Audit Report

DOD INTERNET PRACTICES AND POLICIES

Report No. D-2001-130 May 31, 2001

Office of the Inspector General
Department of Defense

Form SF298 Citation Data

Report Date *("DD MON YYYY")* 31May2001	**Report Type** N/A	**Dates Covered (from... to)** *("DD MON YYYY")*

Title and Subtitle DoD Internet Practices and Policies	**Contract or Grant Number**
	Program Element Number
Authors	**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 Number(s)** D-2001-130
Sponsoring/Monitoring Agency Name(s) and Address(es)	**Monitoring Agency Acronym**
	Monitoring Agency Report Number(s)
Distribution/Availability Statement Approved for public release, distribution unlimited	
Supplementary Notes	

Abstract
This report is in response to Section 646 of the Treasury and General Government Appropriations Act, 2001, as contained in Public Law 106-554 Consolidated Appropriations Act. Section 646 requires the Inspector General to submit a report to Congress that discloses DoD activity on collecting, creating, sharing, and reviewing personally identifiable information about individuals and their viewing habits at Government web sites. The Office of Management and Budget and DoD issued policy on privacy and data collection activities at Government web sites. That policy prohibits the use of web technology to collect identifying information to build profiles on individuals, and prohibits the use of persistent cookies unless certain conditions are met, including obtaining the personal approval of the head of the agency. That authority for DoD is the Secretary of Defense. Examples of the information-gathering technology are "persistent cookies,le iothird-party cookies,la and inweb bugs." Persistent cookies are a short string of text sent by a web server and stored on a user’s computer until a future expiration date. Third-party cookies are placed by a web site other than the site being visited. Web bugs are almost invisible graphics included on a web site or in an e-mail message that are designed to monitor those who visit the web site. Policy also requires the display of a privacy notice at principal web sites and locations where substantial personal information is collected from visitors. A privacy notice should inform visitors that the web site is public information and uses software programs to monitor for prohibited activities. In addition, the privacy statement should provide a point of contact for the web site.

Subject Terms

Document Classification unclassified	**Classification of SF298** unclassified
Classification of Abstract unclassified	**Limitation of Abstract** unlimited
Number of Pages 36	

Additional Copies

To obtain additional copies of this audit report, 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 or visit the Inspector General, DoD, Home Page at: www.dodig.osd.mil.

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, 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, D.C. 20301-1900. The identity of each writer and caller is fully protected.

Acronym

OMB	Office of Management and Budget

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

May 31, 2001

MEMORANDUM FOR ASSISTANT SECRETARY OF DEFENSE (COMMAND, CONTROL, COMMUNICATIONS AND INTELLIGENCE)
ASSISTANT SECRETARY OF THE AIR FORCE (FINANCIAL MANAGEMENT AND COMPTROLLER)
DIRECTOR, DEFENSE FINANCE AND ACCOUNTING SERVICE
DIRECTOR, DEFENSE INFORMATION SYSTEMS AGENCY
DIRECTOR, DEFENSE LOGISTICS AGENCY
NAVAL INSPECTOR GENERAL
AUDITOR GENERAL, DEPARTMENT OF THE ARMY

SUBJECT: Audit Report on DoD Internet Access, Practices, and Policies (Report No. D-2001-130)

We are providing this report for review and comment. This audit was performed in response to the Treasury and General Government Appropriations Act, 2001. We considered management comments on a draft of this report when preparing the final report.

DoD Directive 7650.3 requires that all recommendations be resolved promptly. The Deputy Assistant Secretary of Defense (Security and Information Operations) who responded for the Assistant Secretary of Defense (Command, Control, Communications and Intelligence), comments were responsive. However, we added Recommendation 2. to the final report that addressed a new DoD internet policy. Therefore, we request management comments on the new recommendation by July 2, 2001.

We appreciate the courtesies extended to the audit staff. For additional information on this report, please contact Mr. Raymond A. Spencer at (703) 604-9071 (DSN 664-9071) (rspencer@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.

David K. Steensma

David K. Steensma
Acting Assistant Inspector General
for Auditing

Office of the Inspector General, DoD

Report No. D-2001-130 **May 31, 2001**
(Project No. D2001AB-0065)

DoD Internet Practices and Policies

Executive Summary

Introduction. This report is in response to Section 646 of the Treasury and General Government Appropriations Act, 2001, as contained in Public Law 106-554 Consolidated Appropriations Act. Section 646 requires the Inspector General to submit a report to Congress that discloses DoD activity on collecting, creating, sharing, and reviewing personally identifiable information about individuals and their viewing habits at Government web sites.

The Office of Management and Budget and DoD issued policy on privacy and data collection activities at Government web sites. That policy prohibits the use of web technology to collect identifying information to build profiles on individuals, and prohibits the use of persistent cookies unless certain conditions are met, including obtaining the personal approval of the head of the agency. That authority for DoD is the Secretary of Defense. Examples of the information-gathering technology are "persistent cookies," "third-party cookies," and "web bugs." Persistent cookies are a short string of text sent by a web server and stored on a user's computer until a future expiration date. Third-party cookies are placed by a web site other than the site being visited. Web bugs are almost invisible graphics included on a web site or in an e-mail message that are designed to monitor those who visit the web site. Policy also requires the display of a privacy notice at principal web sites and locations where substantial personal information is collected from visitors. A privacy notice should inform visitors that the web site is public information and uses software programs to monitor for prohibited activities. In addition, the privacy statement should provide a point of contact for the web site.

Objectives. Our objective was to evaluate the DoD practices and policies on personally identifiable information gathered on individuals who access DoD Internet web sites.

Results. DoD issued privacy and data collection policy on DoD public web sites and took steps to validate compliance with Office of Management and Budget guidance on privacy. However, for 400 DoD Internet web sites reviewed, we identified:

- 128 persistent cookies, of which 38 were third-party commercial cookies, and 7 contained known web bugs.
- 100 sites that did not contain a privacy notice.
- 61 of 80 sites that requested voluntary personal information and did not contain a privacy notice.

Further, DoD was unaware of how commercial companies store, protect, and market information collected from DoD web sites. As a result, DoD Components and commercial companies supporting the web sites knowingly and unknowingly collected information on individuals without providing adequate disclosures in a privacy statement and without the approval of the Secretary of Defense. We did not specifically identify the type of information collected. Also, previous DoD assurances to the Office of Management and Budget that the requisite policies had been fully implemented were premature. For details of the audit results, see the Finding section of the report.

Management Actions. All 36 web masters whose sites contained collection devices agreed to remove the persistent cookies and web bugs, or remove the web site from the Internet. The web masters also agreed to verify that corrective actions were taken. In addition, on April 26, 2001, DoD updated the "DoD Web Site Administration Policies and Procedures," December 7, 1998, to incorporate changes in the Office of Management and Budget policy on privacy, data collection, and the use of cookies at Federal web sites. The April 26, 2001, policy update is in Appendix B.

Summary of Recommendations. We recommend that the Assistant Secretary of Defense (Command, Control, Communications and Intelligence), in consultation with the Defense Privacy Office, require the DoD Components to report on their actions to distribute DoD privacy and data collection policy to their web masters, provide their web masters with instructions to identify data collection devices, eliminate third-party cookies and other data collection devices, post privacy notices at major entry points to a site and at sites where substantial personal information is collected from the public, hold web masters accountable for compliance with DoD and Office of Management and Budget data collection policy on a continuing basis. We also recommended that the Assistant Secretary of Defense (Command, Control, Communications and Intelligence) revise the DoD Web Site Administration Policy to clearly show that the policy on the use of persistent cookies applies to non-user-identifying information and user-identifying information.

