

U.S. DEPARTMENT OF COMMERCE
Office of Inspector General



**PUBLIC
RELEASE**

*OFFICE OF THE CHIEF
INFORMATION OFFICER*

*Use of Internet “Cookies” and
“Web Bugs” on Commerce Web Sites
Raises Privacy and Security Concerns*

Inspection Report No. OSE-14257/April 2001

Office of Systems Evaluation



TABLE OF CONTENTS

EXECUTIVE SUMMARY	i
INTRODUCTION	1
OBJECTIVES, SCOPE, AND METHODOLOGY	2
FINDINGS AND RECOMMENDATIONS.....	4
I. Unauthorized Internet Cookies Were Found on Department Web Sites.....	4
A. Recommendations.....	6
II. Use of Web Bugs Raises Privacy and Security Concerns.....	7
A. Recommendations.....	7
III. Privacy Statements Should Be Modified to Comply with Department Policy	8
A. Recommendations.....	10
APPENDIXES	
A. Department Web Pages Where Web Bugs Were Detected	
B. CIO Response to Report	

EXECUTIVE SUMMARY

Persistent Internet “cookies” are data stored on web users’ hard drives that can identify users’ computers and track their browsing habits. “Web bugs” are software code that can monitor who is reading a web page. In addition to being able to track a user’s browsing habits, web bugs can also download files from and upload files to a user’s computer. Although these technologies have uses that do not raise privacy concerns, they are capable of being employed in a way that would violate the privacy of individuals visiting the Department’s web sites. Web bugs can also be security threats.

This report documents our evaluation of the use of persistent Internet cookies and web bugs by departmental Internet sites, as well as the adequacy of the privacy statements posted on the main web pages¹ of the Department and its operating units. We conducted our evaluation in response to Public Law 106-554, the Consolidated Appropriations Act of 2001, which requires the Inspector General of each department or agency to submit a report to the Congress disclosing any activity regarding the collection of information relating to any individual’s access or viewing habits on the department’s or agency’s Internet sites.²

We found that the majority of the Department’s Internet sites do not use either persistent cookies or web bugs. However, we did find several instances in which persistent cookies were being used without a compelling reason or the approval of the Secretary of Commerce, as required by Department and Office of Management and Budget policy. (See page 4.) We also found a number of web pages using web bug technology. (See page 7.) At the time of our fieldwork, the Department did not have a policy regulating web bug use. On April 24, the Chief Information Officer (CIO) issued a memorandum entitled *Use of “Web Bugs” on Commerce Web Sites*, which establishes a policy for web bugs similar to that for persistent cookies. Finally, we found that many of the operating units’ privacy statements do not provide all of the information required by the Department’s privacy policy. (See page 8.)

We recommend that the Department’s CIO direct operating unit CIOs and senior management to implement a strategy to control the use of persistent cookies and web bugs and to certify annually that the operating unit is in compliance with the Department’s applicable policies. (See pages 6 and 7.) We also recommend that the Department’s CIO direct operating unit CIOs and senior management to revise their privacy policy statements to make them compliant with the Department’s privacy policy. (See page 10).

We discussed our findings with the Department’s CIO on April 16, 2001. The CIO agreed with our findings, quickly promulgated a policy addressing the use of web bugs, worked with us to help ensure that the cookies we had identified were removed, and is now working to remove the web bugs. Because the CIO agreed with the findings and recommendations, we are issuing this report in final. The CIO’s memorandum indicating his concurrence is included as Appendix B to this report.

¹ A web page is an entry point, often called a home page, to a World Wide Web information site.

² An Internet site is a computer system hosting a collection of web pages on a particular subject.

