell. Both the Air Force and the Navy have Web Risk Assessment Cells operated by reservists, which supplement the Joint Web Risk Assessment Cell. The Army Web Risk Assessment Cell could be responsible for vulnerability analyses and threat assessments of the content on Army Web sites. In addition, the Web Risk Assessment Cell could analyze content and data of Army Web sites, and review cross-sectional Web information, trend analysis, and aggregate data that could pose a threat to ongoing operations or personnel. Also, the Web Risk Assessment Cell could review Army Web sites for compliance with Army instructions, recognize and report vulnerabilities at one or more Web sites, and notify officials of the results. The Director for Information Systems for Command, Control, Communications, and Computers should establish a separate Web Risk Assessment Cell to facilitate reviews of Web sites for potential inappropriate information.

Summary

The GILS was established to help citizens identify, locate, and retrieve information about the Government. Web sites must be informative and contain only information appropriate for posting. To achieve this, managers who are responsible for Web administration, including posting information on Web sites, must be aware of the policy and process for establishing and revising Web sites, and appropriate Web page content. Information must be approved for public release. Training in Web site administration is a first step to safeguarding sensitive information along with establishing an oversight Web Risk Assessment Cell. In addition, performing periodic policy compliance reviews and annual security reviews of Web sites is imperative so that only appropriate information is posted. Further, a listing of Web administrators and Web sites that are consistently reported in DoD and Army databases will help facilitate the

distribution of new policy, assist in the oversight of known public Web sites, and ensure training of appropriate officials. All of those steps will help prevent the disclosure of sensitive movements of military assets or personnel; locations of units, installations, or personnel; personal information protected under the Privacy Act; copyright information; trademarks and logos; and classified information on Army publicly accessible Web sites.

Management Actions in Response to the Report

The Director of Enterprise Integration, Office of the Director of Information Systems for Command, Control, Communications, and Computers[1] provided the Army response. She stated that the Army has made progress in resolving many of the findings and recommendations that we identified in our report. Web content violations are being alleviated through the Army's strategy to improve business practices. Specifically, the Army has established the Army worldwide Intranet and single portal for the Army to conduct its business operations. Army organizations are moving their business information and applications to the security of the Army Intranet and removing the data from public Web pages. The Army also plans to consolidate all the Army servers including those of the National Guard and the Reserve. Control of the servers will be through three regional centers under the direct control of the Chief Information Officer, G-6. Additionally, Web policy was promulgated, formal management controls were developed, and an Army Web Risk Assessment Cell was created to strengthen Army Web site administration.

[1]The Director of Information Systems is now called the Chief Information Officer, G-6.

Recommendations, Management Comments and Audit Response

1. We recommend that the Director for Information Systems for Command, Control, Communications, and Computers:

a. Revise policy to require major commands to document periodic policy compliance reviews of publicly accessible Web sites, report results to the Director for Information Systems for Command, Control, Communications and Computers, and establish a followup system to resolve discrepancies identified.

Management Comments. The Director of Enterprise Integration partially concurred with the recommendation. The Director stated that the Army recently revised AR 25-1 "Army Information Management," to require Army organizations to designate a reviewer to clear information that is posted to the World Wide Web site. The reviewer is required to conduct routine reviews of Web sites on a quarterly basis to ensure compliance with DoD and Army policy. At a minimum, the review will include all of the Web site management control checklist items contained in Appendix B-4 of the AR 25-1 (see the Management Comments section). The revisions are awaiting the approval of the Secretary of the Army. Further, due to resource constraints, the Director did not concur with requiring major commands to report results of the periodic reviews to the Chief Information Officer. Instead, she stated that the requirement of report submissions through the chain of command from organizations that have been notified of specific violations on their Web sites would be supported, and the requirement of ad hoc reporting to the Chief Information Officer,G-6 on the violations that have been identified would be continued.

