UNCLASSIFIED

MEMORANDUM REPORT 01-IT-M-017
DEPARTMENTWIDE WEB SITE MANAGEMENT NEEDS TO BE STRENGTHENED
March 2001

In response to requirements of Section 646 of the Treasury and General Government Appropriations Act, 2001, the Office of Inspector General conducted a review of Internet privacy management at the Department of State. This report focuses on the Department's practices regarding the collection of personally identifiable information through the use of "cookies"[1] and other means on its public web sites.

Specific objectives of our review were to (1) identify the Department's policies and procedures for managing its Internet web sites in accordance with Federal guidance, (2) determine whether the Department's web sites use or have entered into third-party agreements concerning the use of cookies, and (3) determine whether all of the Department's major web entry points have privacy statements posted that adequately reflect what, if any, personal information is collected on the web sites and how that information is used. In addition, during the course of our review, we examined the Department's structure for managing web sites and ensuring Internet privacy organizationwide. We have included a discussion of these issues and related recommendations in this report.

RESULTS IN BRIEF

The Department of State has become increasingly reliant on the World Wide Web as a means to inform the public about its activities and services, both here and abroad. Toward that end, the Department is instituting policies to ensure that its web sites are managed in accordance with Federal privacy guidelines prescribed by the Office of Management and Budget (OMB).

The Department's policies restrict the use of persistent cookies on its public web sites without the Secretary's approval. Cookies are a typical means of collecting personal data on Internet sites, often without the site visitors' awareness. Despite the restriction, we found that 9 of the 206 web sites that we identified in the Department are using persistent cookies without proper authorization. Further, 116 of 206--well over half of the Department's sites that we reviewed--had no privacy statements and therefore no means of advising users of any information collected on the sites. We found no evidence that the cookies were used to collect personally identifiable information.

[1] A cookie is a small text file placed on a site visitor's computer hard drive by a web server. A cookie allows a server to recognize returning users, track online purchases, or maintain and serve customized web pages. A cookie also facilitates the collection of personal information, such as extensive lists of previously visited sites, e-mail addresses, or other information to identify or build profiles on individual site visitors.

These problems resulted in part from the Department's highly decentralized approach to web site management, in which numerous organizations share responsibility for guiding or controlling various aspects of Internet management. The Department recognizes that it needs to strengthen web site management across the organization and, as a first step, has established a permanent, senior-level Internet Steering Committee. We recommend that the Department go even further, and establish an Internet Program Office within the Office of the Under Secretary for Public Diplomacy and Public Affairs to support the Internet Steering Committee in overseeing and coordinating web sites on an agencywide basis.

BACKGROUND

Rapid innovations in technology in recent years offer increasing opportunities for the U.S. Government to improve the quality of information and service that it provides to its citizens. The World Wide Web, also known as the Internet, has emerged as a powerful tool for communicating large amounts of information on Federal activities, policies, and programs. At the same time, however, the Internet has made it possible for web sites to track and collect personally identifiable data[2] from site visitors, making online privacy one of the key and most contentious issues in this information management age.

Internet cookies are a principal means by which web sites can collect personal information from site visitors, often without the visitors' knowledge or consent. There are two types of cookies—"session cookies" and "persistent cookies." Session cookies are short-lived, used only during a single browsing session, expire when the user quits the browser, and consequently do not raise privacy concerns. Persistent cookies track information over time or across web sites. They remain stored on visitors' computers until a specified expiration date and can be used to collect information, such as a visitor's areas of interests and individual browsing habits. Persistent cookies may raise the public's apprehension about what information is collected and how it could be used.

The full potential of the Internet to help improve Federal service cannot be realized until U.S. citizens are confident that their online privacy will be safeguarded. Recognizing this, and building on principles established by the Privacy Act of 1974 (5 USC 552a) and related legislation, the U.S. Government has recently taken steps to help ensure the privacy of visitors to Federal web sites. Specifically, over the past 2 years, OMB issued guidance that establishes the U.S. Government policy for the use of cookies on department and agency public web sites.[3] Taken together, the OMB guidance directs that Federal web sites, and contractors operating web sites on behalf of Federal

[2] Personally identifiable data includes an individual's name, e-mail address, postal address, telephone number, Social Security number, or credit card number.

[3] The OMB guidance includes (1) Memorandum M-99-18, *Privacy Policies on Federal Web Sites*, June 2, 1999, (2) Memorandum 00-13*, Privacy Policies and Data Collection on Federal Web Sites*, June 22, 2000, and (3) a letter from the Administrator, OMB Office of Information and Regulatory Affairs, to the Chief Information Office, Department of Commerce, September 5, 2000, clarifying the previously issued guidance.

agencies, should not use persistent cookies on the web sites unless they provide clear and conspicuous notice of those activities and meet the following conditions: (1) a compelling need to gather the data on the site, (2) appropriate and publicly disclosed privacy safeguards for handling of information derived from cookies, and (3) personal approval by the head of the agency. The OMB guidance further exempts Federal use of session cookies from these requirements.

PURPOSE, SCOPE, AND METHODOLOGY

Section 646 of the Treasury and General Government Appropriations Act, 2001, directs all Inspectors General to report on their respective agencies' practices to collect any personally identifiable information from their public Internet sites. Such information could be collected either on an agency's web sites or through third-party agreements. In response to the Act, the Office of Inspector General conducted a review with the specific objectives of (1) identifying the Department's policies and procedures for managing its Internet web sites in accordance with Federal guidance, (2) determining whether the Department's web sites use or have entered into third-party agreements concerning the use of cookies, and (3) determining whether all of the Department's major web entry points have privacy statements posted that adequately reflect what, if any, personal information is collected on the web sites and how that information is used.

To fulfill our review objectives, we researched guidance used at the Department of State to govern Internet privacy in accordance with Federal laws and regulations. We met with officials from organizations across the Department to learn how they manage their public Internet sites and whether they collect any personal information on the Internet via cookies, third-party agreements, or other electronic means. We also tested 22 headquarters and 184 overseas Internet sites that we identified within the Department to determine if cookies are used and whether privacy statements are posted to advise of such practices.[4] Where necessary, we followed up with responsible officials to obtain explanations of their web management practices and plans for corrective actions. Throughout our review, we also studied the Department's structure for coordinating management of web sites organizationwide.