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) partially concurred with the recommendations and provided a completion date of August 31, 2001. He agreed that DoD used persistent cookies but that our report did not necessarily support a conclusion that the persistent cookies were being used to collect user-identifying information. The Director, Defense Privacy Office, stated that the report did not address whether the information collected was user-identifying data and whether the data were used in a prohibited manner or used to build profiles or track visitors' activities. The Director stated that the report assumed the web sites visited were principal web sites, known major entry points, or sites where substantial personal information is collected and therefore required privacy statements. The Deputy Assistant Secretary and the Director suggested changes to the report to consider recent policy changes and other points. The Finding section of the report contains a discussion of management comments. The complete text of management comments is in the Management Comments section.

Audit Response. Management comments to the recommendations were responsive. We acknowledge that our review did not specifically identify what type of information was collected. However, our review focused on whether collection devices, such as persistent cookies, existed at the web sites. As stated in the Office of Management and Budget policy, even if persistent cookies did not themselves contain personally identifiable information, such cookies can often be linked to a person after the fact, even where that was not the original intent of the web master. The Office of Management and Budget policy clearly applies to all uses of persistent cookies because by their very nature those cookies collect some type of information based on visits made by individuals to a web site. We used the Internet web sites listed in the Government Information Locator Service because it is the single entry point where the public can locate, access, and obtain DoD information. We made changes to the report based on the Director and Deputy Assistant Secretary comments. We revised and added recommendations. Accordingly, we request additional management comments by July 2, 2001.

Table of Contents

Background

Section 646 of the Treasury and General Government Appropriations Act 2001. As contained in Public Law 106-554, the Consolidated Appropriations Act requires the Inspector General of each Government Department to submit a report to Congress that discloses the agency's activity on collecting or reviewing singular data, or the creation of aggregate lists that include personally identifying information, about individuals who access the Department's Internet web sites. In addition, the Inspectors General must report agency activities relating to agreements with third parties, including other Government agencies, to collect, review, and obtain aggregate lists or singular data of personally identifiable information relating to an individual's access or viewing habits.

Internet Web Site. Congressional officials defined an Internet web site as an agency's principal web site, as well as any other major entry point that includes home pages of agency components and web sites that receive a high number of visits, and any web site where substantial amounts of personal information are collected or posted. Involuntary information can be collected through the use of cookies and web bugs.

Cookies. Cookies are short strings of text sent by a web server and stored on a user's system so it can later be read back from that system. Using cookies is a convenient technique for having the browser remember some specific information. Two types of cookies are used: domain and third-party. Domain cookies are placed by the visited web site. Third-party cookies are placed by a web site other than the site being visited. Cookies may also be either session or persistent cookies. Session cookies are short-lived and expire once the user exits the browser, whereas persistent cookies have specific expiration dates and remain on the client's computer until the specified expiration date. Persistent cookies can be used to track users' browsing behavior by identifying user's Internet web addresses.

Web Bug. A web bug is an invisible graphic included on a web site or in an e-mail message designed to monitor who visits the web site or reads e-mail messages. Web bugs may be used to add information to a personal profile of what sites a person is visiting. Other uses of web bugs include counting the number of people that visit a particular site, and gathering statistics about browser usage at different places on the Internet. Web bugs are not readily visible because they are very small.

Office of Management and Budget Privacy Policy. The Office of Management and Budget (OMB) Memorandum M99-18, "Privacy Policies on Federal Web Sites," dated June 2, 1999, directed agencies to post clear privacy policies on world wide web sites, at other known major entry points to the site, and on any web page where substantial personal information is collected from the public. The policy states that, if an agency collects information, it must disclose the information collected and why and how it will be used.

OMB Memorandum M-00-13, "Privacy Policies and Data Collection on Federal Web Sites," dated June 22, 2000, reaffirmed the June 1999 memorandum and

prohibits the use of cookies unless there is a compelling need to collect the data, a conspicuous notice is given by the collection activity, appropriate and publicly disclosed privacy safeguards are implemented for handling the data, and the collection is personally approved by the head of the agency. In the memorandum, OMB requested that all Federal agencies, as part of the agency budget submission, describe their privacy policy and steps to ensure compliance with the OMB guidance. On September 5, 2000, OMB issued clarifying guidance stating that the June 2000 guidance would apply to persistent cookies only.

DoD Privacy Guidance. Two years before OMB issued its policy on posting privacy notices, DoD had promulgated policies in that area in "Web Site Administration," December 7, 1998. Three years before OMB issued its policy on cookies, DoD established policies on collection of user-identifying information and the use of cookies in "Establishing and Maintaining a Publicly Accessible Department of Defense Web Information Service," July 18, 1997. Upon receipt of OMB Memorandum M-00-13, which reaffirmed its policy on privacy notices and established its cookie policy, DoD again issued privacy and data collection policy on DoD public web sites and took steps to validate compliance with OMB guidance on privacy.

DoD Memorandum, "Privacy Policies and Data Collection on DoD Public Web Sites," July 13, 2000, requires the display of a privacy notice at principal web sites and at locations where substantial personal information is collected from visitors. The policy does not permit the use of web technology to collect identifying information to build profiles on individuals. Also prohibited is the use of persistent cookies without notification in the privacy statement of what is being collected and how it would be used. In addition, the use of a persistent cookie must be personally approved by the Secretary of Defense.

On April 26, 2001, DoD updated the "DoD Web Site Administration Policies and Procedures," December 7, 1998, to incorporate changes in the Office of Management and Budget policy on privacy, data collection, and the use of cookies on Federal web sites. The changes prohibited the use of persistent cookies unless specific conditions were met and required the personal approval of the Secretary of Defense. The changes in part restated the July 13, 2000, memorandum on privacy. The changes are included in Appendix B.

Objectives

Our objective was to evaluate the DoD practices and policies on personally identifiable information gathered on individuals who access DoD Internet web sites. See Appendix A for a discussion of the audit scope and methodology and prior audit coverage.

DoD Internet Access, Practices, and Policies

DoD issued privacy and data collection policy on DoD public web sites and took steps to validate compliance with OMB guidance on privacy. However, for 400 DoD Internet web sites reviewed, we identified:

- 128 persistent cookies, of which 38 were third-party commercial cookies, and 7 contained known web bugs.
- 100 sites that did not contain a privacy notice.
- 61 sites that requested voluntary personal information and did not contain a privacy notice.

Further, DoD was unaware of how commercial companies store, protect, and market information collected from DoD web sites. Noncompliance with DoD and OMB policies occurred because the Services and DoD Components did not adequately disseminate guidance on privacy disclosure and on the use of collection devices to the web masters of DoD Internet sites, did not adequately educate the web masters on identifying collection devices, and did not have a process to verify compliance with DoD and OMB policy. As a result, DoD and commercial companies supporting the web sites knowingly and unknowingly collected information on individuals without providing adequate disclosures in a privacy statement and without the approval of the Secretary of Defense. We did not specifically identify the type of information collected.