Audit Response. Although the Director nonconcurred with part of the recommendation, planned actions meet the intent of the recommendation.

b. Coordinate with the Training and Doctrine Command to establish a training requirement and curriculum for Army Web administrators and require that Web administration personnel be trained before being assigned Web duties.

Management Comments. The Director concurred with the recommendation and is coordinating with the Training and Doctrine Command and the Army Signal Center and School to determine the training requirement for Web site administration personnel.

c. Revise policy to require the reconciliation and verification of data contained on the Army Home Page with data contained in the Government Information Locator Service as part of the periodic review.

Management Comments. The Director concurred with the recommendation. The Army Web Risk Assessment Cell is performing a reconciliation to ensure

that every Army Web site has been properly registered in the Government Information Locator Service. Once the reconciliation is complete, the Army Web Risk Assessment Cell will conduct spot-checks to ensure registration in the Government Information Locator Service.

d. Establish an Army Web Risk Assessment Cell.

Management Comments. The Director concurred with the recommendation. On February 26, 2002, the Army established a Web Risk Assessment Cell to conduct routine reviews of Army Web sites for compliance with DoD and Army policies, conduct random reviews of Army Web sites, notify components of security concerns, ensure corrective action, and report corrective action results.

2. We recommend that the Deputy Chief of Staff for Operations and Plans require major commands' operational security personnel perform independent annual operational security reviews of Web sites as part of their Operational Security Program and annual Operational Security Report.

Management Comments. The Deputy Chief of Staff for Operations and Plans, now the Deputy Chief of Staff, G-3 concurred with the recommendation. The Deputy Chief of Staff will direct all major commands to add an annual review of their publicly accessible Web sites for operational security and address the results in their annual operational security reports.

3. We recommend that the Chief of Public Affairs, in coordination with the Director of Information Systems for Command, Control, Communications, and Computers, establish an oversight mechanism to monitor whether Army organizations are using consistent procedures for reviewing and approving all information posted to Web sites.

Management Comments. The Director concurred with the recommendation. She and the Public Affairs Officer will use performance measures established by the Army Web Risk Assessment Cell for assessing improvements in the security and compliance of the Army's Web sites.

Appendix A. Audit Process

Scope

Work Performed. We visited the Forces Command and the Training and Doctrine Command. We selected the Forces Command because it included the majority of Army units. We selected the Training and Doctrine Command because it was responsible for information technology training. The subordinate Components visited included the Reserve Command, the I Corps, Fifth Army, 70th Regional Support Command, 94th Regional Support Command, Cadet Command, Adjutant General School, Army Chaplain School, Army Finance School, the Recruiting and Retention School, and Soldier Support Institute. The results of our review of 2 major commands and 11 subordinate Components do not reflect a projection to all Army major commands and subordinate Components. We reviewed and evaluated Army Web site policies for publicly accessible Web sites. We conducted discussions with officials to evaluate whether policies and practices were adequate. We reviewed records and documents dated from November 1998 through December 2001.

Methodology

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 the audit.

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

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 (MC) Program," August 26, 1996, and DoD Instruction 5010.40, "Management Controls (MC) 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 Army management controls over DoD and Army 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 Army Web sites, how the Army registers and monitors Web sites for compliance with policy, and how the Army 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 Army as defined by DoD Instruction 5010.40. Army management controls for oversight of Army Web sites were not adequate to identify a complete listing of Web sites, conduct annual multi-disciplinary reviews, and establish a followup system to track inappropriate information posted. The recommendations, if implemented, will improve the oversight process and the Web site administration process. A copy of the report will be provided to the senior official responsible for management controls in the Office of the Assistant Secretary of Defense (Command, Control, Communications, and Intelligence).

Adequacy of Management's Self-Evaluation. The Director for Information Systems for Command, Control, Communications, and Computers did not identify oversight of Army Web sites as an assessable unit and therefore did not identify or report the material management control weakness identified by the audit.