Appendix A provides details on our methodology for testing the Department's Internet sites. As a part of this approach, we did not examine every page on a web site, but rather spent a limited time navigating through each site to look for cookie indicators. We also relied on discussions with web management officials to learn about third-party agreements or other practices to collect information on public web sites. To validate our treatment in the report of Internet management practices that the officials described, we obtained comments on a draft of the report from organizations that participated in our review. We have incorporated their comments and suggested changes where appropriate.

We also obtained written comments on a draft of this report from both the Office of the Under Secretary for Management and the Office of the Under Secretary for Public

[4] We did not include issues related to management of the Department's internal Intranet sites in our review.

Diplomacy and Public Affairs. We have incorporated their comments and suggested changes where appropriate and have included a copy of the comments at Appendix B.

We conducted our review from January to March 2001 at the Department of State in Washington, DC. Appendix C provides a list of the Department bureaus and offices that participated in our review. We performed our work in accordance with generally accepted government auditing standards. Major contributors to this report were Frank Deffer, Sondra McCauley, and John Shiffer. Comments or questions about the report can be directed to Mr. Deffer at defferf@state.gov or at (703) 284-2715.

AUDIT FINDINGS

DEPARTMENTAL INTERNET GUIDANCE BEING ESTABLISHED

In keeping with OMB directives, the Department of State has ongoing efforts to establish guidance for managing its public Internet sites. Specifically, on June 20, 2000, a working group of representatives from across the organization issued a Department Notice, *Interim Guidance on Public Web Site Hosting*, to establish policies for Internet access and site hosting until the details on web systems requirements, content, security, incident handling, and other issues could be finalized. A second notice, *Policy for the Use of "Cookie" on Department of State Web Sites*, issued on September 27, 2000, as an addendum to the Interim Guidance, establishes the presumption that cookies should not be used on the Department's web sites.

The working group followed up with development of *Guidelines for Public Information Dissemination on the Internet*. The guidelines are designed to help ensure high quality and consistent standards for the content, organization, and presentation of information on the Department's public web sites. The guidelines reiterate restrictions on Internet cookie use, directing that bureaus, offices, or missions consult with the Bureau of Administration for advice on cookie usage and guidance on submitting requests for such approval to the head of the Department. The guidelines also discuss the requirement that web sites display privacy and security notices informing users that cookies or other means to collect data from the public are employed on the sites. The guidelines were just recently approved in February 2001 and are awaiting release throughout the Department. The guidelines will ultimately be institutionalized as regulatory policy in the Department through incorporation into chapter 5, section 700, of the Foreign Affairs Manual, *Internet and Intranet Use*, which is currently undergoing review.

DEPARTMENT WEB SITES DO NOT COLLECT PERSONALLY IDENTIFIABLE DATA

The Department of State does not use its Internet sites as a means to collect personally identifiable information on site visitors without their awareness. Our current review, similar to prior assessments, identified instances in which persistent cookies were used on the Department's web sites; however, none of the cookies were used to gather data on site visitors. In all cases, web site managers have been informed, and corrective actions are either underway or completed. The Department has other processes to collect web statistics, trend data, or log files for security purposes, but these processes also are not used to track individual users over time. Given recent legislation and ongoing discussions within the Department about potentially using the Internet to conduct electronic business, consideration may have to be given in the future to possibly using cookies or other means to collect personal information on web site visitors.

Cookies Generally Not Used on Department Web Sites

The Department generally does not use cookies on its public web sites. We found that of the 206 sites that we visited and tested, 16 used cookies. Of those 16, 7 were session cookies, which are permitted under OMB guidance. The remaining nine sites used persistent cookies, which are not allowed under Federal guidelines without the agency head approval. At two of those sites, the web managers knew that the persistent cookies were being used, but did not realize they needed authorization. For the remaining seven situations, the web managers told us they did not know that persistent cookies were being used. Web managers are currently taking steps to remove or seek Secretary approval for the nine persistent cookies that we discovered during our review. We found persistent cookies at the following sites:

Domestic

- Foreign Buildings Operations, Art in Embassies Program (aiep.state.gov)
- Diplomatic Security, Overseas Security Advisory Council (www.ds-osac.org)
- Bureau of Educational and Cultural Affairs, International Visitors Program (www.ivprograms.org)

Overseas Posts

- Namibia (www.usembassy.namib.com)
- Belize (www.usemb-belize.gov)
- Auckland (homepages.ihug.co.nz/~amcongen/ieindex.htm)
- Athens (www.usisathens.gr)
- Thessalonika (virtuals.compulink.gr/us-consulate)
- Vladivostok (vladivostok.com/usis)

Persistent Cookies Not Used to Collect Personal Data

In all nine instances where we found persistent cookies, we found no evidence that they were being used to collect personal data on site visitors. Specifically, on the three domestic web sites that had cookies, the web managers used a web site development tool, called ColdFusion. This tool automatically uses persistent cookies, which provide a convenient way to maintain user preferences (i.e., graphics display, screen color, etc.) as a user navigates from one web page to another during a site visit. The user's preferences are automatically removed from memory when the user's session ends. Web managers for these domestic sites stated that they were unaware that ColdFusion automatically uses persistent cookies. As of February 21, 2001, one office had removed the cookie from its web site, and the second office had not yet begun corrective actions. The third organization has tentative plans to seek the Secretary of State's approval to continue to use the cookie. Officials told us that several other bureaus are also planning to use ColdFusion for their web development and may not be aware that the application might automatically place cookies on their web sites.

We notified officials from the Office of International Information Programs of instances where we found persistent cookies on overseas web sites. The Office, which has responsibility for coordinating and advising overseas posts concerning their public web sites, contacted the webmasters to request explanations about the cookies and advise that they must either remove the cookies from their web sites or seek agency head approval for their use. Overseas web officials provided various reasons for using cookies. Although several of the cookies had been placed by third-party contractors, the cookies were only used for such activities as analyzing web trends, counting visitors, and facilitating user navigation through the sites. All posts that had persistent cookies have removed them from their sites.

Persistent Cookies Identified Prior to Office of Inspector General Review

Over the past year, the Department has had to address a number of other instances where persistent cookies were found on its web sites. For example, in August 2000, the Office of International Information Programs identified two overseas posts that were using cookies placed by third-party organizations to monitor web site usage. The web managers at both locations have deleted the cookies from their sites.

