



U.S. Agency for  
INTERNATIONAL  
DEVELOPMENT

*Washington, D.C.*

May 14, 2001

**MEMORANDUM FOR A-CIO, Peter Benedict**

**FROM:** IG/A/ITSA, Melinda G. Dempsey

**SUBJECT:** Audit of USAID's Compliance with Internet Privacy Policies  
(Report No. A-000-01-001-P)

This memorandum is our report on the subject audit. Thank you for the level of importance you attach to individual privacy issues. Your comments on the draft report are included in Appendix II.

This report contains two recommendations for your action. Based on your comments, management decisions have been reached on these recommendations. The Office of Management Planning and Innovation (M/MPI/MIC) will make a determination of final action for these recommendations when planned corrective actions are completed.

I appreciate the cooperation and courtesy extended to my staff during the audit.

---

---

**Table of  
Contents**

Summary of Results	3
Background	3
Audit Objectives	4
Audit Findings	5
Does USAID collect or enter into agreements with third parties to obtain personally identifying information about individuals who access the Agency’s website?	5
Does USAID post privacy notices and restrict the use of Internet cookies in accordance with Office of Management and Budget Memoranda M-99-18 and M-00-13?	5
Management Comments and Our Evaluation	9
Appendix I - Scope and Methodology	10
Appendix II - Management Comments	12

---

## **Summary of Results**

This report discusses how the agency collects personally identifying information and describes our assessment of USAID's compliance with the Office of Management and Budget's requirements to post privacy policies on websites and to limit use of Internet cookies<sup>1</sup>, except under certain conditions. The specific objectives of the audit are to determine whether: (1) USAID collects through its own efforts or obtains from third parties personally identifying information about visitors to its public website [page 5] and (2) USAID complies with federal guidance related to protecting Internet users' privacy when visiting federal websites [page 5].

Our audit work documented that USAID does collect personally identifying information from website visitors [page 5]. In addition, based on management representations, USAID has not entered into any agreements with third parties to obtain personally identifying information related to website users' viewing habits [page 5].

Our work also indicated that USAID does comply with federal regulations that require agencies to post privacy notices on their websites [page 5]. However, USAID does not fully comply with requirements that govern the use of Internet cookies [page 6], nor does it adequately safeguard personal information collected [page 8].

The acting Chief Information Officer (CIO) has agreed with the report and is planning to implement both recommendations [page 9].

---

## **Background**

As the Internet pervades the personal and work lives of Americans, greater focus is placed on protecting personal privacy. The Congress has long recognized the importance of privacy in American society. The Privacy Act of 1974 requires that federal agencies protect an individual's right to privacy when they collect personal information. This concern was continued by enactment of the Treasury and General Appropriations Act of 2001 which states that:

Not later than 60 days after the date of enactment of this Act, the Inspector General of each department or agency shall submit to Congress a report that discloses any activity of the applicable department or agency relating to--

---

<sup>1</sup> A cookie is a text data file that is sent from a web server to a web browser when the browser accesses a web page. Cookies allow the web server to recognize a user who returns to a particular site. Cookies can be used to track on-line purchases or to maintain and serve customized web pages.

- 
- (1) the collection or review of singular data, or the creation of aggregate lists that include personally identifiable information, about individuals who access any Internet site of the department or agency; and
  - (2) entering into agreements with third parties, including other government agencies, to collect, review, or obtain aggregate lists or singular data containing personally identifiable information relating to any individual's access or viewing habits for governmental and nongovernmental Internet sites.

The Office of Management and Budget (OMB) has provided specific guidance to agencies to help protect privacy. This guidance is primarily in the form of two memoranda to agencies. The first, Memorandum M-99-18, provides criteria for posting privacy notices on federal websites. The second, Memorandum M-00-13, addresses Internet cookies, text or data files stored on a visitor's computer. The memorandum provides that cookies may not be created by a federal website unless certain requirements are met.

At USAID several offices have responsibilities over USAID's website. The Chief Information Officer (CIO) is responsible for directing, managing, and providing policy guidance and oversight with respect to all USAID information resource management activities. The Bureau for Legislative and Public Affairs (LPA) is responsible for the review of USAID produced or funded materials available to the public on the Internet. The Bureau for Management, Office of Information Resources Management (M/IRM) is responsible for operating USAID's external website.