INTRODUCTION

On December 21, 2000, the President signed Public Law 106-554, the Consolidated Appropriations Act of 2001.³ Section 646 of the act requires the Inspector General of each department or agency to submit a report to the Congress disclosing any activity regarding the collection of information relating to any individual's access or viewing habits on the department's or agency's Internet sites.⁴

This report documents our evaluation of the use of persistent Internet cookies and web bugs by Departmental Internet sites, as well as the adequacy of the privacy statements posted on the main web page⁵ of the Department and each operating unit. Persistent cookies are data stored on web users' hard drives that can identify the users and track their browsing habits. Web bugs are software code that can monitor who is reading a web page. In addition to being able to track a user's browsing habits, web bugs can also download files from and upload files to a user's computer. Although these technologies have uses that do not raise privacy concerns, they are capable of being employed in a way that would violate the privacy of individuals visiting the Department's web sites. Web bugs can also be security threats.

Persistent Internet Cookies

To address Internet privacy concerns of users of government web pages, the Office of Management and Budget (OMB) issued OMB Memorandum 00-13, *Privacy Policies and Data Collection on Federal Web Sites*, dated June 22, 2000. The memorandum states that government web pages should not use Internet cookies without the approval of the agency head and that cookies can be used only if (1) the site gives clear and conspicuous notice, (2) there is a compelling need to gather the data, and (3) appropriate and publicly disclosed privacy safeguards exist for handling any information so gathered.

The Department's Chief Information Officer (CIO) clarified OMB's policy to the operating unit CIOs in an October 20, 2000, memorandum, *Use of "persistent cookies" on Commerce Web Sites*. This memorandum distinguished between persistent cookies and session cookies. Because persistent cookies remain on users' hard drives after a browsing session is completed and can be used to track individuals' browsing habits, they are not allowed without Secretarial approval. Session cookies, which are not used to track the browsing habits of users, do not remain on users' hard drives and are permitted if their use is disclosed in the web page privacy statement.

The CIO's memorandum assigns to operating unit CIOs the responsibility for ensuring that persistent cookies are not used to collect personal information and track the browsing habits of

³ The law comprises several appropriations measures, including the Departments of Treasury, Labor, Health and Human Services, and Education, and Related Agencies Appropriations Act, 2001.

⁴ An Internet site is a computer system hosting a collection of web pages on a particular subject.

⁵ A web page is an entry point, often called a home page, to a World Wide Web information site.

Department web page users. If an operating unit requires the use of persistent cookies, it must submit a request describing the compelling need to the Secretary of Commerce through the Department's CIO and provide a copy of the web page privacy statement that discloses how the information derived from persistent cookies will be used.

On January 11, 2001, Commerce's CIO council adopted the Department's policy on the use of persistent cookies, which supercedes the CIO's October 20 memorandum. In general, this policy restates the content of the CIO's memorandum and the OMB memorandum. At the time of our fieldwork, no operating unit had submitted a request to the Secretary for approval to use persistent cookies on any Department web page.

Web Bugs

A growing threat to both privacy and security is a technology known as web bugs. Web bugs are capable of tracking web users' browsing habits, downloading files from users' computers, and storing files on users' computers without their knowledge. Web bugs are invisible to a user without specific detection software. The software code associated with web bugs can exist on the computer hosting the web page or on another computer connected to the Internet. When a user views the web page, the results from the execution of the web bug are sent to the web user's computer and acted upon. The actions performed by a web bug that resides on a computer outside the control of the web page owner (i.e., non-departmental controlled computers) cannot be certified to perform the intended action. For example, the code could have a hidden malicious action, such as to install an application on the user's computer to monitor and track information when interacting on the Internet or to assume control of the computer.

Because the use of web bugs is relatively new, neither OMB nor the Department had a policy regulating their use on government web pages. On April 24, after we brought this matter to his attention, the Department's CIO issued a policy for use of web bugs similar to that for use of persistent cookies.

OBJECTIVES, SCOPE, AND METHODOLOGY

The objective of this evaluation was to determine whether the Department's web pages comply with Department and OMB policies regarding Internet privacy. Specifically, we evaluated the web pages to determine if persistent cookies were being used, and we reviewed the adequacy of the privacy statements posted on the main web pages of the Department and its operating units. We expanded our scope to address web bugs since their use raises privacy concerns similar to those raised by persistent cookies, as well as security concerns. To view the web pages of the Department and its operating units, we used Microsoft Internet Explorer configured to detect the presence of Internet persistent cookies. Additionally, we used a tool obtained from the University of Denver Privacy Center, which we installed in Explorer, to detect the presence of web bugs.