Further, in September 2000, the U.S. General Accounting Office reported on cookies found at two of the Department's web sites: www.usia.gov and travel.state.gov.[5] According to Department officials, the United States Information Agency web site has been shut down,[6] and the cookie at the travel web site has been eliminated. More recently, on January 26, 2001, the U.S. General Accounting Office notified the Department that it had found a third-party cookie on a Bureau of Human Resources recruitment site (www.state.gov/www/careers) and that there was no privacy notice posted about cookie use. In its response, the Department stated that the cookie had been inserted into the home page of the careers site to assess the effectiveness of banner ads that had been purchased on other web sites to promote recruitment. The Department stated that it was not aware that the cookie was being used and indicated that it has since been eliminated from the web site.

[5] *Internet Privacy: Comparison of Federal Agency Practices With FTC's Fair Information Principles*, U.S. General Accounting Office (GAO/AIMD-00-296R, September 11, 2000).

[6] The United States Information Agency has been merged into the Department of State and is no longer a separate agency.

Other Methods for Handling Personally Identifiable Data on Department Web Sites

There are several other ways in which personal data may be handled on Department of State web sites, as permitted by Federal and Departmental Internet guidelines. For example, for audit and security purposes, the Bureau of Diplomatic Security requires that the Department's web sites generate log files of when their sites are visited. The log files do not record information on individual web users. Rather, they include information such as Internet protocol addresses,[7] time frames, and Internet service providers used to access web sites. For example, when a visitor connects from America Online to a Department web site, the web management system will generate information about the visitor's web domain (aol.com) and the date and time of the visit. The logs are amassed in large files that are stored and secured for a period of 6 months, after which time they are destroyed. In case of computer security incidents, such as hacker intrusions or denials of service, the logs are turned over to security officials for investigation. The Department also uses the logs to determine web trends, create summary statistics on what information is of most and least interest, or identify systems performance or problem areas. Commercial software programs are available to enable systems administrators to easily view and analyze the logs. Officials told us that the Department began generating the logs about 2 to 3 years ago when it began increasing the number of agency web sites.

Other ways in which personal data might be handled on the Department's web sites include having individuals that live or travel abroad register electronically, providing personally identifiable information to U.S. embassy and consulate web sites to facilitate emergency communications, security preparations, or evacuations. A visitor to a Department of State web site might also provide personal information in an e-mail message sent through the site. When this occurs, the Department uses any information the visitor might provide only as a means of responding to the message. In both such instances, individuals voluntarily provide the personal information to the Department; the information is not collected on the web site without the individuals' knowledge. We found that no unauthorized ways of handling personal information were used—either directly or through third-party agreements—on the Department of State web sites that we reviewed.

Potential Need for Persistent Cookies in the Future

Although current guidance restricts cookie use, senior Department officials told us that it might be necessary in the future to use cookies on Internet web sites in order to improve the quality of service to the public. For example, Section 1704 of the Government Paperwork Elimination Act[8] requires that by 2003, executive agencies provide options for the electronic maintenance, submission, or disclosure of information, when practical, as a substitute for paper. To comply with the legislation, agencies may find it necessary to use cookies on their web sites. Currently, Department of State web sites only provide

[7] An Internet protocol address is a series of numbers used to identify a computer on the Internet. When transferring data from one computer to another, both the sending and receiving Internet protocol addresses are attached to the data packet to allow two-way communications.

[8] Government Paperwork Elimination Act, 44 USC 3504, October 1998.

information on the Department and its services. However, in the future, the Department plans to offer a variety of online services, such as passport applications, that may require the use of cookies. Further, if the Department allows users to customize their view of State web sites to display only specified information, cookies may be needed to remember the user preferences.

> **Recommendation 1:** We recommend that, in accordance with established Federal policy and Department of State guidelines, the Under Secretary for Public Diplomacy and Public Affairs direct all of the Department's bureaus, offices, and overseas missions to inspect their web sites to identify any persistent cookies and either remove them or request the Secretary's approval for their continued use.

PRIVACY STATEMENTS NOT CONSISTENTLY POSTED ON DEPARTMENT WEB SITES

We found that a number of Department of State organizations do not comply with Federal and agency requirements for posting up-to-date privacy notices on their Internet sites. The general practice is to provide a link on the initial home page that provides a central location for various disclaimers and legal notices to cover the web site as a whole. Additional privacy notices are also needed wherever information is collected from the public on the web site.

However, as of early February 2001, 116 of 206--well over half of the Department's sites that we reviewed--had no privacy statements and therefore no means of advising users of any information collected on the sites. Of the 90 sites that had privacy statements,

- 48 sites had their own privacy statements,
- 5 sites linked to the privacy statement at usinfo.state.gov, and
- 37 sites linked to the generic statement on the Department's main Internet site at www.state.gov.

Of the 37 sites that linked to the main State Department site, only 3 referenced the current notice. The other 34 referenced an outdated privacy statement, archived from a time when the main site was hosted at the University of Illinois at Chicago. The Department's main site has been managed by UUNET, another Internet service provider, since January 2001. Webmasters that we informed of the outdated privacy notices all agreed to update their site links.

Further, we found that the two sites that knowingly used persistent cookies did not post adequate privacy statements to advise site visitors of this practice. As discussed above, however, none of the persistent cookies identified were used to track or collect personal data on individual site users.

> **Recommendation 2:** We recommend that the Under Secretary for Public Diplomacy and Public Affairs direct all Department of State organizations to examine their web sites to ensure that complete and up-to-date privacy statements are posted to their web

sites, or appropriately linked to privacy statements on the primary Department web site, advising site visitors of any personally identifiable data that is collected, stored, or used by the web site for any purpose.

DECENTRALIZED MANAGEMENT STRUCTURE HINDERS DEPARTMENTWIDE OVERSIGHT OF WEB SITES

The Department's structure for managing its public web sites is highly decentralized in that a number of different organizations share responsibility for guiding or controlling various aspects of Internet management. Domestic bureaus and posts also have considerable independence regarding how to manage and host their web sites. This fragmented management structure may have contributed to the uneven compliance with Internet cookie restrictions and privacy statement requirements that we found across the Department.

Fragmented Internet Guidance, Oversight, and Control

The Department has not established a single office with responsibility for all the different aspects of web site management organizationwide. Rather, several organizations share this responsibility, individually providing coordination, guidance, oversight, and/or operational support for the Department's various public web sites.