Prior Audit Coverage

During the last 5 years, the GAO and the Inspector General of the Department of Defense both issued two reports 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, "Federal Agencies' Fair Information Practices," September 11, 2000

Inspector General of the Department of Defense (IG DoD)

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

IG DoD Report No. D2002-062 "Air Force Web site Administration, Policies, and Practices," March 13, 2002

Appendix B. Report Distribution

Office of the Secretary of Defense

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

Department of the Army

Commanding General, Forces Command, Department of the Army
Commanding General, Training and Doctrine Command, Department of the Army
Assistant Secretary of the Army (Financial Management and Comptroller)
Director of Information Systems for Command, Control, Communications, and Computers, Department of the Army
Deputy Chief of Staff for Operations and Plans, Department of the Army
Chief of Public Affairs, Department of the Army
Auditor General, Department of the Army

Other Defense Organization

Director, Defense Information Systems 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

Department of Army Comments

DEPARTMENT OF THE ARMY
OFFICE OF THE SECRETARY OF THE ARMY
107 ARMY PENTAGON
WASHINGTON DC 20310-0107

09 MAY 2002

Office, Director of Information
Systems for Command, Control,
Communications and Computers

MEMORANDUM FOR INSPECTOR GENERAL (IG), DEPARTMENT OF DEFENSE
(AUDITING), 400 ARMY NAVY DRIVE, ARLINGTON, VA 22202

SUBJECT: Comments on Draft Audit Report on Army Web Site Administration, Policies, and Practices (Project No. D2001AB-0116.001)

The purpose of this memorandum is to provide comments and recommendations on subject report.

In general, many of the findings and recommendations in the report address items the Army has already identified and made great progress in resolving. Web content violations are being alleviated through the Army's strategy to improve business practices and transform itself into a knowledge-based enterprise. The key vehicle of this change is the Army Knowledge Online (AKO), a worldwide Intranet and single portal for Army to conduct its business operations. Army activities are rapidly moving their business information and applications to the security of the AKO and removing the data from public web pages. Within the AKO, the information is further restricted to communities of interest which have a need to share and exchange information.

Another strategic initiative that will facilitate the management and control of the Army's web sites is the consolidation of Army's servers (including the National Guard and the Army Reserve). The consolidation mechanism will allow management and control of all of Army's web sites (to include routine scanning of content) as a function of server management. Control of the servers will be through three regional centers under the direct control of the Army Chief Information Officer (CIO)/G-6.

In addition to the strategic initiatives identified above, immediate measures have been taken to shore up the Army's web site administration, to include promulgation of additional policy, development of formal management controls, and establishment of an Army Web Risk Assessment Cell (AWRAC). These areas are detailed in comments specific to the recommendations on page 11 and other areas of the report. (Enclosure)

Please note that the Director of Information Systems for Command, Control, Communications, and Computers (DISC4) has been formally re-designated as the CIO/G-6. This response will refer to the CIO/G-6 title instead of the DISC4 title.

SAIS-EIG
SUBJECT: Comments on (Draft) Audit Report on Army Web Site Administration, Policies, and Practices (Project No. D2001AB-0116.001)

The point of contact is Ms. Arlene Dukanauskas, (703)614-0418, e-mail: arlene.dukanauskas@us.army.mil.

for Miriam F. Browning
Director of Enterprise Integration

Enclosure

Comments on Draft Audit Report on Army Web Site Administration, Policies, and Practices (Project No. D2001AB-0116.001)

Comments specific to the Recommendations (page 11)

(1) Reference Recommendation 1.a. Revise policy to require major commands to document periodic policy compliance reviews of publicly accessible Web sites, report results to the Director of Information Systems for Command, Control, Communications and Computers, and establish a followup system to resolve discrepancies identified.