In discussions held with the Department's CIO staff and operating unit CIOs and staff as we planned our evaluation strategy, we found that reliable data was not available on the number of web sites or web pages in the Department. This is the case, in part, because the operating unit CIOs do not control many of the departmental web sites. Instead, a significant number of web sites are controlled by line organizations within the operating units. Therefore, our evaluation strategy was to start with the main Department web site, along with the main web site for each of the operating units, and systematically assess them. For each web page, this involved spending several minutes making selections to obtain information available on that web page and then visiting other web pages that were referenced by the initial web page under evaluation. While our evaluation could not be exhaustive in terms of assessing every Department web page, we believe that our work provides an important indication of the challenges of complying with privacy requirements on federal web sites.

We conducted our fieldwork between February and April 2001, holding an entrance conference with the Department's CIO on February 14, and meeting with him again on April 16 to discuss our findings. Because the CIO concurred with our findings and recommendations, we are issuing this report in final.

This evaluation was conducted in accordance with the *Quality Standards for Inspections* issued by the President's Council on Integrity and Efficiency and was performed under the authority of the Inspector General Act of 1978, as amended, and Department Organization Order 10-13, dated May 22, 1980, as amended.

FINDINGS AND RECOMMENDATIONS

I. Unauthorized Internet Cookies Were Found on Department Web Sites

Our evaluation detected 12 unauthorized persistent cookies on Department web pages in violation of both Department and OMB policy. Four of the cookies are what are known as client-side state cookies, and the other eight are known as third-party cookies. While privacy issues are a concern with both types of cookies, the presence of third-party cookies is especially serious because the data they collect is completely out of the Department's control.

Client-side state cookies are used by web pages to store small amounts of information on the user's hard drive and exchange it with the web server each time the web page is visited. At present, the primary privacy threat is the ability to actively track web visitors by assigning a unique tag that is stored in the cookie and maintained by the web site. Thus, every time the web user visits the web page, the unique tag stored in the cookie is matched with a tag stored in a database on the web site, resulting in browsing habit information being captured and maintained on specific web users. In our discussions with the officials responsible for the web sites, we were told that one was using a client-side cookie to identify new web site visitors, while the others were not obtaining any specific user information.

Third-party cookies raise additional privacy concerns. They are commonly associated with graphic images referenced in the HTML⁶ code for a web page. These images actually reside on another computer connected to the Internet. As the HTML code is executed to present the user with the display of the web page, the images are retrieved from the third-party computer and displayed on the user's computer, third-party cookies are stored on the user's computer, and browsing habit information is captured and maintained on the third-party computer in a way similar to client-side cookies. The third-party cookies we detected were associated with non-government computers, resulting in the storage of any captured privacy information on computers over which the Department has no control. Unless users specifically configure their browsers to alert them to cookies, the information is sent and received without user knowledge or involvement.

The 12 persistent cookies that we detected are discussed below:

Client-State Persistent Cookies

- Found on the web page <http://oamweb.osec.doc.gov>, hosted by the Office of Acquisition Management within the Office of the Secretary, with an expiration date of December 31, 2010. According to this office, the cookie was being used to count the number of visitors to the site and was not capturing any privacy information. After being informed that the cookie violated Department and OMB policy, the office removed it.

⁶ HTML stands for Hyper Text Markup Language, the language used to create web documents and to generate the web page on a user's display.

- Found on the web page <http://www.commits.doc.gov>, hosted by the Office of Acquisition Management within the Office of the Secretary, with an expiration date of December 31, 2010. According to this office, the cookie was being used to count the number of visitors to the site and was not capturing any privacy information. After being informed that the cookie violated Department and OMB policy, the office removed it.
- Found on the web page <http://www.osf.noaa.gov>, hosted by the Next Generation Weather Radar Operations Center within the National Weather Service (NWS), with an expiration date of January 1, 2035. According to NWS officials, they were not aware of the existence of the cookie because it was not part of the code associated with the web page. Rather, the cookie was produced by the Microsoft Internet Information Server product, which is used to support the center's web page operation. After we identified the cookie, NWS learned that a default installation setting caused the server product to generate a persistent cookie and changed the setting to eliminate the cookie. NWS told us that no privacy information was captured through the use of the cookie.
- Found on web page <http://www.fakr.noaa.gov>, hosted by the Alaska Regional Office of the National Marine Fisheries Service, with an expiration date of December 31, 2010. The cookie was being used to identify new visitors to the web site. After being informed that the cookie violated Department and OMB policy, the office removed it.