Two organizations within the Office of Public Diplomacy and Public Affairs share responsibility for coordinating Internet web site management at headquarters and at overseas missions. Specifically, the Office of Electronic Information within the Bureau of Public Affairs clears information for public dissemination on the Internet and has basic responsibility for coordinating Internet web sites for regional and functional bureaus at Department headquarters. This Office also operates and maintains the official primary web access point for the Department at www.state.gov and provides content and design guidance to organizations that publish web pages. Similarly, the Office of International Information Programs operates and maintains the international home page for the Department, located at usinfo.state.gov. The Office provides advice and assistance to several local sites, but is primarily responsible for helping overseas missions set up their own web sites. Embassies are encouraged to consult with the Office of International Information Programs on site content and design. Neither the Office of Electronic Information nor the Office of International Information Programs has the authority to enforce web site management policy, including ensuring compliance with Federal and State Department Internet privacy guidelines.

A number of other organizations provide Internet guidance and support for web sites across the entire Department. For example, the Bureau of Diplomatic Security provides advice on web page development to ensure that Internet sites conform with security requirements, including the use of log files discussed above. The Bureau of Information Resource Management provides operational support for some web sites and incorporates Internet guidance into the Foreign Affairs Manual. Further, several organizations within the Department, including the Office of the Legal Adviser and the Office of Records and

Publishing Services within the Bureau of Administration, have responsibility for clearing privacy notices and disclaimers.

Domestic Organizations and Overseas Posts Have Web Hosting Flexibility

Amid this fragmented organizational structure, the Department's bureaus and posts have considerable flexibility regarding how they individually manage their Internet web sites. They have primary responsibility for complying with prescribed policies and ensuring privacy on their Internet sites. Because there is no mandated standard, organizations can also choose from among several web site hosting options.

Specifically, organizations can have the Department host their sites on www.state.gov, the official primary web site run by Public Affairs. With few exceptions, these sites use a standard "state.gov" naming convention. The Office of Electronic Information uses a Document Management System to centrally coordinate and monitor sites that use this naming convention. The system also facilitates update of the state.gov sites without having to input individual code changes.

Organizations, primarily overseas missions, can also have their sites hosted under a contract managed by the Office of International Information Programs, which sponsors the central usinfo.state.gov home page. Like sites on the domestic www.state.gov home page, overseas sites hosted through the Office also generally use a standard naming convention that begins with "usembassy.state.gov." The Office of International Information Programs periodically examines web sites on its home page, sends out policy reminders, and encourages regional monitoring of web sites overseas. Although the Office has no direct Internet oversight or enforcement authority, the Office has makeshift arrangements to monitor web sites for such things as cookies, install updates, or ensure that no unauthorized or classified information is used on the sites. Sites under both the central www.state.gov and the usinfo.state.gov home pages are currently hosted and provided with Internet connectivity by UUNET.

Further, organizations can host their sites at locations within the Department, independent of the two primary web sites. For example, some organizations have their sites hosted by the Business Center within the Bureau of Information Resource Management on a fee-for-service basis. Others host their web sites on their own internal web servers. Still other organizations have contracts for web hosting through local or overseas third-party companies. As discussed above, we found that at least one site hosted by a third-party contractor used a persistent cookie. Organizations that host their sites independently, either internally or externally, use a range of Internet service providers. They also use different domain names for their Internet addresses--i.e., .org, .mil, or .com--and not just .gov. The Department encourages organizations that independently host their web sites to inform and consult with the Office of Electronic Information and the Office of International Information Programs about their web sites.

Officials we interviewed expressed a variety of reasons for hosting their web sites independent of the two primary Department of State sites. For example, some had established their web sites before the two central home pages were in place. A few preferred to host their own sites internally for security reasons. Others believed that it is more efficient to have contractors externally host their sites and retain responsibility for keeping the hardware, software, and firewall security up-to date. Still others believed that third-party hosting provides greater capability and public access than the Department's two primary web pages. In the case of the overseas sites, there are some locations where local hosting is a necessity due to either a lack of adequate bandwidth or host government restrictions on access to sites outside of a country's natural domain.

A number of officials told us that, because of this fragmented Internet management structure, it is difficult to ensure that all sites are kept up-to-date or in compliance with established Internet guidelines, such as restrictions on cookie use. Further, we found no single consolidated list of every public web site in existence throughout the Department. Only by visiting offices and talking with officials across the Department were we able to identify the 206 public sites that we discuss in this report. We consequently have no means of ensuring that we identified and included all of the Department's public web sites in our Internet privacy management review.

Steps Taken to Improve Departmentwide Web Site Management

The Department of State's Internet Working Group is a first step to instituting organizationwide control of web site management. The working group began meeting in October 1999 to address public web security issues in the wake of an attack on one of the Department's overseas web sites. The working group is made up of about 30 representatives from various organizations in the Department, primarily the Bureaus of Administration, Information Resource Management, Diplomatic Security, and Public Affairs, and the Office of International Information Programs. The group meets periodically to discuss web-related issues, examine Internet use, and recommend policies to govern Internet management across the Department. It is this working group that drafted a domain name paper for simplifying web access and developed the *Guidelines for Public Information Dissemination on the Internet*. Because the working group has no authority to issue policy, the guidelines were implemented under the auspices of the five principal organizations represented in the group.

Given the great number of web-related issues that need attention, the Internet Working Group recently took steps to become formally chartered as a permanent senior-level Internet steering committee within the Department. A memorandum issued by the working group recently transmitted a draft charter and requested approval for establishing the committee from the five Assistant Secretaries of the previously mentioned organizations. The memorandum suggested that the committee serve as a forum for discussing the full range of Internet issues, including web site content and presentation, and standardizing site-naming conventions. The memo also proposed that the committee be charged with recommending policies and priorities for the development, management, and operation of Internet web sites and related services Departmentwide. The Internet Steering Committee was chartered in February 2001. To maintain continuity, the chair of the Internet Working Group volunteered to kick off the new committee and serve as chair for its first year. The committee chair, along with other officials we interviewed, suggested that establishing a staff office with full-time responsibility for web policy development, coordination, and oversight on a daily basis would also be useful to support the work of the permanent committee.

> **Recommendation 3:** We recommend that the Under Secretary for Public Diplomacy and Public Affairs establish a small Internet Program Office to provide full-time, day-to-day support for the work of the Internet Steering Committee in coordinating and addressing public web site management issues on a Departmentwide basis. The Program Office should, at a minimum, be comprised of officials from the five principal organizations represented on the Internet Steering Committee. Program Office responsibilities should include, but not be limited to:
>
> - coordinating with and supporting the activities of the Internet Steering Committee to carry out its web site policy responsibilities;
> - developing and/or updating internal policies, guidelines, and standards adopted by the committee to govern the Department's web sites in accordance with Federal guidelines;
> - providing advice and assistance to the Department's bureaus, offices, and missions regarding web site content and design;
> - maintaining a complete and up-to-date inventory of all of the Department's domestic and overseas web sites and their site hosting arrangements;
> - monitoring the Department's web sites to ensure that they are kept up-to-date and in compliance with established web management guidelines and standards;
> - referring web sites found noncompliant with established guidelines and standards to the attention of the Office of the Under Secretary for Public Diplomacy and Public Affairs, along with recommendations for corrective action; and
> - identifying and promoting the use of best practices in web site management across the Department.