DoD Implementation and Verification of Privacy Policies

Section 552a of the Privacy Act of 1974. Section 552a, title 5, United States Code of the Privacy Act of 1974 (the Act) states that individuals have a right to access agency records containing information about themselves and the right to request amendments to the records that are inaccurate, irrelevant, untimely, or incomplete. The Act applies only to Federal records that are retrieved by name or other personal identifier. The Act requires agencies to inform an individual of the authority for collecting, whether disclosure by the individual is voluntary or mandatory, the principal purposes for which the information will be used, the routine uses that may be made of the information, and the consequences of not providing the information. In addition, agencies must establish appropriate administrative, technical, and physical safeguards to ensure the security and confidentiality of the records

DoD Privacy Guidance. DoD Memorandum, "Privacy Policies and Data Collection on DoD Public Web Sites," July 13, 2000, requires the display of a privacy notice at principal web sites and where substantial personal information is collected from visitors. Privacy notices should inform visitors that the web site is public information, the Government collects information for statistical purposes, and it uses software programs to monitor for prohibited activities. In

addition, the privacy statement should provide a point of contact for the web site. The policy guidance prohibits the use of web technology to collect user-identifying information to build profiles on individuals, and prohibits the use of persistent cookies. It permits the use of web technology to obtain non-user-identifying information only if visitors are advised in the privacy statement of what is being collected, and why and how it would be used. In addition, the use of a persistent cookie must be personally approved by the Secretary of Defense. The memorandum requires Components to review their privacy practices and take corrective action to comply with policy.

Verification of OMB Guidance. To verify compliance with the July 13, 2000, DoD Memorandum, the Director, Administration and Management, Office of the Secretary of Defense, contacted DoD agencies, including the Services, to request that they report the status of their web sites' compliance with DoD policy and OMB guidance by October 2000. Twenty responded in writing that they had taken steps to ensure that their sites conformed to guidance. On December 14, 2000, the Office of the Assistant Secretary of Defense (Command, Control, Communications and Intelligence) reported to OMB that DoD Components' web sites complied with privacy guidance or, if not, that corrective actions were being taken to bring them into compliance.

DoD issued policy, obtained written confirmation of compliance, and reported to OMB that DoD Components complied with OMB guidelines on privacy policies for DoD Internet web sites.

Sample of DoD Internet Web Sites

Using the January 10, 2001, listing of DoD Internet web sites included in the Government Information Locator Service, we selected 400 DoD Internet web sites from a universe of 2,608 registered sites to review for the presence of persistent cookies, third-party commercial cookies, and web bugs; for privacy statements at Internet sites and at information collection locations; and for measures taken to safeguard the information collected. The Government Information Locator Service is the single entry point where the public can locate, access, and obtain DoD information. The universe and sample by Component are shown in Table 1.

Table 1. Universe and Sample of DoD Internet Sites Registered with the Government Information Locator Service

Component	Universe	Sample
Army	414	90
Navy	1,441	110
Air Force	416	90
Marines	172	60
Other[1]	165	50
Total	**2,608**	**400**

[1]Others include the Office of the Secretary of Defense, Defense agencies, the Unified Commands, and DoD Field Activities

Involuntary Collection of Personal Information

Collection Devices. At the 400 DoD web sites sampled, we identified 128 persistent cookies, including 38 placed by a commercial web site and 7 containing known web bugs. Table 2 displays by Service the number of web sites sampled, the number of persistent cookies, third-party cookies, and known web bugs.

Table 2. Sample of DoD Web Sites and Numbers of Sites That Contain Persistent Cookies, Third-Party Commercial Cookies, and Web Bugs

Component	Sample	Persistent Cookies	Third-Party Commercial Cookies	Web Bugs
Army	90	26	9	0
Navy	110	40	11	2
Air Force	90	29	6	2
Marine Corps	60	18	8	3
Other	50	15	4	0
Total	**400**	**128**	**38**	**7**

Persistent and Third-Party Cookies. We performed tests using the Microsoft Internet Explorer to identify persistent cookies. Where a persistent cookie appeared, we made a second visit to the site using a different computer at a different time to confirm the finding. During both visits, we documented the time and the date to validate the cookie. We identified 128 persistent cookies of which 38 cookies, or 30 percent, were third-party cookies placed by commercial web sites outside the DoD and Government community. Although we identified persistent cookies, DoD officials stated that the Secretary of Defense had not granted permission for any of the Services or DoD agencies to use them on DoD Internet web sites.

Web Bugs. At the 400 sites visited, we used a software program "Bugnosis Beta 5," provided by the Privacy Foundation, University of Denver, to profile DoD web sites for web bugs. A rating of 1 or more indicates that a web bug was probably in use at the site. Using the software program, we profiled 30 potential web bugs. After an analysis of the web site's software code, only 7 were determined to be known web bugs. However, based on the information available at the web site, we could not determine whether the 7 web bugs collected personal information. Two of the 7 had a DoD Internet web address with the suffix of ".MIL." The other 5 sites were commercial web addresses.

Web Masters and Involuntary Collection of Personal Information. We visited 36 web masters who managed the sites where we found 36 cookies and 3 known web bugs. A web master manages the web site and is responsible for the editorial content, quality, and style of the site. Of the 36 cookies, 14 were third-party cookies set by a commercial company. We asked the web masters whether they were aware of the cookie or web bug and whether they were aware of the DoD policy on these collection devices. Of the 36 webmasters, 10 were

aware of the collection device at those sites. Table 3 shows the number of web masters by Component who were aware of the cookie or web bug and their knowledge of the DoD policy.

Table 3. Web Masters Aware of the Collection Device

		Aware Of DoD Policy	
Component	Number	Yes	No
Army	3	1	2
Navy	1	0	1
Air Force	3	1	2
Marine Corps	2	0	2
Other	1	1	0
Total	**10**	**3**	**7**

Seven web masters were aware of the collection devices but were unaware of DoD policy. As a result, they did not review their web site for compliance. Three web masters who were aware of the collection device and DoD policy took no action to remove the device or ask permission to retain it. The web master for an Army site stated that he used a commercial service to locate his web site while awaiting a military address. The commercial service set a persistent cookie on visitors. The web master attempted to remove the cookie but could not because the site was controlled by a commercial company. After our visit, the web master agreed to conform his web site to DoD policy. An Air Force web master stated that a persistent cookie was placed by another Air Force base using a software program called "web trends," which provides web masters with statistical information on web site visitors. Since our visit, web site officials removed the persistent cookie from the program. The web master for a Defense Logistics Agency site stated that he obtained permission to use a persistent cookie; however, the Defense Logistics Agency granted permission to use a session cookie only. Officials agreed to remove the persistent cookie.

Of 36 web masters, 26 were unaware of the collection device at their sites. Table 4 shows the number of web masters by Component who were unaware of the cookie or web bug and their knowledge of the DoD policy.

Table 4. Web Masters Unaware of the Collection Device

		Aware Of DoD Policy	
Component	Number	Yes	No
Army	5	4	1
Navy	9	5	4
Air Force	6	2	4
Marine Corps	2	0	2
Other	4	3	1
Total	**26**	**14**	**12**

Fourteen web masters were unaware of a cookie or web bug on their site but were aware of the policy; however, they did not take steps to ensure that their web site was compliant. The other 12 web masters were not aware of the

cookie or web bug and were unaware of the policy. Consequently, they took no action. Web masters complained that they were not provided guidance on the DoD policy or instructions to identify persistent cookies or web bugs.

All of the web masters visited agreed to remove the persistent cookie, including commercial third-party cookies, web bug, or remove the web site from the Internet. The web masters agreed to perform reviews to verify that corrective actions have been taken.