Third-Party Persistent Cookies

- Found on web page <http://sites.usatrade.gov/ctm>, hosted by the U.S. and Foreign Commercial Services within the International Trade Administration. The third-party web site that created the cookie was located at *netscape.com*, and the expiration date was June 29, 3379. The cookie was being used to count the number of visitors to the web site. After being informed that the cookie violated Department and OMB policy, the office removed it.
- Found on web page <http://www.mac.doc.gov/ftaa2005/index.htm>, hosted by the Office of NAFTA and Intra-American Affairs within the International Trade Administration. The third-party web site that created the cookie was located at *h2.humanclick.com*, and the expiration date was April 13, 2002. The purpose of the cookie is not known, and it has been removed.
- Found on web page <http://www.ita.doc.gov/td/energy>, hosted by the Office of Trade Development within the International Trade Administration. The third-party web site that created the cookie was located at *h2.humanclick.com*, and the expiration date was April 13, 2002. The purpose of the cookie is not known. After being informed that the cookie violated Department and OMB policy, the office removed it.
- Found four cookies on web page <http://www.nmfs.noaa.gov/aquaculture.htm>, hosted by the National Marine Fisheries Service. The third-party web site that created the cookies was

located at *superstates.com*, and their expiration date was December 31, 2010. The cookies were being used to count the number of visitors to the web site. After being informed that the cookies violated Department and OMB policy, the office removed them.

- Found on web page <http://seafood.nmfs.noaa.gov>, hosted by the National Marine Fisheries Service. The third-party web site that created the cookie was located at *aaddzz.com*, and the expiration date was May 3, 2001. The cookie was being used to count the number of visitors to the web site. After being informed that the cookie violated Department and OMB policy, the office removed it.

The Department currently has a policy entitled *Enforcement of Web Site Standards and Policies*, requiring the operating unit CIOs to certify annually to the Department's CIO that all web sites of their organization comply with the Department's web standards and policies. If any deficiencies exist, the operating unit CIO is to provide a plan to bring the web sites into compliance, and the Department's CIO is to determine whether the proposed approach is acceptable. The Department's CIO has the authority to shut down any site for non-compliance. We believe that the certification should explicitly state whether persistent cookies are being used, and if so, indicate the compelling reason and whether Secretarial approval has been obtained. Most operating unit CIOs do not control all of the web pages of their unit. For those units, we believe that the certification regarding persistent cookies should be made by the head of the operating unit.

The Department and operating units must take aggressive steps to ensure that persistent cookies are not used on their web pages unless a compelling need can be demonstrated and Secretarial approval is obtained. Particular vigilance is needed to ensure that third-party cookies are not used.

A. Recommendations

We recommend that the Department's Chief Information Officer:

1. Reiterate the Department's policy on use of persistent cookies to all operating unit CIOs and senior management.
2. Work with each operating unit's CIO and senior management to implement a strategy to control the use of persistent Internet cookies to include:
 - a. Activities to monitor the use of persistent cookies on their web pages,
 - b. Definition of a periodic timeframe to perform monitoring activities, and
 - c. Annual certification by the senior management or CIO of each operating unit to the Department's CIO that either no persistent cookies or only approved persistent cookies are used on its web pages.

II. Use of Web Bugs Raises Privacy and Security Concerns

We found web bugs on 23 web pages. The locations of these web bugs are listed in Appendix A. As noted previously, because the use of web bugs is relatively new, the Department did not have a policy to regulate their use at the time of our fieldwork, but has recently issued such a policy. The privacy concern is that, like persistent cookies, web bugs can be used to track the web browsing habits of visitors to Department web page. Web bugs also present a security threat because they can be used to perform malicious actions against the computer systems used by web page visitors.