---

## **Audit Objectives**

The Congress, as part of Treasury and General Appropriations Act of 2001, mandated the first objective of this audit. The second objective was to test agency compliance with existing federal guidance. As a result, the objectives of this audit were to answer the following questions:

**Does USAID collect or enter into agreements with third parties to obtain personally identifying information about individuals who access the Agency's website?**

**Does USAID post privacy notices and restrict the use of Internet cookies in accordance with Office of Management and Budget Memoranda M-99-18 and M-00-13?**

A detailed discussion of our scope and methodology is presented in Appendix I.

---

---

## **Audit Findings**

### **Does USAID collect or enter into agreements with third parties to obtain personally identifying information about individuals who access the Agency's website?**

USAID collects limited personal information about visitors and is unaware of any third party agreements to collect personal information. Information such as a visitor's computer Internet address and date and time of access are collected in website log files. Visitor names, e-mail addresses, and any other information that the visitor provides is also solicited and collected from visitors who have comments or suggestions. USAID discloses the types of information collected and how it will be used in privacy notices posted on the website. Privacy notices are discussed in more detail under the second audit objective below.

According to USAID management, USAID does not have any agreements with third parties to collect, review, or obtain aggregate lists or singular data containing personally identifiable information relating to any individual's access or viewing habits for its Internet sites. We consider the likelihood that USAID has agreements of this nature to be low, but the cost of extensive verification would be high because of the many contracts USAID has with partners and vendors. Accordingly, we limited our verification efforts to discussions with management responsible for the USAID privacy program and with management responsible for website content.

### **Does USAID post privacy notices and restrict the use of Internet cookies in accordance with Office of Management and Budget Memoranda M-99-18 and M-00-13?**

USAID includes a privacy notice on its websites that complies with OMB Memorandum M-99-18. However, USAID does not fully comply with OMB Memorandum M-00-13 requirements on using cookies on federal websites. These two issues are detailed in the following sections of this report.

### **USAID Does Comply with OMB's Requirements on Privacy Notices**

OMB Memorandum M-99-18 requires agencies to post privacy policies in accordance with the following.

- Privacy policies must be posted on agency websites, at major entry points to sites, and on any page where substantial personal information is collected from the public;

- 
- Policies must clearly and concisely inform visitors to the site what information the agency collects about individuals, why the information is collected, and how the information is used; and
  - Policies must be clearly labeled and easily accessed.

Specifically, links to USAID's privacy notice are prominently posted on the main webpage and on other major points of entry to USAID's website. The notice informs visitors to the site that USAID collects domain name, the date and time the site was accessed, and the Internet address of the website from which the visitor was linked directly to USAID's site. The policy outlines that the Agency collects statistics on which webpages visitor's view at the website. It also clearly indicates that information is collected for site management and, in the case of suspected unauthorized activity, for law enforcement and possible criminal prosecution. Visitors are also informed that personally identifying information is collected when sending an e-mail message. This information is then used to respond to comments or suggestions. Finally, the privacy notices policies are clearly labeled and easily accessed.

### **USAID Does Not Fully Comply with OMB's Requirements on Cookies**

OMB Memorandum M-00-13 states that "the presumption should be that 'cookies' will not be used" on federal websites. Nevertheless, if cookies are used, the following criteria must be met.

- The site must give clear and conspicuous notice that cookies are used;
- A compelling need to gather data on the site must exist;
- Appropriate and publicly disclosed privacy safeguards must be in place to protect any information derived from cookies; and
- The agency head must give personal approval for the use of the cookie.

USAID was aware of the requirements of M-00-13 and was attempting to comply with the guidance. However, when we searched a copy of USAID's website, we found two webpages that caused cookies to be created. Both cookies did not meet all the conditions for use under the OMB's memorandum.