Army policy in the AR 25-1 has been revised recently (and is currently awaiting Secretary of the Army signature) to require Army organizations to designate a reviewer to clear information posted to the WWW. The designated reviewer is required to conduct routine reviews of web sites on a quarterly basis to ensure that each web site is in compliance with the DOD and Army policy. The review will include, as a minimum, all of the web site Management Control Checklist items contained in Appendix B-4 of the AR 25-1. (Attachment to Enclosure)

The Office of the CIO/G-6 does not concur with major commands submitting routine reports on their reviews to the CIO/G-6 because we do not view it as an effective and efficient tool for determining web site compliance. We do support the requirement of report submissions through chain of command from activities that have been notified of specific violations in their web sites. We will continue to require ad hoc reporting to the Army CIO/G-6 based on violations that have been identified. Limited resources dictate that the Army CIO/G-6 focus on web sites with identified deficiencies and on building the AKO to support the needs of Army communities which have a need to share and exchange information internal to the Army. Greater utilization of AKO will reap the greatest benefits of the CIO's efforts. The web site focus areas will be identified by the Joint Web Risk Assessment Cell (JWRAC) and the AWRAC.

(2) Reference Recommendation 1.b. Coordinate with the Training and Doctrine Command to establish a training requirement and curriculum for Army Web administrators and require that Web administration personnel be trained before being assigned web duties.

The CIO/G-6 is currently coordinating with the Training and Doctrine Command and US Army Signal Center and School to determine the training requirement for web administration personnel. It should be noted that considerable web site administration and web security training is already offered in the Operational Security (OPSEC), Director of Information Management (DOIM), and the Information Assurance Security Officer courses.

(3) Reference Recommendation 1.c. Revise policy to require the reconciliation and verification of data contained on the Army Home Page with data contained in the Government Information Locator Service as part of the periodic review.

Army policy requires organizations maintaining publicly accessible web sites to register the site with the Government Information Locator Service (GILS)

at http://sites.defenselink.mil/. The AWRAC is performing a reconciliation process to ensure that every Army public web site has been properly registered in GILS. After the reconciliation process is concluded, the AWRAC will continue to do spot-checks of web sites to ensure registration in GILS, as required.

(4) Reference Recommendation 1.d. Establish an Army Web Risk Assessment Cell.

As stated in paragraph 3 of the memorandum, the AWRAC has been established. It was established 26 February 2002 to conduct routine reviews of Army web sites to ensure that they are in compliance with DoD and Army policies. The AWRAC mission is to:

a. Conduct random sampling of web sites to identify security concerns or review web site concerns provided by the JWRAC or Army leadership.
b. Review and verify initial findings and confirm that the web site is registered in the Government Information Locater Service (GILS).
c. Notify the website points of contact and their respective MACOM's Information Assurance Program Managers of suspense dates for reporting corrective actions.
d. Report results of corrective actions to the JWRAC and/or the Army CIO.

In coordination with the JWRAC and the Army CIO, the AWRAC is identifying and training additional personnel for the continuing mission of monitoring Army web sites. The AWRAC has established a process to assess and remediate policy and security concerns.

(5) Ref Recommendation 2. We recommend that the Deputy Chief of Staff for Operations and Plans require major commands' operational security personnel perform independent annual operational security reviews of Web sites as part of their Operational Security Program and annual Operational Security Report.

The ODCSOPS (now called the Deputy Chief of Staff, G-3) will direct all MACOMS to add an annual review of their publicly accessible web sites for OPSEC. Additionally, as a performance measure, MACOMs will be directed to address the results of this review, in their annual OPSEC reports.

(6) Ref Recommendation 3. We recommend that the Chief of Public Affairs in coordination with the Director of Information Systems for Command, Control, Communications and Computers establish an oversight mechanism to monitor whether Army organizations are using consistent procedures for reviewing and approving all information posted to Web sites.

The Offices of the CIO/G-6 and the Public Affairs have agreed to jointly review the effectiveness of the additional measures taken (as identified above) in improving web site administration practices. The performance measures established by the AWRAC will be used for assessing improvements in the security and compliance of the Army's web sites.

Other comment.