Some examples of the malicious actions that web bugs can perform include searching for the existence of specific information, such as financial information, on a user's hard drive; downloading files from a user's system; and uploading files onto a user's computer. A web user would be unaware of the presence of web bugs without using detection software. Even if such software were used, the malicious actions performed by identified web bugs could go undetected.

In all but a single instance, the web bugs that we detected exchanged information with non-government computers. Thus, for all of the identified web bugs but one, the software executed by the web bugs resides on non-government computers. The fundamental risk to privacy and information security is the lack of Department control over the web bug software. Even if the web bug software were determined by Department information security personnel to be safe to use, the software is still not under Department control. Consequently, the software could be modified without Department knowledge, and malicious actions could be inserted into the web bug code. Due to the limited scope of our review, we did not evaluate the web bugs that we found for malicious actions.

As with persistent cookies, we believe that the certification of compliance with web standards and policies should explicitly state whether web bugs are being used, and if so, indicate the compelling reason and whether Secretarial approval has been obtained. In operating units where the CIO does not control all of the web pages, the certification regarding use of web bugs should be made by the head of the operating unit. Finally, the Department and operating units must aggressively ensure that web bugs are not used on their web pages unless a compelling need can be demonstrated and Secretarial approval is obtained.

A. Recommendations

We recommend that the Department's Chief Information Officer:

1. Ensure that all web bugs found by our evaluation, as well as any other web bugs, are removed from Department web pages.
2. Reiterate the Department's policy on use of web bugs to all operating unit CIOs and senior management.

3. Work with each operating unit's CIO and senior management to implement a strategy to control the use of web bugs to include:
 - a. Activities to monitor the use of web bugs on their web pages,
 - b. Definition of a periodic timeframe to perform monitoring activities, and
 - c. Annual certification by the senior management or CIO of each operating unit to the Department's CIO that either no web bugs or only approved web bugs are used on its web pages.

III. Privacy Statements Should Be Modified to Comply with Department Policy

Our review of the privacy statements posted on the Department's and operating units' main web pages revealed that the majority do not comply with Department policy. The Department's CIO Council approved the policy entitled *Privacy Statements and Information Collection* on September 14, 2000.⁷ The policy requires that the information collection practices be described in terms of (1) what information is collected, (2) how long information is retained, (3) how the information is used, (4) how e-mail messages are handled, and (5) what use, if any, is being made of Internet cookies. In addition, the link from a web page to the privacy statement should be clearly labeled.

Table 1 identifies which elements of the privacy statements that we examined comply with the Department's privacy policy. Of the 23 privacy statements we reviewed, we found the following five to be compliant: Department, Office of the Secretary, Economic Development Administration, National Institute of Standards and Technology, and Office of Inspector General. The privacy statements of the Bureau of Export Administration and the Bureau of Economic Analysis partially address the policy in terms of generally defining the kinds of information collected but do not precisely describe this information. Two elements of the Economic Development Administration's statement are marked as not applicable because the privacy statement indicates that its web pages do not collect any information from web visitors.

The web pages for the Technology Administration and the Office of Technology Policy do not clearly identify the link to their privacy statements. For both of these web pages, the link used to obtain the privacy statement is labeled as "Credits and Disclaimers." The Department's policy states that the link to a privacy statement must be clearly labeled.

⁷ Because of our limited scope, we did not evaluate the privacy statements on pages beyond the operating units' main web pages.