Without knowing how to identify the persistent cookie and the DoD policy on collection devices, web masters cannot be assured that their sites are in compliance with DoD and OMB policy. The DoD Components must distribute DoD policy to each web master, provide instructions to identify collection devices, require them to eliminate cookies or third-party cookies that are not approved, and verify that web masters have complied with policy.

Privacy Statements At Web Sites and Voluntary Collection Locations

Privacy Statement. Of the 400 DoD Internet web sites that we sampled, we identified 100 that did not contain a privacy statement. Of those 100 web sites, 34 contained a security statement instead of a privacy statement stating that it was a DoD site and that DoD would monitor visitors to ensure authorized use only. For the 34 sites that placed persistent cookies on visitors, the security notice did not disclose what information was collected, why it was collected, and how it would be used.

In addition, 80 of the 400 web sites gathered voluntary personal information from visiting guests. For example, information solicited were names, e-mail addresses, office addresses, and telephone numbers. Of these 80 collection sites, 61, or 76 percent, did not contain a required privacy statement at the collection site as required by DoD policy. Table 5 displays the sample of web sites by Component, the number of web sites without a privacy statement, the number that collected personal information, and the number without a privacy statement at the personal collection location.

Table 5. Sample by DoD Component of Government Internet Web Sites, Without a Privacy Statement at the Web Site and at the Personal Collection Location

Component	Sample	Missing Privacy Statement at Web Site	Web Sites that Collect Voluntary Information	Missing Privacy Statement at Collection Location
Army	90	19	18	14
Navy	110	28	19	12
Air Force	90	26	22	18
Marine Corps	60	16	10	9
Other	50	11	11	8
Total	**400**	**100**	**80**	**61**

We visited 32 web masters who did not place a privacy statement at the web site and the data collection site, or who placed a security statement at the web site while employing cookies or web bugs. We asked them if they were aware of the missing privacy statement and aware of the DoD policy. Six of the 32 web masters indicated they were aware that their web site did not contain a privacy statement; however, they also stated that they had not been informed of the DoD policy to include a privacy statement on the web site. All agreed to take corrective action and include the necessary privacy notification.

Twenty three of 32 web masters stated that they were unaware of the missing privacy statement. We asked them whether they were aware of the DoD policy. Ten of the 23 web masters were aware of the DoD policy but did not review their site to ensure compliance because they thought their web sites already met the policy requirements. The other 13 were unaware of the policy and the missing statement and consequently took no action. Table 6 is a summary of the 23 web masters' knowledge of DoD policy on privacy statements.

Table 6. Web Masters Knowledge of Privacy Statements

		Aware Of DoD Policy	
Component	Number	Yes	No
Army	4	2	2
Navy	4	1	3
Air Force	6	3	3
Marine Corps	4	0	4
Other	5	4	1
Total	**23**	**10**	**13**

The remaining three web masters visited had web sites that did not contain a privacy statement at the entry page and at the data collection location. Officials stated that they were aware of the disclosure requirement at the entry page but not at the collection site. None of the three web masters made their web site compliant until our visit.

The Services and DoD agencies did not distribute the policy to all of the web masters. The web masters should be aware of the DoD policy on privacy statements and disclosure requirements. They must also review their web sites and collection locations for the presence of a privacy statement after they establish or revise the web site or after DoD issues new policy. In addition, DoD must verify compliance.

Security Over Information Collected

Security of Voluntary Information. We visited 17 web masters to review the security of the voluntary personal information collected. We discussed data access, computer logs, corrections to inaccurate information, and third-party collection activities. We also asked whether visitors could request correction to data submitted, whether information collected was combined with other personal information and whether information was sold or given away.

The web masters responded that they limited access to locations that stored personal information. All except one had procedures to limit access to locations that stored personal information, to protect voluntary information from unauthorized access through the use of passwords, and to delete information from storage locations when no long required. A Navy web master was uncertain how the voluntary information collected was stored and protected because the voluntary information was transferred to a centralized server outside his control; however, he agreed to determine what the procedures were for storage and protection. Web masters permitted corrections to voluntary information collected from visitors if inaccuracies existed. All stated that they had not sold or combined the information with other personal data to maintain or build profiles on visitors.

Although controls over the access to and use of voluntary information were adequate to ensure that the privacy of individuals was protected at DoD-controlled collection storage locations, no controls were present at 3 of 17 sites where web masters allowed third parties to use persistent cookies to collect involuntary information. At those sites, the web masters did not know what information the third party collected, how it was stored, and had little assurance that the information was protected and had not been sold or given away.

Conclusion

DoD privacy guidance requires the display of a privacy notice on principal web sites and at locations where substantial personal information from visitors is collected. It prohibits using web technology to collect identifying information; build profiles on individuals; and use persistent cookies except when visitors are advised of what is being collected, why, and how it will be used. The Secretary of Defense must approve the use of persistent cookies.

Although the DoD guidance was adequate, collecting and obtaining information on web site visitors by collection devices was present at 128 sites, or 32 percent of the sites sampled. The continued lack of privacy statements at web sites and collection locations and the use of third-party cookies indicated that previous DoD feedback to OMB that requisite policies had been fully implemented was

premature. Also, DoD has inadequate assurance that the involuntary collection of personal information by commercial companies at DoD web sites is safeguarded and not sold or given away after it is collected.

All DoD web masters must be made aware of the DoD and OMB policy that ensures the rights of individuals who visit DoD web sites will be protected. DoD web masters must be held accountable for compliance.

All 36 web masters visited whose sites contained collection devices agreed to remove the persistent cookies, including commercial third-party cookies, and web bugs, or remove the web site from the Internet. The web masters also agreed to verify that corrective actions were taken.

Management Comments on the Finding and Audit Response

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), stated that the Heads of Components are responsible for compliance to policy, and they generally delegate it to the sponsoring organization's commander and not to the web masters. He agreed that DoD used persistent cookies but that our report did not necessarily support a conclusion that the persistent cookies were being used to collect user-identifying information. He also stated that the updated policy following issuance of the OMB policy now prohibits all uses of persistent cookies without the specific waiver.

Although not required to comment, the Director, Defense Privacy Office, stated that he believed the congressional tasking was designed to determine whether Federal agencies were knowingly using web technology to collect information on visitors to Government public web sites and using it in a prohibited manner. He stated that the report did not address this aspect. He commented that the report stated that most web masters were unaware of the collection activity, which he believed constitutes an act of nonfeasance and not malfeasance. The Director also commented that the report provided no indication that those who were aware of the collection activity used the information to build profiles or track visitors, and that the report should clarify those results in its conclusion. He further stated that it was assumed that the web sites visited constituted a principal web site, a known major entry point, or a site where substantial personal information was collected. Many users bypass the major entry points where the privacy and security notices are posted. However, a visitor can review the privacy notice of the web site by visiting the major entry point where those notices are posted. The Director recommended that the report be revised to recognize recent policy changes regarding the use of persistent cookies and voluntary collection of information.

Audit Response. The June 22, 2000, OMB memorandum stated that because of the unique laws and traditions about Government access to citizens' personal information, the presumption should be that "cookies" will not be used at Federal web sites. The memorandum further stated that particular privacy concerns may be raised when use of web technology (such as persistent cookies) can track the activities of users over time and across different web sites.