DEPARTMENT COMMENTS AND OUR EVALUATION

The Office of the Under Secretary for Management and the Office of the Under Secretary for Public Diplomacy and Public Affairs provided written comments on a draft of our report. Copies of their comments are included in Appendix B. The Office of the Under Secretary for Public Diplomacy and Public Affairs generally agreed with our first two recommendations about ensuring that Department of State organizations comply with web site management requirements, such as restrictions on cookie use and requirements on posting privacy statements. Specifically, this office stated that the Department should continue its interbureau collaborative approach through the Internet Steering Committee and proposed that the committee notify all bureaus and posts on how to fully comply with these regulations. The office further stated plans to have International Information Programs and Public Affairs--its organizations with primary responsibility for

Department public web site coordination--supply staff resources in the short term to monitor and provide committee guidance to help ensure compliance with the immediate OMB requirements. We recognize recent preparations along these lines to disseminate the *Guidelines for Public Information Dissemination on the Internet* to all diplomatic and consular posts. We also support the office's ongoing commitment to providing much-needed oversight to help ensure compliance with existing Federal web management guidance.

However, the Office of the Under Secretary for Management and the Office of the Under Secretary for Public Diplomacy and Public Affairs expressed varying concerns with our third recommendation about establishing an Internet Program Office. For example, the Office of the Under Secretary for Public Diplomacy and Public Affairs recognized the need for more systematic oversight of the Department's public Internet sites and acknowledged that this might require staffing, as our recommendation suggests. However, the office preferred to work out this matter and allocate resources jointly with the Office of Management once the Internet Steering Committee is in place and its function better defined. We believe this to be a reasonable approach and acknowledge that the offices involved must have flexibility to establish the Internet Program Office as they deem appropriate. We also agree that the Internet Steering Committee is the correct forum for collaboratively finalizing such arrangements. However, to ensure Departmentwide involvement, we reemphasize our recommendation that the Program Office be comprised of officials from all principal organizations represented on the Internet Steering Committee—not just the Office of the Under Secretary of Management and the Under Secretary of Public Diplomacy and Public Affairs. Given the inconsistent compliance we found with Internet policy guidelines, we also encourage that steps be taken as soon as possible to establish the Program Office and that this matter not be prolonged beyond the FY 2002 budget planning cycle--the time frame that the Office of the Under Secretary for Public Diplomacy and Public Affairs suggested.

In contrast, the Office of the Under Secretary for Management disagreed with the need for an Internet Program Office. This office stated that our proposal for establishing such an organization conflicts with current thought on reform and delayering of the Department's Management structure. In the office's view, creation of such a Program Office constituted appointment of an "Internet Czar," which would adversely affect the Department's use of the Internet. We disagree. Our report does not advocate establishing a central, high-level office to police Departmentwide Internet management. Rather, we recommend establishing a working level office to support the activities of the Internet Steering Committee, representing multiple organizations across the Department. Our recommendation is based upon our own observations, as well as comments by a number of officials that we interviewed, concerning the Department's need for a full-time, operational body to provide day-to-day assistance for web site design and maintenance, as well as monitoring and advice to help ensure compliance with established web guidelines.

The Office of the Under Secretary for Management was also concerned that we had addressed our report recommendations only to the Under Secretary for Public Diplomacy and Public Affairs, countering that a number of organizations across the Department have responsibility for various aspects of Internet management and policy guidance. The office suggested that we address our recommendations to both Under Secretaries jointly. Again, we disagree. We recognize the Department's decentralized structure for web management and discuss this issue in detail in our report. Nonetheless, we believe that we have appropriately directed our report because our recommendations involve posting of privacy notices and use of cookies, issues closely related to web content and design, which currently fall under the purview of the Office of the Under Secretary for Public Diplomacy and Public Affairs. Specifically, the Bureau of Public Affairs and the Office of International Information within the Office of the Under Secretary for Public Diplomacy and Public Affairs currently have responsibility for coordinating and providing advice on web site management at headquarters and overseas posts. They also monitor web site content--albeit at times in a makeshift, collateral manner, as discussed in our report. As such, the Office of the Under Secretary for Public Diplomacy and Public Affairs is in the best position to lead the rest of the Department in ensuring much-needed web oversight.

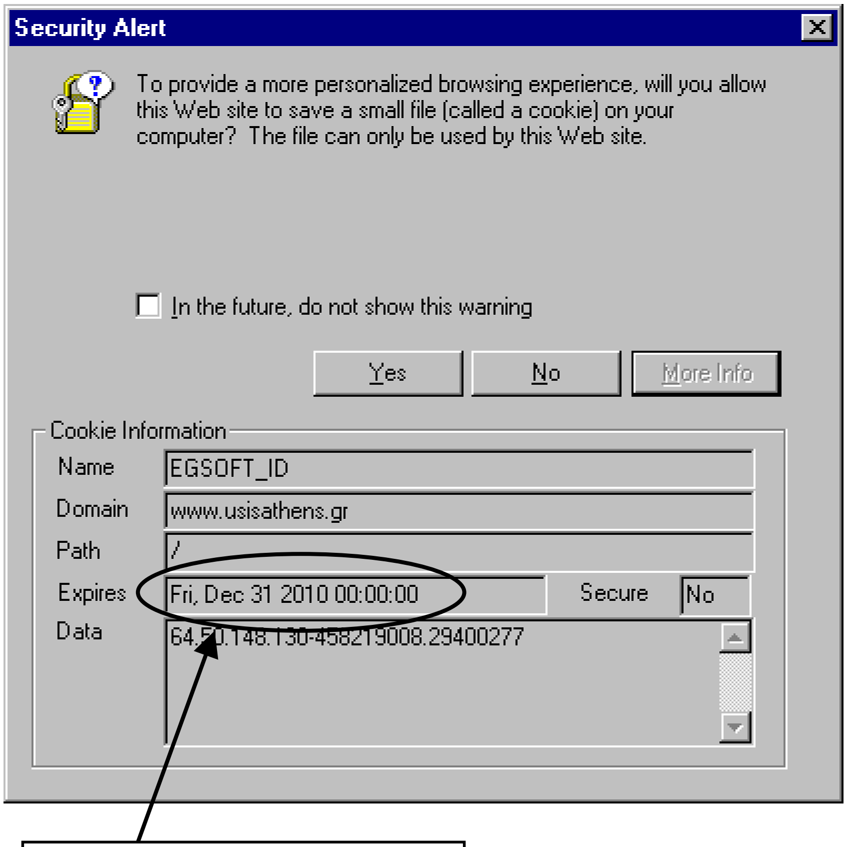
Finally, the Office of the Under Secretary for Management stated that the scope of our review went beyond the requirements of Section 646 of the Treasury and General Government Appropriations Act, 2001, in addressing issues concerning the Department's decentralized management structure. We recognize that our report moves beyond the statutory requirements and discuss this in the purpose, scope, and methodology section of our report. We believed it necessary to discuss the Internet privacy management problems we found, and to determine why these problems occurred. As we assert in our report, it is the Department's fragmented management structure that may have contributed to unauthorized use of Internet cookies and inconsistent posting of privacy statements on Department of State web sites.