Reference page 4, last paragraph, last sentence, and page 5, Listing of Types of Inappropriate Information on Army Web Sites. Recommend you change the term "Internal Policies and Procedures" to "Policies and Procedures on military operations" or delete it altogether. Reason: Clarity. The term "internal" is vague and misleading. It could be interpreted as publications "internal to Army headquarters, major commands, or installations." Neither DoD nor Army policy prohibits the posting of "policy and procedure," per se. Both the DoD and the Army have public web sites which display its Departmental publications. Major commands and installations are not prohibited from displaying their authenticated publications. The prohibition is for policies and procedures of an operational nature which may pose a security risk. These areas are currently identified clearly in DoD and Army policy.

Management Control Checklist for Web Site Management Review (Extract from the AR 25-1).

Under Section d.

21. Does the web site contain a clearly defined purpose statement that supports the mission of the organization? (All)
22. Are users of each publicly accessible web site provided with a privacy and security notice prominently displayed or announced on at least the first page of all major sections of each web information service? (All)
23. If applicable, does this web site contain a Disclaimer for External Links notice for any site outside of the official DoD web information service (usually the .mil domain)? (All)
24. Is this web site free of commercial sponsorship and advertising? (All)
25. Is the web site free of persistent cookies or other devices designed to collect personally identifiable information about web visitors? (All)
26. Is each web site made accessible to handicapped users IAW Section 508 of the Rehabilitation Act? (All)
27. Is operational Information identified below purged from publicly accessible web sites? (All)
a. Plans or lessons learned which would reveal military operations, exercises or vulnerabilities?
b. Sensitive movements of military assets or the location of units, installations, or personnel where uncertainty regarding location is an element of the security of a military plan or program?
c. Personal Information about U.S. citizens, DoD employees and military personnel, to include the following:
- Social Security Account Numbers?
- Dates of Birth?
- Home Addresses?
- Home Telephone Numbers?
- Names, Locations, or any other identifying information about family members of DoD employees or military personnel?
d. Technological Data such as:
- Weapon Schematics?
- Weapon System Vulnerabilities?
- Electronic Wire Diagrams?
- Frequency Spectrum Data?
28. Are Operational Security (OPSEC) "Tip Off Indicators" in the following categories purged from the organization's publicly accessible web site? (All)
a. Administrative:
- Personnel Travel (personal and official business).
- Attendance at planning conferences.
- Commercial support contracts.
b. Operations, Plans, and Training:
- Operational orders and plans.
- Mission specific training.
- Exercise and simulations activity.
- Exercise, deployment or training schedules.
- Unit relocation/deployment.
- Inspection results, findings, deficiencies.
- Unit vulnerabilities or weaknesses.
c. Communications:
- Spectrum emissions and associated documentation.
- Changes in activity or communications patterns.
- Use of Internet and/or e-mail by unit personnel (personal or official business).
- Availability of secure communications.
- Hypertext links with other agencies or units.
- Family support plans.
- Bulletin board/messages between soldiers and family members.

Attachment

4

Enclosure

d. Logistics/Maintenance:
- Supply and equipment orders/deliveries.
- Transportation plans.
- Mapping, imagery and special documentation support.
- Maintenance and logistics requirements.
- Receipt or installation of special equipment.

29. Has the web site reviewer performed a Key Word Search for any of these documents and subsequently removed sensitive personal or unit information from publicly accessible web sites? (All)
- Deployment Schedules
- Exercise Plans
- Contingency Plans
- Training Schedules
- Inspection results, findings, deficiencies
- Biographies
- Family Support Activities
- Phone Directories
- Lists of personnel

Audit Team Members

The Acquisition Management Directorate of the 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
Lisa E. Novis
Thomas J. Hilliard
Thelma E. Jackson
Carrie J. Gravely
Mandi L. Markwart
Patrice A. Cousins
Constance E. Halahan
Jacqueline N. Pugh
Jenshel D. Marshall