Further, these concerns are especially great where individuals who have come to Government web sites do not have clear and conspicuous notice of any such tracking activities. The September 5, 2000, letter from OMB further clarified the June 2000 memorandum and stated that persistent cookies should not be used unless four conditions were met which included the approval by the head of the agency. Our review did not specifically identify what was collected. However, our review focused on whether collection devices, such as persistent cookies, existed at the web sites. As stated in the Office of Management and Budget September 5, 2000, letter, even if persistent cookies did not themselves contain personally identifiable information, such cookies can often be linked to a person after the fact, even where that was not the original intent of the web master. The Office of Management and Budget policy clearly applies to all uses of persistent cookies because by their very nature those cookies collect some type of information based on visits made by individuals to a web site. Also, the Deputy Assistant Secretary's response indicated that DoD policy had been updated following the issuance of OMB policy, and prohibited all uses of persistent cookies without a specific waiver. However, the April 26, 2001, policy update placed the policy on the use of persistent cookies under section 12.2.3, "Automated Collection of User-Identifying Information on Publicly Accessible Web Sites." By doing so, the policy on the use of persistent cookies appears to apply only to user-identifying information. The OMB policy clearly intended the policy on the use of persistent cookies to apply to both user-identifying and non-user-identifying information. Management comments were generally consistent with OMB policy; however, the April 26, 2001, policy update was not. Accordingly, we have added a recommendation to require DoD to correct its policy on the use of persistent cookies.

With respect to the Director's comments on the Internet web sites reviewed, we selected a sample of DoD web sites listed in the Government Information and Locator Service, which is the single entry point where the public can locate, access, and obtain DoD information.

We made changes to the report based on other comments made by the Deputy Assistant Secretary and the Director. Those changes are referenced in the Management Comments section of the report.

Recommendations, Management Comments, and Audit Response

Renumbered, Revised and Added Recommendation. As a result of management comments, we revised the recommendation to include the Defense Privacy Office to recognize its role in ensuring privacy policy compliance. We also added Recommendation 2. to correct the DoD policy concerning the use of persistent cookies.

1. We recommend that the Assistant Secretary of Defense (Command, Control, Communications and Intelligence), in consultation with the Defense Privacy Office, require the DoD Components to report on what they have done to:

a. Distribute DoD privacy and data collection policy to their web masters.

b. Provide their web masters with instructions to identify data collection devices.

c. Eliminate third-party cookies and other data collection devices.

d. Post privacy notices at major entry points to a site and at sites where substantial personal information is collected from the public.

e. Hold web masters accountable for compliance with DoD and Office of Management and Budget policy on a continuing basis.

2. We recommend that the Assistant Secretary of Defense (Command, Control, Communications and Intelligence) revise the DoD Web Site Administration Policy to clearly show that the policy on the use of persistent cookies applies to non-user-identifying information and user-identifying information.

Management Comments. The Deputy Assistant Secretary of Defense (Security and Information Operations), responding for the Assistant Secretary of Defense (Command, Control, Communications and Intelligence), partially agreed with the recommendation. He set an August 31, 2001, date for DoD Components to complete actions to implement the recommendations. The Director, Defense Privacy Office, stated that the recommendation should be revised to include the Defense Privacy Office because it has a role in ensuring that the DoD Components comply with privacy policy.

Audit Response. The Deputy Assistant Secretary comments were responsive to Recommendation 1. We also ask for comments on Recommendation 2. that was added.

Appendix A. Audit Process

Scope and Methodology

Audit Type, Dates and Standards. We performed this economy and efficiency audit from December 2000 through May 2001, in accordance with auditing standards issued by the Comptroller General of the United States, as implemented by the Inspector General, DoD. We judgmentally selected 400 DoD agencies, the Office of the Secretary of Defense, and Service web sites registered in the Government Information Locator Service. We relied on computer-processed data from the Government Information Locator Service 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.

We reviewed and evaluated web sites of the Army, Navy, Air Force, Marine Corps, and other DoD agencies. We compared those sites to OMB and DoD policies on privacy, specifically on collecting, creating, reviewing, and sharing with third parties, personally identifiable information about individuals and their access and viewing habits at Government and nongovernment sites.

We used Microsoft Internet Explorer to assist us in identifying and validating cookies, and used a software program "Bugnosis Beta 5," provided to us by the Privacy Foundation to assist us in identifying web bugs. We conducted discussions with DoD Components and the Services to evaluate whether web site administrators were aware of the DoD and OMB policies on personal information. We attempted to determine what information was being collected, why it was being collected, how it was stored, and whether personal information was sold or provided to any party outside the Government for any purpose. For the most part, where we identified a collection device, we could not determine what was being collected or whether it was sold or given away to any party. Because many of the web masters we contacted were unaware of the collection device, we could not in many cases, determine how it was stored and why it was collected. We did not evaluate the management control program as it related to the overall objectives due to the narrow time frame provided by Congress to issue a report.

Use of Technical Assistance. The Technical Assessment Division, Audit Followup and Technical Support Directorate, Quantitative Methods Division, and the Information Systems Directorate, Office of the Inspector General, provided expertise in identifying web bugs. The Technical Assessment Division reviewed cookies and other means used to obtain personal information. The Quantitative Methods Division assisted in the judgmental selection of our sample. The Information Systems Directorate reviewed source code and other information at each site where we received a numerical rating of 1 or greater and concluded that there were 7 web bugs.

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

General Accounting Office High-Risk Area and Corporate-Level Goals. The General Accounting Office lists information assurance as a high-risk area. Although the Secretary of Defense annually establishes DoD-wide corporate-level goals and performance measures to address the requirements of the Government Performance and Results Act, the Act does not currently provide corporate-level goals for information assurance.

Prior Audit Coverage

General Accounting Office

During the last 5 years, GAO issued two reports on the subject of Internet privacy.

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

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

Appendix B. Revision to DoD Web Site Administration Policy

THE DEPUTY SECRETARY OF DEFENSE
WASHINGTON, D.C. 20301-1000

APR 26

MEMORANDUM FOR SECRETARIES OF THE MILITARY DEPARTMENTS
CHAIRMAN OF THE JOINT CHIEFS OF STAFF
UNDER SECRETARIES OF DEFENSE
DIRECTOR, DEFENSE RESEARCH AND ENGINEERING
ASSISTANT SECRETARIES OF DEFENSE
GENERAL COUNSEL OF THE DEPARTMENT OF DEFENSE
INSPECTOR GENERAL OF THE DEPARTMENT OF DEFENSE
DIRECTOR, OPERATIONAL TEST AND EVALUATION
ASSISTANTS TO THE SECRETARY OF DEFENSE
DIRECTOR, ADMINISTRATION AND MANAGEMENT
DIRECTORS OF THE DEFENSE AGENCIES
DIRECTORS OF THE DOD FIELD ACTIVITIES

SUBJECT: DoD Web Site Administration Policy

In a June 22, 2000 memorandum, the Office of Management and Budget (OMB) reiterated the requirement for privacy policies for web activities and issued a new Federal policy on privacy and data collection on Federal web sites that addresses the use of "cookies." This new policy was subsequently clarified in a September 5, 2000 letter from John Spotila, Administrator, Office of Information and Regulatory Affairs, OMB, to Roger Baker, Chief Information Officer, Department of Commerce, and chair of the Federal CIO Council Privacy Subcommittee.