APPENDIX A

WEB SITE TEST METHODOLOGY

We reviewed the 22 domestic and 184 overseas Internet web sites that we identified within the Department from January 30 through February 27, 2001. Our review entailed navigating through the web pages within each site--generally spending 3 to 10 minutes per site--to determine whether the site used cookies and posted a privacy statement advising of this practice and any other automated activities to collect personal data. To determine cookie use on the web site, we first had to change the security settings on Microsoft's Internet Explorer so that the browser would prompt us if web sites tried to place cookies on our computer. For each web site visited, we printed a copy of the site's home page, privacy statement, and any cookie notification[9] that appeared. We also examined the cookie notification to determine whether session or persistent cookies were used. Figure 1 below provides an example of a persistent cookie notification.

Figure 1: *Sample Persistent Cookie Notification*



Security Alert

To provide a more personalized browsing experience, will you allow this Web site to save a small file (called a cookie) on your computer? The file can only be used by this Web site.

□ In the future, do not show this warning

Cookie Information

Name EGSOFT_ID

Domain www.usisathens.gr

Path /

Expires Fri, Dec 31 2010 00:00:00 Secure No

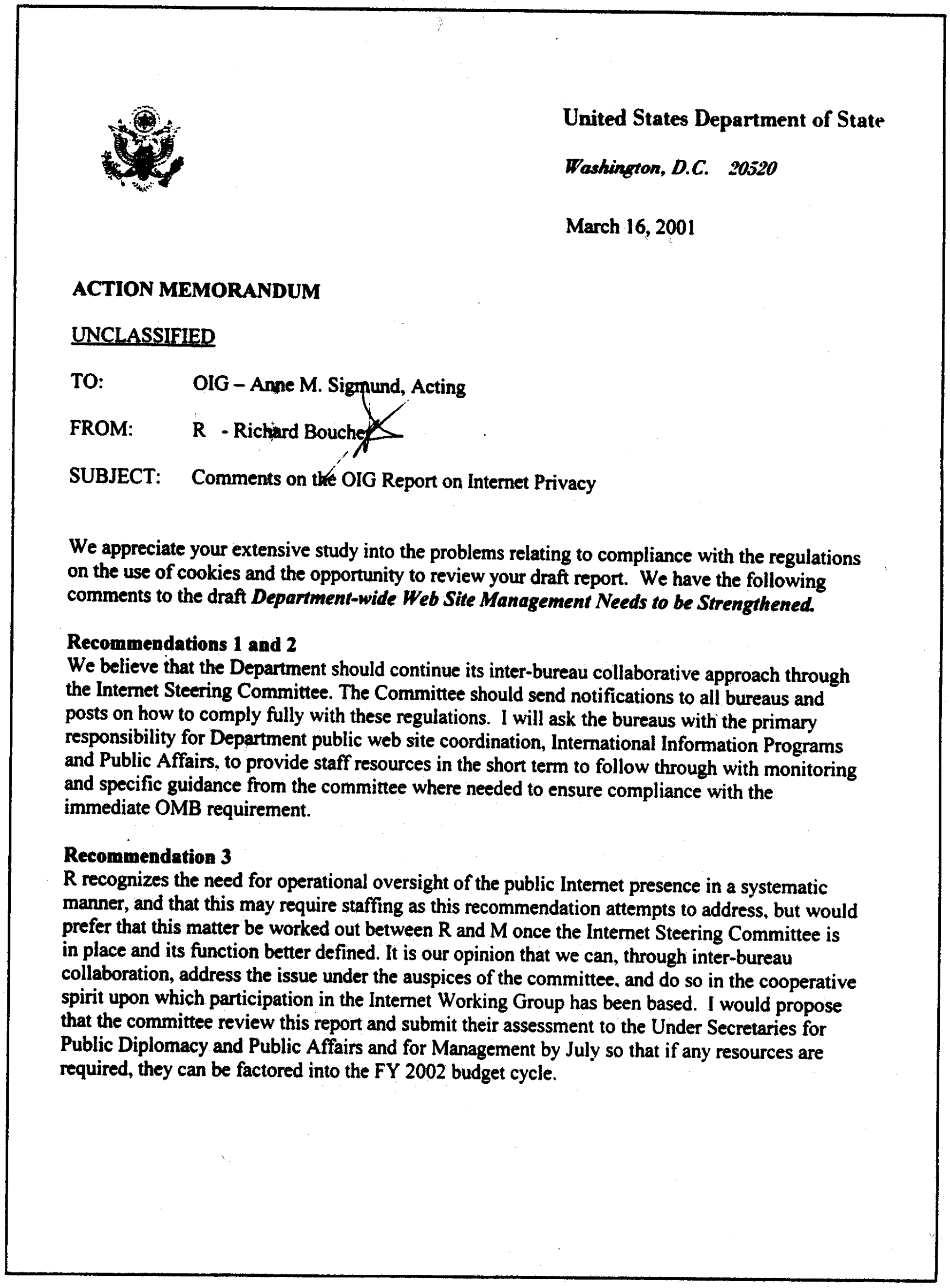
Data 64.50.148.130-458219008.29400277

Because this cookie does not expire until 2010, it is a persistent cookie.

[9] Such cookie notifications do not adequately fulfill OMB requirements to post clear, conspicuous privacy statements at major web entry points to reflect what, if any, personal information is collected on web sites and how that information is used.