Table 1
Status of Department and Operating Unit Privacy Statements

Organization	Information Collected	Information Retention	Information Use	E-Mail Handling	Internet Cookie Use
Department of Commerce	Ö	Ö	Ö	Ö	Ö
Office of the Secretary	Ö	Ö	Ö	Ö	Ö
Bureau of Export Administration	Partial		Ö	Ö	Ö
Economics and Statistics Administration	Ö	Ö	Ö	Ö	
Bureau of Economic Analysis	Partial	Ö	Ö		Ö
Bureau of the Census	Ö		Ö	Ö	Ö
STAT USA	Ö	Ö	Ö	Ö	
Economic Development Administration	Ö	N/A	N/A	Ö	Ö
International Trade Administration	Ö		Ö		
Minority Business Development Agency					
National Oceanic and Atmospheric Administration	Ö	Ö	Ö		
National Weather Service			Ö		
National Environmental Satellite, Data, and Information Service	Ö	Ö	Ö		
National Marine Fisheries Service	Ö	Ö	Ö		
National Ocean Service	Ö		Ö	Ö	Ö
NOAA Research	Ö	Ö	Ö		
National Telecommunications and Information Administration	Ö	Ö	Ö		
Office of Inspector General	Ö	Ö	Ö	Ö	Ö
U.S. Patent and Trademark Office	Ö		Ö	Ö	Ö
Technology Administration	Ö		Ö	Ö	
National Institute of Standards and Technology	Ö	Ö	Ö	Ö	Ö
National Technical Information Service	Ö			Ö	Ö
Office of Technology Policy	Ö		Ö	Ö	

Ö Indicates compliance with the specified policy element.

 Denotes that the organization is fully compliant with all policy elements.

N/A—Not applicable

A. Recommendations

We recommend that the Department's Chief Information Officer:

1. Direct the operating unit CIOs and senior management to ensure that appropriate changes are made to their privacy statements so that they are compliant with the Department's privacy policy.
2. Direct the operating unit CIOs and senior management to ensure that all web page links to a privacy statement are labeled as either "Privacy Statement" or "Privacy Notice."

APPENDIX A

Department Web Pages Where Web Bugs Were Detected¹

The Bureau of Export Administration

www.bxa.doc.gov
www.bxa.doc.gov/factsheets/facts3.htm
www.bxa.doc.gov/FOIA/PrivacyInfo.html
www.bxa.doc.gov/factsheets/ExporterAssistance.html
www.bxa.doc.gov/AntiboycottCompliance/OACRequirements.html
www.bxa.doc.gov/AntiboycottCompliance/OACAntiboycottRequestExamples.html
www.bxa.doc.gov/Seminars/SeminarDescription.htm
www.bxa.doc.gov/Seminars/elsem.htm
www.bxa.doc.gov/DPL
www.bxa.doc.gov/DPL/denialist.html
www.bxa.doc.gov/DPL/LastChanges.html
www.bxa.doc.gov/Enforcement/eeprogrm.htm

International Trade Administration

www.trade.gov/td/tic/
www.ita.doc.gov/td/aerospace/
www.ita.doc.gov/td/energy/
infoserv2.ita.doc.gov/ot/home.nsf
www.ita.doc.gov/td/auto/

National Oceanic and Atmospheric Administration

seafood.nmfs.noaa.gov/
www.nmfs.noaa.gov/trade/Japan98SoftshellTurtleMarket.htm
www.nmfs.noaa.gov/trade/JAPAN98LIVEfishreport.htm
www.nmfs.noaa.gov/trade/Japan98SummerFlounder.htm
www.nmfs.noaa.gov/trade/EUCONTENTS.htm

National Institute of Standards and Technology

www.nist.gov/success/

¹ All of the web bugs except for NIST's exchanged information with non-government computers.



UNITED STATES DEPARTMENT OF COMMERCE
Chief Financial Officer
Assistant Secretary for Administration
Washington, D.C. 20230

APR 27 2001

APPENDIX B

MEMORANDUM FOR: Judy Gordon
Assistant Inspector General for Systems
Evaluation

FROM: Roger W. Baker *Roger W. Baker*
Chief Information Officer

SUBJECT: Inspection Report No. OSE-14257

We concur with the findings and recommendations of your report on the use of Internet cookies and Web bugs on Department of Commerce Web sites.

Your report states that the Department has issued good, sound policies that prohibit the use of persistent cookies and Web bugs, but that these policies have not been followed in all cases. We will be taking corrective actions to comply with your recommendations. Thanks for the opportunity to comment.