While DoD policy already addresses the concerns covered by these memoranda, detailed implementation necessitates changes to the "DoD Web Site Administration Policies and Procedures," issued by DEPSECDEF memorandum, "Web Site Administration," December 7, 1998 (http://www.defenselink.mil/admin/dod_web_policy_12071998.pdf).

The required changes are detailed in the attachment and are effective immediately. Note in particular the changes regarding permissible uses of "cookies" and privacy notices required for voluntarily provided user-identifying information.

Questions regarding this policy change should be directed to Ms. Linda Brown, OASD(C3I), (703) 695-2289, Linda.Brown@osd.mil.

Paul Wolfowitz

Attachment
As stated

U06609 /01

DoD Web Site Administration Policies and Procedures
Dated November 25, 1998

- Amend Part II, paragraph 7 to read:

7. PRIVACY AND SECURITY NOTICE

A privacy and security notice must be given to users of each Web site and shall be prominently displayed or announced on at least the first page of all major sections of each Web site. The notice describes how, in general, security is maintained on the site, and what specific information is collected, why it is collected, and how it is used. All information collected must be described in this notice. Providing a statement such as "Please read this privacy and security notice" linked to the actual notice is satisfactory. Organizations shall avoid flashy graphics or other indicators that create a misperception of danger, such as skull-and-crossbones logos or "warning" signs. Agencies subject to DoD Directive 5240.1 (reference (q)) must comply with its provisions. See paragraph 12 below for details and limitations regarding the collection of information, including information voluntarily provided by the user (e.g., e-mail to the webmaster). See Part V for the text of the required privacy and security notice.

- Substitute the following for Part II, paragraph 12:

12. COLLECTION OF INFORMATION

In certain instances,it is necessary and appropriate to collect information from visitors to Web sites. Agencies subject to DoD Directive 5240.1 (reference (q)) must comply with its provisions in addition to those cited below.

12.1. Compliance with the Paperwork Reduction Act. Publicly accessible Web sites shall comply with the requirements of Paperwork Reduction Act of 1995 (PRA), (reference (a)), as described below. The PRA requires that collection of information from the public be approved by OMB under some circumstances.

12.1.1. Requests for identical information from ten or more members of the public, to include DoD contractors, must be approved by OMB. Such requests include surveys using check box, radio button or text form fields.

12.1.2. The PRA applies to electronic forms/information collections on Web sites that collect standardized information from the public. It does not apply to collection of information strictly from current DoD employees or service members in the scope of their employment. Surveys on publicly accessible Web sites will not ordinarily be exempt from the requirement to obtain OMB approval under this exception.

12.1.3. Forms for general solicitations of comments that do not seek responses to standard questions, such as the common opinion-based feedback forms and e-mail links, do not require OMB clearance. See, however, paragraph 12.2 below.

12.1.4. Organizations are responsible for ensuring their publicly accessible Web sites comply with this requirement and follow procedures in DoD 8910.1-M (reference (l)). For more information about the Paperwork Reduction Act of 1995, contact your local Information Management Control Office.

12.2 Collection of User-Identifying Information from DoD Web Sites. The solicitation or collection of personally identifying information, including automated collection or collection through capabilities which allow a user to contact the Web site owner or webmaster, triggers the requirement for either a Privacy Act Statement (PAS) or a privacy advisory (PA).

12.2.1 Use of a Privacy Act Statement.

12.2.1.1 Whenever personally-identifying information (see Part III, Definitions) is solicited from an individual (e.g., eligibility for benefits determinations) and the information is maintained in a Privacy Act system of records (i.e., information about the individual is retrieved by name or other personal identifier), a Privacy Act Statement (PAS), consistent with the requirements of reference (mm), must be posted to the Web page where the information is being solicited or provided through a well-marked hyperlink.

12.2.1.2 If the information collected is being maintained in a Privacy Act system of records for which a notice has not yet been published in the *Federal Register*, such a notice must be published, consistent with the requirements of the Act, prior to any information being collected.

12.2.1.3 If a PAS would be required if the solicitation were made in the paper-based world, it is required in the on-line world, whether the site is publicly accessible or non-publicly accessible.

12.2.2 Use of a Privacy Advisory.

12.2.2.1. If personally-identifying information (see Part III, Definitions) is solicited by a DoD Web site (e.g., collected as part of an email feedback/comments feature on a Web site) and the information is not maintained in a Privacy Act system of records, the solicitation of such information triggers the requirement for a privacy advisory (PA). The PA informs the individual as to why the information is being solicited (e.g., so that the Department can provide the information that has been requested by the individual) and how such information will be used (e.g., it will be destroyed after the information the individual is seeking has been forwarded to him or her).

12.2.2.2. If personally-identifying information (see Part III, Definitions) is solicited by a DoD Web site (e.g., as part of electronic commerce transactions), a PA must be provided regardless of where the information is maintained.

12.2.2.3. The PA must be posted to the Web page where the information is being solicited or provided through a well-marked hyperlink. Providing a statement such as "Privacy Advisory: Please refer to the Privacy and Security Notice that describes why this information is being collected and how it will be used." linked to the applicable portion of the privacy and security notice required by paragraph 7 above is satisfactory.

12.2.3 Automated Collection of User-Identifying Information on Publicly Accessible Web Sites

12.2.3.1 Use of Session Cookies. The use of session cookies (see Part III, Definitions) is permitted for session control and to maintain state, but such cookies shall expire at the end of the logical session. Data from those cookies may not be utilized for other purposes or stored subsequently. The use of session cookies shall be explicitly identified in the site's privacy notice (see Part V, paragraph 4.1).

12.2.3.2 Use of Persistent Cookies. The use of persistent cookies is authorized only if all of the following conditions are met:

(a) there is a compelling need to gather the data on the Web site;
(b) appropriate technical procedures have been established to safeguard the data;
(c) the Secretary of Defense has personally approved use of the cookie prior to implementation of the data collection; and
(d) privacy notices clearly specify, in addition to other required information, that cookies are being used and describe the safeguards for handling the information collected from the cookies.

Requests for approval to use persistent cookies should be submitted at least 30 days prior to operational need date, through the appropriate chain of command, to the Office of the Assistant Secretary of Defense (C3I), for processing prior to submission to the Secretary of Defense for decision. The request shall describe the need and the safeguards to be used to protect the data, provide an explanation of why other technical approaches are inadequate, and include a copy of the privacy notice(s) proposed for use.

12.2.3.3. Other Automated Means of Collecting User-Identifying Information. The use of any other automated means to collect user-identifying information without the express permission of the user requires the same approvals as described in paragraph 12.2.3.2 above.

12.3. Usage Statistics. As a management function, evaluation of site usage data (log files) is a valuable way to evaluate the effectiveness of Web sites. However, collection of data from publicly accessible sites for undisclosed purposes is inappropriate. There are commercially available software packages that will summarize log file data into usable statistics for management purposes, such as the most/least requested documents, type of browser software used to access the Web site, etc. Use of this type of software is appropriate, as long as there is

full disclosure as specified in the privacy and security notice, referenced in paragraph 7 above. Organizations shall establish a destruction disposition schedule for collected data.

- Amend Part III, to add the following two new definitions:

Cookie. A "cookie" is a small piece of information (token) sent by a Web server and stored on a user's system (hard drive) so it can later be read back from that system. Using cookies is a convenient technique for having the browser remember some specific information. Cookies may be categorized as "session" or "persistent" cookies. "Session" cookies are temporary cookies that are used to maintain context or "state" between otherwise stateless Web transactions (e.g., to maintain a "shopping basket" of goods selected during a single logical session at a site) and that must be deleted at the end of the web session in which they are created. "Persistent" cookies remain over time and can be used for a variety of purposes, including to track a user's access over time and across Web sites, or to establish user preferences.