APPENDIX B

DEPARTMENT COMMENTS



United States Department of State

Washington, D.C. 20520

March 16, 2001

ACTION MEMORANDUM

UNCLASSIFIED

TO: OIG – Anne M. Sigmund, Acting

FROM: R - Richard Boucher

SUBJECT: Comments on the OIG Report on Internet Privacy

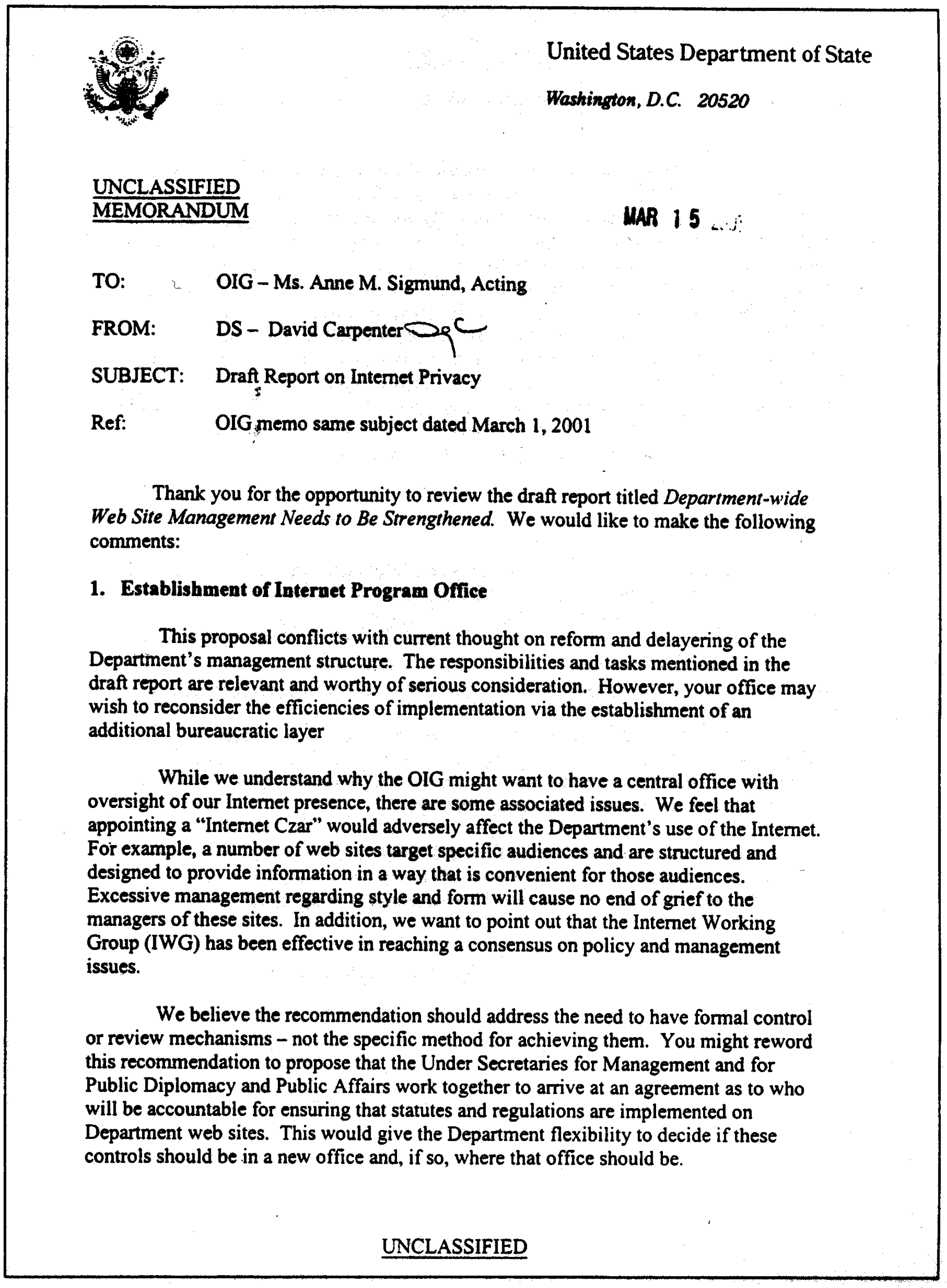
We appreciate your extensive study into the problems relating to compliance with the regulations on the use of cookies and the opportunity to review your draft report. We have the following comments to the draft ***Department-wide Web Site Management Needs to be Strengthened.***

Recommendations 1 and 2
We believe that the Department should continue its inter-bureau collaborative approach through the Internet Steering Committee. The Committee should send notifications to all bureaus and posts on how to comply fully with these regulations. I will ask the bureaus with the primary responsibility for Department public web site coordination, International Information Programs and Public Affairs, to provide staff resources in the short term to follow through with monitoring and specific guidance from the committee where needed to ensure compliance with the immediate OMB requirement.

Recommendation 3
R recognizes the need for operational oversight of the public Internet presence in a systematic manner, and that this may require staffing as this recommendation attempts to address, but would prefer that this matter be worked out between R and M once the Internet Steering Committee is in place and its function better defined. It is our opinion that we can, through inter-bureau collaboration, address the issue under the auspices of the committee, and do so in the cooperative spirit upon which participation in the Internet Working Group has been based. I would propose that the committee review this report and submit their assessment to the Under Secretaries for Public Diplomacy and Public Affairs and for Management by July so that if any resources are required, they can be factored into the FY 2002 budget cycle.

APPENDIX B

DEPARTMENT COMMENTS



United States Department of State

Washington, D.C. 20520

UNCLASSIFIED
MEMORANDUM

MAR 15

TO: OIG – Ms. Anne M. Sigmund, Acting

FROM: DS – David Carpenter

SUBJECT: Draft Report on Internet Privacy

Ref: OIG memo same subject dated March 1, 2001

Thank you for the opportunity to review the draft report titled *Department-wide Web Site Management Needs to Be Strengthened.* We would like to make the following comments:

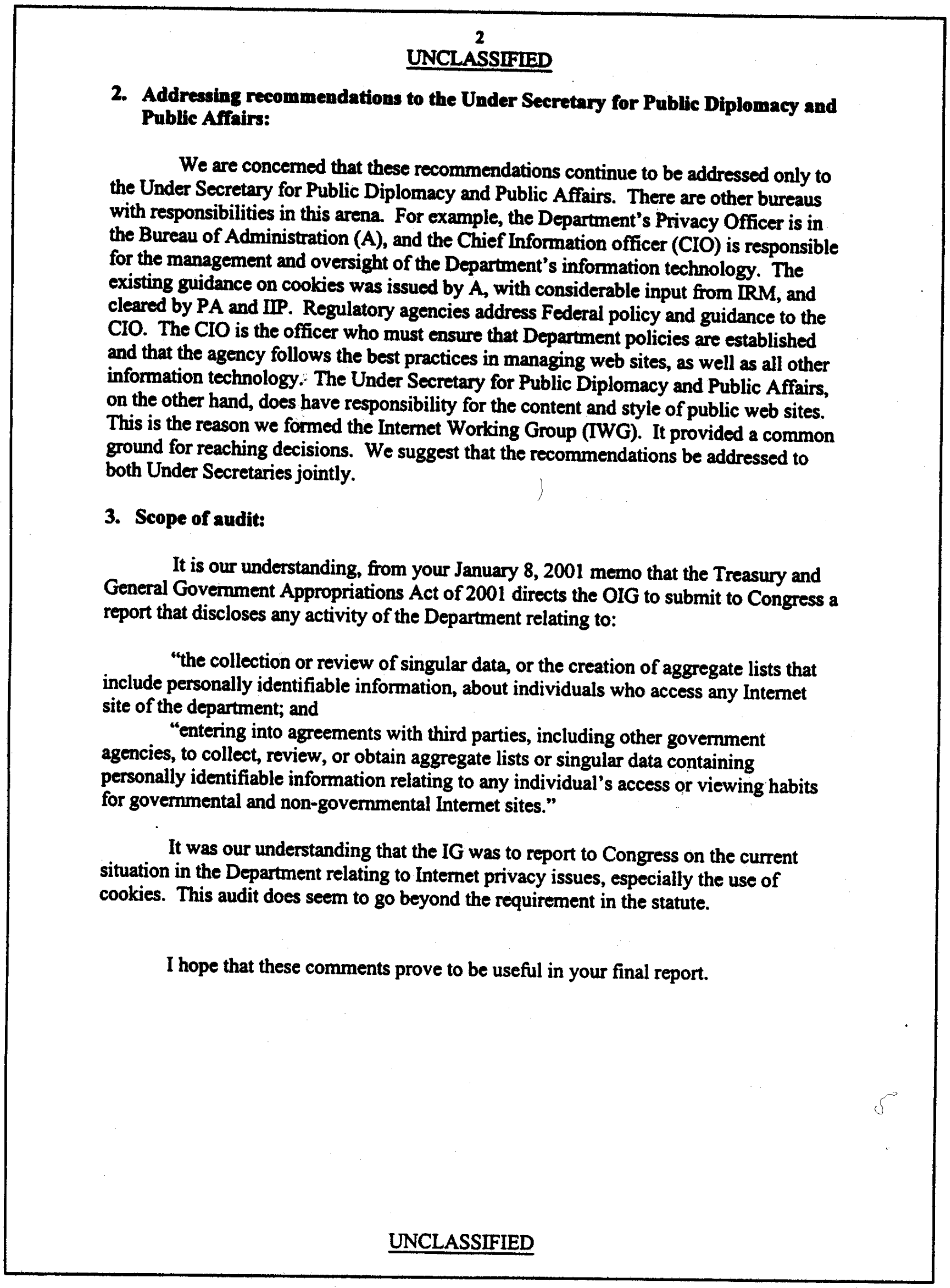
1. Establishment of Internet Program Office

This proposal conflicts with current thought on reform and delayering of the Department's management structure. The responsibilities and tasks mentioned in the draft report are relevant and worthy of serious consideration. However, your office may wish to reconsider the efficiencies of implementation via the establishment of an additional bureaucratic layer

While we understand why the OIG might want to have a central office with oversight of our Internet presence, there are some associated issues. We feel that appointing a "Internet Czar" would adversely affect the Department's use of the Internet. For example, a number of web sites target specific audiences and are structured and designed to provide information in a way that is convenient for those audiences. Excessive management regarding style and form will cause no end of grief to the managers of these sites. In addition, we want to point out that the Internet Working Group (IWG) has been effective in reaching a consensus on policy and management issues.

We believe the recommendation should address the need to have formal control or review mechanisms – not the specific method for achieving them. You might reword this recommendation to propose that the Under Secretaries for Management and for Public Diplomacy and Public Affairs work together to arrive at an agreement as to who will be accountable for ensuring that statutes and regulations are implemented on Department web sites. This would give the Department flexibility to decide if these controls should be in a new office and, if so, where that office should be.

UNCLASSIFIED



2. Addressing recommendations to the Under Secretary for Public Diplomacy and Public Affairs:

We are concerned that these recommendations continue to be addressed only to the Under Secretary for Public Diplomacy and Public Affairs. There are other bureaus with responsibilities in this arena. For example, the Department's Privacy Officer is in the Bureau of Administration (A), and the Chief Information officer (CIO) is responsible for the management and oversight of the Department's information technology. The existing guidance on cookies was issued by A, with considerable input from IRM, and cleared by PA and IIP. Regulatory agencies address Federal policy and guidance to the CIO. The CIO is the officer who must ensure that Department policies are established and that the agency follows the best practices in managing web sites, as well as all other information technology. The Under Secretary for Public Diplomacy and Public Affairs, on the other hand, does have responsibility for the content and style of public web sites. This is the reason we formed the Internet Working Group (IWG). It provided a common ground for reaching decisions. We suggest that the recommendations be addressed to both Under Secretaries jointly.

3. Scope of audit:

It is our understanding, from your January 8, 2001 memo that the Treasury and General Government Appropriations Act of 2001 directs the OIG to submit to Congress a report that discloses any activity of the Department relating to:

"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; and

"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 non-governmental Internet sites."

It was our understanding that the IG was to report to Congress on the current situation in the Department relating to Internet privacy issues, especially the use of cookies. This audit does seem to go beyond the requirement in the statute.

I hope that these comments prove to be useful in your final report.

APPENDIX C

ORGANIZATIONS THAT PARTICIPATED IN OUR REVIEW

Bureau of Administration

Bureau of Consular Affairs

Bureau of Diplomatic Security

Bureau of Educational and Cultural Affairs

Bureau of Information Resource Management

Bureau of Intelligence and Research

Bureau of Nonproliferation

Bureau of Political-Military Affairs

Bureau of Public Affairs

International Cooperative Administrative Support Services

Office of International Information Programs

Office of the Legal Adviser

Office of the Procurement Executive