---

In the first instance, USAID developed an application, which used cookies to collect and store information that can be associated with a particular person. USAID did not intend for the application that created the cookie to be available to the public. However, in order to demonstrate the functionality of the application to a remote party, USAID placed the application on the public website but did not provide any links or indication to the public that it existed. While on the website, the application could only have been accessed by visitors who knew its webpage address. Notwithstanding that the application was not publicized nor readily available to the public, it was accessible on the website and the cookie it created did not comply with any of the requirements of OMB M-00-13.

In the second instance, a USAID application, which allowed visitors to search for past contract awards information, created a cookie on a site visitor's computer. USAID disclosed the use of this cookie in the web page's privacy notice but did not attempt to ensure that the other conditions of OMB M-00-13 were met before using the cookie. At the time, management did not believe that this particular cookie was subject to the OMB memorandum. In practice, a cookie can be classified as either a "session" or as a "persistent" cookie. Session cookies are not saved on a visitor's computer after disconnecting from the Internet. Persistent cookies remain on a visitor's computer indefinitely or until they are deleted. After issuing M-00-13, OMB clarified its position on using cookies to state that the four conditions cited above applied only to using persistent cookies<sup>2</sup>. USAID mistakenly believed that the cookie created by this application was a session cookie and therefore not subject to M-00-13.

Subsequent to our audit, USAID management has removed the sources of both cookies from the website. The previously cited conditions resulted because procedures and monitoring activities are not in place to ensure complete compliance with the policy. By USAID not complying with the policy, USAID's visitors to the website may not have been aware that information was collected about them, how this information was being used, and how this information was being safeguarded.

**Recommendation No. 1: We recommend that the Chief Information Officer require USAID's, Office of Information Resources Management to periodically search USAID's external website for cookies that do not comply with OMB M-00-13.**

---

<sup>2</sup> See September 5, 2000, letter from John T. Spotilla, Administrator, Office of Information and Regulatory Affairs, Office of Management and Budget to Roger Baker, Chief Information Officer, U.S. Department of Commerce.

---

## **USAID Does Not Adequately Safeguard Personal Information**

OMB Memorandum M-00-13's third requirement, that appropriate privacy safeguards must be in place to protect any information derived from cookies, can be extended to information solicited from visitors. Personal information collected on USAID websites is protected by operating system security on the web server. However, access to this server is not restricted by the agency's firewall, a combination of hardware and software specifically designed to provide a greater level of security to computer networks. Firewalls are desirable to protect sensitive data and networks from intrusion and unauthorized use.

USAID solicits visitor feedback on the website via forms. Forms are web pages that include fields for the user to voluntarily provide information to the web server. The form collects the visitor's name and address and any other personally identifiable information that is typed into the form by the site visitor. This information is logged in a file and is used to respond to visitor inquiries. Presently, USAID does not have a policy, together with procedures and monitoring activities, to ensure that personally identifying information collected by web servers or applications is adequately safeguarded.

**Recommendation No. 2: We recommend that the Chief Information Officer require that security policies, procedures, and monitoring activities are formulated to ensure that personally identifying information collected by web servers or applications is adequately safeguarded.**

---

**Management  
Comments and  
Our Evaluation**

USAID removed the cookies that did not comply with OMB-00-13 and removed personally identifying information from the external web servers. The acting Chief Information Officer has agreed with the report and is planning to implement both recommendations. Consequently, management decisions have been reached on Recommendation Nos. 1 and 2.

Management's complete response is included in this report in Appendix II.

**Scope and  
Methodology****Scope**

The Office of the Inspector General in Washington conducted an audit, in accordance with generally accepted government auditing standards, to determine if USAID was collecting, reviewing, or creating aggregate lists that include personally identifying information about individuals who access the Agency's website. The audit encompassed all files and applications that comprised USAID's external website located at "www.usaid.gov" as of January 20, 2001. Because Internet cookies can be used to collect personally identifying information, the audit also determined whether the cookies being used on the website were used in accordance with OMB Memorandum M-00-13. The audit reviewed privacy notices on the website for compliance with OMB Memorandum M-99-18. The audit was conducted from January 19, 2001, through March 28, 2001.