Personally-Identifying Information. Information, including, but not limited to, name, e-mail or postal address, or telephone number, that can be used to identify an individual.

- Amend Part IV, to correct paragraph (l) and add new paragraph (mm):

(l) DoD 8910.1-M, "DoD Procedures for Management of Information Requirements," June 30, 1998, authorized by DoD Directive 8910.1, "Management and Control of Information Requirements," June 11, 1993

(mm) Section 552a of title 5, United States Code, as implemented by DoD 5400.11-R, "Department of Defense Privacy Program, " August 1983.

- Amend Part V, paragraph 4.1, PRIVACY AND SECURITY NOTICE, to add:

The following, when appropriately tailored, may be used as a notice for sites using session cookies.

8. Cookie Disclaimer. (DefenseLINK) does not use persistent cookies, i.e., tokens that pass information back and forth from your machine to the server and remain after you close your browser. (DefenseLINK) does use session cookies, i.e., tokens that remain active only until you close your browser, in order to (make the site easier for you to use). No database of information obtained from these cookies is kept and when you close your browser, the cookie is deleted from your computer. (DefenseLINK) uses cookies in the following ways:

- (Describe use, e.g., "to save you time in filling out forms," "to maintain a relationship between the image and the correct link, the program that displays the banners on the bottom of some of our pages uses a session cookie.")

You can chose not to accept these cookies and still use the site, but (you may need to enter the same information repeatedly and clicking on the banners will not take you to the correct page). The help information in your browser software should provide you with instruction on how to disable cookies.

- Amend Part V, paragraph 4.1, by deleting the word "other" from the last sentence, so it then reads:

Requests for other types of documents use similar information. No user-identifying information is collected.

Appendix C. 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)
Director, Administration and Management

Department of the Army

Auditor General, Department of the Army

Department of the Navy

Naval Inspector General

Department of the Air Force

Assistant Secretary of the Air Force (Financial Management and Comptroller)

Other Defense Organizations

Director, Defense Contract Audit Agency
Defense, Finance and Accounting Service
Director, Defense Logistics Agency
Director, Defense Information Systems Agency
Washington Headquarters Service
Director, Defense Privacy Office

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 Subcommittee on Treasury and General Government, 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 Subcommittee on Treasury, Postal Service and General Government, 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

Office of the Assistant Secretary of Defense (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

May 15, 2001

MEMORANDUM FOR DIRECTOR, ACQUISITION MANAGEMENT DIRECTORATE, OFFICE OF THE INSPECTOR GENERAL

SUBJECT: Draft Audit Report on DoD Internet Access, Practices, and Policies (Project No. D2001AB-0065), May 3, 2001

This office appreciates the opportunity to comment on the subject report.

The use of persistent cookies on some DoD sites is not disputed. However, this does not necessarily support a conclusion that, in general, the cookies were being used to collect user-identifying information. This fact is acknowledged in Appendix A of the report, where the OIG states: "For the most part, where we identified a collection device, we could not determine what was being collected...."

The DoD has been proactive in addressing issues of personal privacy and the web, a fact recognized by both the Office of Management and Budget (OMB) and private interest groups. Since 1997, DoD web policy has specifically addressed, and prohibited, automated collection of user-identifying information. However, the policy also explicitly allowed use of cookies or other methods to collect or store non-user-identifying information. This approval was recognition that there are technically valid reasons to utilize cookies that do not collect user-identifying information. Nonetheless, the DoD policy was updated following issuance of the OMB policy and now prohibits all uses of persistent cookies without the specified waiver. The GAO, in their September 2000 report "INTERNET PRIVACY: Agencies' Efforts to Implement OMB's Privacy Policy," found none of the DoD sites in their random sample missing posted privacy notices and concluded that the estimated number of major entry points without privacy notices does not exceed 5 percent of all the Department's major entry points.

This office partially concurs with the recommendation. The OIG findings indicate the Department's webmasters are insufficiently aware of the Web Site Administration policy. The DoD policy assigns the Heads of Components responsibility for "ensur[ing] compliance with [DoD] policy for those functions, missions, agencies, and activities in their purview"; this responsibility is generally delegated to the sponsoring organization's

commander, not to the webmaster. Thus, this office will require the DoD Components to report not later than August 31, 2001, on what they have done to:

- disseminate the Web Site Administration policy and ensure that all subordinate organizations sponsoring web sites are aware of the policy;
- provide their webmasters instructions on how to identify data collection devices (e.g., persistent cookies; web bugs);
- eliminate or ensure use of third-party cookies complies with all of the DoD and OMB requirements for use of cookies, including waiver approval and appropriate notices and protection of the data collected; and
- hold the commanders of the organizations sponsoring web sites accountable for compliance with issued policies on a continuing basis.

Additional comments are included in the attachment.

Questions may be directed to the OSD action officer, Ms. Linda Brown, at (703) 695-2289.

J. William Leonard
Deputy Assistant Secretary of Defense
(Security and Information Operations)

Attachment
As stated

Final Report Reference

Additional Comments
on
Draft Audit Report on DoD Internet Access, Practices, and Policies
(Project No. D2001AB-0065)

1. Page 2, DoD Privacy Guidance. The second sentence of this paragraph should acknowledge that the 1997 policy also established prohibitions on collection of user-identifying information. The 1997 policy explicitly stated: "it is prohibited to use methods which collect user-identifying information"; at the same time it allowed use of cookies or other methods to collect or store non-user-identifying information. Recommend the second sentence be modified to read: "…DoD established policies on collection of user-identifying information and use of cookies in …" — Revised

2. Page 3, DoD Privacy Guidance. This paragraph does not acknowledge the fact that, in large part, the July 13, 2000, DoD Memorandum, reiterated provisions of the DoD Web Site Administration policy issued in December 1998. While the provisions relating to specifically to the use of persistent cookies were new, the requirements for privacy statements and the prohibitions on collecting user-identifying information were restatements of the 1998 policy. — Revised

3. Page 5, Web Masters Visited…. The information posting process specified by DoD policy, assigns editorial control of web site content to the content provider/originating office (i.e., the entity that created or sponsored development of the information).

Defense Privacy Office Comments

Final Report Reference

DEPARTMENT OF DEFENSE
DEFENSE PRIVACY OFFICE
1941 JEFFERSON DAVIS HIGHWAY, SUITE 920
ARLINGTON, VA 22202-4502

May 11, 2001

MEMORANDUM FOR OFFICE OF THE ASSISTANT INSPECTOR GENERAL FOR AUDITING,
ATTN: MR. TOM BARTOSZEK, 400 ARMY NAVY DRIVE, ROOM 626,
ARLINGTON, VA 22202

SUBJECT: DODIG Draft Report/DoD Internet Access, Practices, and Policies

This responds to your request for my views on the draft report on DoD Internet Access, Practices, and Polices.

