

DEPARTMENT OF THE AIR FORCE
WASHINGTON DC

Chief Information Officer

19 September 2001

MEMORANDUM FOR DISTRIBUTION C

ALMAJCOM-FOA-DRU/CV

FROM: CIO-BIM
1155 Air Force Pentagon
Washington DC 20330-1155

SUBJECT: Web Site Administration Policy

DoD has revised their web site administration policy as a result of OMB privacy guidance. The attachment reflects changes to OSD's 25 Nov 98, "Web Site Administration Policies and Procedures." Note in particular, the changes on permissible uses of "cookies" and privacy notices required for voluntarily-provided, user-identifying information. The entire policy is available at

http://www.defenselink.mil/webmasters/policy/dod_web_policy_12071998_includes_amendments_from_04262001.html.

These changes are effective immediately and will be in the next revision to AFI 33-129. Please provide this information to all Privacy Act managers, network control centers, system administrators, Web site Administrators, and Web page maintainers. We are researching tools that may assist in identifying persistent cookies and web bugs, and will keep you informed of our progress.

CIO-BIM point of contact is Mrs. Anne Rollins, CIO-BIM/P, (703) 601-4043.

Attachment:

Amended Web Policy

cc: CIO EXCOM

Amendment to DoD Web Site Administration Policies and Procedures

Dated November 25, 1998

Found at (http://www.defenselink.mil/webmasters/policy/dod_web_policy_12071998_includes_amendments_from_04262001.html)

- 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.

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 (G2D), for processing prior to submission to the Secretary of Defense for decision. The request shall describe the need and

Office of the Assistant Secretary of Defense (CS1), 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.