**Methodology**

To answer the question raised in the first audit objective, we held discussions with the following USAID bureaus: Bureau for Legislative and Public Affairs (LPA); Bureau for Management, Office of Information Resources Management (M/IRM); and Bureau for Management, Office of Assistant Administrator (M/AA). The Deputy Assistant Administrator serves as the Chief Information Officer.

In considering the likelihood that USAID would enter into an agreement with a third party to obtain personally identifying information, we noted targeting advertising, identification of personal assets, and identification of other information to support an entitlement or a claim to be factors that could motivate an agency to collect personally identifying information. We consider the likelihood that USAID has agreements of this nature to be low, but the cost of extensive verification would be high because of the many contracts USAID has with partners and vendors. Accordingly, we limited our verification efforts to discussions with management responsible for the USAID privacy program and with management responsible for website content.

We obtained a copy of all the USAID web files from the web server and from the application server. These files were searched using the "Find File" functionality included with Windows 95. We searched for syntax that would have been used to set cookies using the following programming languages: Cold Fusion, Java, JavaScript, PERL, Active Server Pages, and VBScript.

---

This search covered all files that were on the web server as of January 20, 2001. We set our materiality threshold for the audit as any occurrence of a non-compliant cookie.

USAID management gave us a copy of the Internet files on compact disc as of January 20, 2001. Due to the number and size of the data and due to the fact that we received the disc after January 20, 2001, we relied on management's representation that the discs contain a complete set of the actual files that were available to the public. To provide assurance that we received all files, we judgmentally selected 30 links off the main webpage. Without exception, the links were found in the files provided on the discs.

We reviewed security logs and web server logs to note whether personally identifying information was being collected in the logs. Discussions were held with M/IRM on its policies and procedures for operating websites and using information obtained from users of the sites.

To answer the question raised by the second objective we reviewed any cookies that we found on the website for compliance with OMB Memorandum M-00-13, and we reviewed the website policy notices for compliance with OMB Memorandum M-99-18.

## Management Comments



U.S. AGENCY FOR  
INTERNATIONAL  
DEVELOPMENT

May 11, 2001

TO:           OIG/A/ITSA, Melinda Dempsey  
THROUGH:    A-AA/M, Richard C. Nygard  
FROM:        A-CIO, Peter Benedict  
SUBJECT:     Management Comments on Draft "Audit of USAID's Compliance  
with Internet Privacy Policies"

USAID management takes the issue of protecting individual privacy seriously, and has taken prompt action to increase the already substantial compliance with the OMB guidance on cookies and protection of personally identifying information. Before this audit started, the CIO was in the process of establishing an intensified program of privacy protection. Efforts to protect individual privacy will continue.

**Regarding Recommendation No. 1:** "We recommend that the Chief Information Officer require USAID's, Office of Information Resources Management to periodically search USAID's external website for cookies that do not comply with OMB M-00-13."

We acknowledge that the OIG found two instances of persistent cookies on USAID managed web sites, which were promptly removed, once found. Even though this number was low, we consider that any level of non-compliance on this issue requires action.

The CIO agrees to task appropriate staff to periodically search USAID's identified<sup>1</sup> external websites for cookies that do not comply with OMB M-00-13. We plan

<sup>1</sup>USAID funds a wide range of web-site operated by contractors. Many are funded by USAID missions overseas. At present we do not have a complete inventory of these sites. Within the limit of available funds the CIO will work with partners in USAID to identify these sites so that the necessary search for cookies can be conducted.

---

to close the recommendation when the process for this search is established and in operation.

**Regarding Recommendation No. 2:** "We recommend that the Chief Information Officer require that security policies, procedures, and monitoring activities are formulated to ensure that personally identifying information collected by web servers or applications is adequately safeguarded".

We agree that personally sensitive information was stored on a server that was effectively outside USAID's firewall protections, and that this was not approved as appropriate.

To ensure the immediate protection of personally identifying information while Recommendation 2 is implemented, all such personally identifying information has been removed from the external web server where its security was in question.

The CIO agrees to require the development of security policies, procedures, and monitoring activities to ensure that personally identifying information collected from the public is adequately safeguarded. When these are approved and in operation, we plan to close this recommendation.