My comments are as follows

- Page ii, Results

Comment: It is my firm belief that the Congressional tasking was principally designed to ascertain whether (1) Federal agencies were knowingly utilizing web technology to collect information on visitors to their public web sites and (2) such information was being utilized in a prohibited manner. I do not believe the report adequately addresses these implied taskings. Specifically, the audit has shown that many web masters, whose sites were collecting such information, were unaware of the on-going collection. Should not such a fact be made clear in the results? I believe it should be because it generally reflects that the proscribed activity results from acts of nonfeasance rather than malfeasance on the part of the web masters. Also, the report does not reflect that web masters, who knowingly were using web technology to collect information, were using this information to track the activities of web visitors or to build profiles on such visitors. Again, should not such a fact be made clear in the results? I believe it should be because it generally reflects that Departmental web masters are not utilizing the data in a manner that violates the privacy of the visitor.

Recommendation: The antepenultimate sentence be deleted and the following substituted:

"Where information was being collected used web technology, most web masters were unaware that the information was being collected. Also, there was no evidence that where the information was knowingly being collected that it was being used for an unlawful purpose by a DoD web master. However, where the information was being collected by commercial companies, DoD has inadequate assurance that such information was not sold or given away."

Page 2, DoD Privacy Guidance

Revised

Comment: I strongly believe that the Report should reflect that the DoD has issued a formal change to its web policies regarding the use of persistent cookies and the voluntary collection of information. Though recognizing that the policy change was issued during the report-

Final Report Reference

writing phase of the IG Audit, the fact remains that it was published and that the change is an integral part of DoD's overall web privacy policy. Therefore, it should be incorporated into your final draft.

Recommendation A third para should be added to read as follows: — Add page 2

"After we had completed the fact-finding phase of our audit, the DoD amended its 1998 web policy which, among other changes, prohibited the use of persistent cookies, unless specified conditions were met and use was personally approved by the Secretary of Defense, and specified what kind of privacy notice was required to be furnished when voluntary information is collected from a visitor to the site."

- Page 3, DoD Internet Access

Comment: The penultimate sentence states that DoD collected personal information on individuals, but the report makes clear that, in some cases, the webmasters responsible for the site were not aware that such information was being collected. Also see, first bullet at page 1. — Revised

Recommendation: The sentence be revised as follows:

"As a result, DoD, knowingly or unknowingly, collected personal...Secretary of Defense."

Page 3, Section 552a of the Privacy Act of 1974

Comment: The paragraph does not accurately capture the requirements of the Act.

Recommendation: The paragraph be rewritten as follows:

"The Privacy Act of 1974 (5 United States Code 552a). Under the Privacy Act, individuals have the right to access agency records containing information about themselves and the right to request amendment of records that are inaccurate, irrelevant, untimely, or incomplete. The Privacy Act only applies to Federal records that are retrieved by name or other personal identifier. The Act requires that agencies inform an individual of the authority for collecting information, whether disclosure by the individual is voluntary or mandatory, the principal purposes for which the information will be used, the routine uses which may be made of the information, and the consequences of not providing the information. In addition, agencies must establish appropriate administrative, technical, and physical safeguards to ensure the security and confidentiality of the records." — Revised

- Page 3, DoD Privacy Guidance

Comment: The fourth sentence is misleading. The sentence states that persistent cookies are prohibited unless visitors are advised in the privacy statement of what is being collected and why and how it would be used. It appears that the report is attempting to couple two different sections of the July 13, 2000 DoD memo. This attempt does not reflect what the DoD memo is saying. The memo makes

Final Report Reference

clear that cookies are prohibited unless specified conditions are satisfied and the use is personally approved by SECDEF. The memo further states that current DoD policy [existing as of the date of the memo] permits use of cookies or other web technology to collect non-user identifying [emphasis added] information, but only if users are advised of what information is collected, why it is being done, and how it is to be used.

Revised

Recommendation The sentence be revised as follows:

"The policy prohibits using web technology to identify and track the activities of web users and advises that current DoD policy, which permits the use of cookies or other technology to collect non-user identifying information when the user is made aware of what information is being collected, why it is being collected, and how it is being used, will be clarified to make clear that persistent cookies are only authorized under specified conditions as set out by OMB."

Page 4, Sample of DoD Internet Web Sites

Comment: The penultimate sentence makes the claim that the GILS helps facilitate interagency data sharing. It is unclear how this is so. As the DoD office responsible for overseeing computer matching with other Federal agencies, this office has never, and to my knowledge no other Federal agency has, resorted to GILS to help facilitate data sharing.

Revised

Recommendation: Delete the sentence unless it can be demonstrated how GILS provides such a service and is, in fact, utilized by the Department for such purposes.

- Page 7, Privacy Statements at Web Sites and Voluntary collection Locations, first para

Comment: It is assumed that each of the 100 identified web sites constitutes either a principal web site, a known major entry point, or a site where substantial personal information is collected. If not, the site would not be in violation of the DoD policy. I only raise this issue as it is common for many users to have by-passed the major entry point. When they do so, they will see a page that does not link to the privacy and security notice. This does not mean the site is violating OMB/DoD policy on the posting of a privacy notice. If one drills up to the major entry point, the privacy notice is posted.

- Page 7, Privacy Statements at Web Sites and Voluntary collection Locations, second para

Comment: The report identifies 80 sites where privacy notices are not posted, but information, such as names, e-mail addresses, office addresses and telephone numbers, is being voluntarily collected I assume the sites are the "feed-back" web pages where a user can comment or request additional information. If this assumption is correct, it is pointed out that, and notwithstanding the 1999 OMB policy, current DoD web policy, until recently, was silent on this issue. However, as discussed above, a change to the policy, which would make clear that such a privacy notice is required when

3

Final Report Reference

voluntarily collecting information from a user, was published on April 26, 2001. I only raise this issue as the Components are not entirely at fault for failing to comply.

Recommendation: A new sentence should be added at the end of the second para to read as follows:

"It is noted that current DoD web policy does not explicitly address the need for a privacy notice when information is being solicited from the visitor. However, this oversight has been remedied as the Deputy Secretary of Defense, on April 26, 2001, published a change to DoD web policy which makes clear that such a notice is required."

- Page 9, Conclusion

Comment: The second sentence of the first para is misleading for the reasons discussed above (see last bullet at page 2).

Recommendation: The sentence be revised as follows and the third sentence be deleted:

"It prohibits using web technology to collect identifying information, building profiles on individuals, and using persistent cookies, except under specified conditions and when such use has been personally approved by the Secretary of Defense." — Revised

Page 10, Recommendations

Comment: I believe that the Defense Privacy Office also has a role in ensuring that Departmental entities are complying with OMB web privacy policies.

Recommendation: The first sentence be revised as follows:

"We recommend that the Assistant Secretary of Defense (Command Control Communications and Intelligence), in consultation with the Defense Privacy Office, require the ..."

- Page 13, Appendix B. Report Distribution — Added

Comment: Because the Director, Administration and Management, serves as the senior privacy official for the Department of Defense, he should be furnished a copy of the Report.

Recommendation: Under the heading "Office of the Secretary of Defense," add the following: — Added

"Director, Administration and Management"

Should you have any questions regarding the above comments, please do not hesitate to contact me at (703) 607-2943.

Vahan Moushegian, Jr.
Director

4

Audit Team Members

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

Mary Ugone
Raymond A. Spencer
Thomas S. Bartoszek
Lisa E. Novis
Thomas J. Hilliard
Thelma E. Jackson
Rudolf Noordhuizen
Gary B. Dutton
Chanda D. Lee
Sarah L. Brownwell
Trisha L. Staley
Stacey L. Kreinbrook
Mandi L. Markwart
Brian K. Jacques
Jenshel D. Marshall