MEMORANDUM FOR: ROLAND DROITSCH
Deputy Assistant Secretary
Office of the Assistant Secretary
for Policy

FROM: JOHN J. GETEK
Assistant Inspector General
for Audit

SUBJECT: OIG Results on Privacy Policies and Data Collections on DOL Web Sites
Final Letter Report Number: 17-01-002-01-010

The Department of Labor's (DOL) Office of Inspector General (OIG) assessed DOL's policies and practices related to personal privacy and data collections on DOL Internet web sites, including the use of cookie technology.

OIG, working cooperatively with the Office of Assistant Secretary for Policy (OASP), recognizes the Department and its agencies took corrective actions while OIG was performing its work to abate vulnerabilities related to visitors being properly notified of their privacy, security, and use of collected personal identifying information. Agencies' actions included modifying their major entry pages and personal information collection vehicles, and the related visitor notifications. Due to these ongoing actions, not all management actions are necessarily reflected in OIG's results. Your full response to the draft report elaborates on this timing issue and is attached to this final report as additional information.

Summary

We found the Department of Labor:

- **!** Has an overall governing web site management policy. Also, OASP has been assigned specific agency responsibility for managing the Department's and agencies' web sites. *OIG has discussed the related policies with the OASP and Office of the Solicitor, and was informed that these offices were coordinating to make further refinements to the related web policies.*

- **!** Collects and reviews personally identifiable information about individuals who access and complete personal identifying collection vehicles on DOL Internet web sites. These collections establish enough personal information about the visitor that can be used, for example, to respond to visitors' requests for public interest material offered by the agencies. *The visitors' personal identifying information, based on OIG interviews and tests, are not maintained for any other purpose.*

- **!** Has one agreement with a third party to collect personal identifying visitor information. The Employment Standards Administration, Office of Federal Contract Compliance Programs, has an agreement with the Eastern Research Group, Inc. The purpose is to conduct the Equal Opportunity Survey to obtain employment information from Federal contractor establishments. The collection instrument, reportedly, is electronically secured and collects only the name of the person(s) responsible for the submission of the Equal Opportunity Survey. *OIG does not consider this collection to be related to maintaining any personal information that can be used to track any individual's Internet access or viewing habits.*

- **!** Has agencies interpreting the related Internet policy differently concerning the definition of what constitutes major entry pages and proper visitor notifications. *OIG identified conditions that show multiple interpretations by DOL agencies as to the implementation of the related Internet policy covering major web entry pages, personal information collection vehicles, and elements of proper notifications to web visitors.*

- **!** Does not use persistent or session cookies to track personal identifying information. *OIG confirmed through testing and interviews that persistent cookies are not in use at DOL.*

Background

Under Section 646 of the Treasury and General Government Appropriations Act of 2001, the Inspector General (IG) was to determine and report to Congress the extent the Department and its agencies are engaged in the following activities:

- -- the collection or review of singular data, or the creation of aggregate lists that include personal identifiable information, about individuals who access any Internet site of the Department or agency; and

- -- the entering into agreements with third parties, including other government agencies, to collect, review, or obtain aggregate lists or singular data containing personal identifiable information relating to any individual's access or viewing habits for governmental and nongovernmental Internet sites.

DOL's governing policies are found in Department of Labor Manual Series (DLMS) - 9, Chapter 1500, Privacy Policy on Data Collection Over Department of Labor Web Sites, which became effective on December 22, 2000.

The following key definitions from the Department's governing policy were used in assessing the Department's and agencies' compliance:

Major Entry Page - is a primary agency web page that acts as a portal to other web pages. It includes the agency's home page; a server home page; a page advertised to the public in pamphlets, brochures, or press releases; major topical and program home pages; and any other DOL portal page or web site main page.

Personal Identifying Information - refers to any information that can be used to ascertain the identity of an individual. Examples include name, address, telephone number, and social security number.

Personal Information Collection Vehicles - refers to forms, questionnaires, and solicitation for the submission of personal identifying information from the public on the DOL Public Web Site. Except for personal information collection vehicles targeted at children (see Section 8g), for the purposes of this definition and policy, excluded are general contact links (i.e., HTML "mail to" links), which do not request specific information including Webmaster, comment, or suggestion links.

Cookie - is data used to establish and maintain a dialog between the user and the web server and/or track the activities of a user through the web site. There are primarily two types: persistent cookies and session cookies. Persistent cookies are stored on a user's hard drive and typically have a longer life, based on expiration date, than session cookies, which are stored in a browser's memory and are discarded after exit from the browser.

Methodology and Scope

In cooperation with the OASP, OIG performed an assessment of the Department's and agencies' Internet web activities by performing a survey, compiling survey results, and testing selected web sites. The assessment was performed using criteria found in: Federal guidance - OMB Memorandum, M-00-13, Privacy Policies and Data Collection on Federal Web Sites; and DOL policy - Secretary's

Order 2-2000, U.S. Department of Labor Internet Services, and
DLMS - 9, Chapter 1500, Privacy Policy on Data Collection Over Department of Labor Web Sites.

The assessment covered the period of January 16, 2001 to February 20, 2001. During this period, OIG interviewed DOL Webmasters and other responsible officials in the following agencies: Employment Standards Administration (ESA), Employment and Training Administration (ETA), Mine Safety and Health Administration (MSHA), Occupational Safety and Health Administration (OSHA), OIG, and OASP. Using judgmental selection, OIG tested 143 DOL web pages to assess agencies' Internet web management practices related to current guidance and policy.

Assessment Results

Web Page Test Results - OIG initially selected 148 DOL web pages for testing. The OIG found five pages did not meet the definition of a major entry page, and, therefore, they were omitted from the testing. The 143 web pages tested included several types of major entry pages and consisted of the following number of each type:

- 4 Server Default Pages
- 7 Agency Home Pages
- 19 Program Home Pages
- 21 Main Menu Pages
- 5 Children's Home Pages
- 35 Topical Home Pages
- 24 Region Home Pages
- 21 Advertised Pages
- 7 Data Collection Vehicles

Each of the 143 web pages was tested for proper privacy, security, and cookie use notifications, and notifications involving use of personally identifiable information. The following test results show various degrees of implementation and interpretation of DOL's related policy.

RESULTS OF TESTING (1)

Number of Occurrences (2)	Characteristics
33	(A) Privacy and Security Statement complies with policy
24	(B) Privacy and Security Statement exists but did not contain the "Cookie Use Notice"
70	(C) Privacy and Security Statement does not exist
22	(D) Privacy and Security Statement does not conform to DOL's model language (Occurs in four agencies)
15	(E) Privacy and Security Statements were found on secondary web pages
1	(F) Privacy Policy icon (button) exists, but page could not be found

(1) Results may not reflect recent changes made by the Department and agencies during this assessment.
(2) Some individual pages tested resulted in identification of multiple characteristics, i.e., (B) & (D).

We found in testing agency web sites for personal information collection vehicles, five agencies (BLS, ESA, ETA, MSHA, and OSHA) had personal information collection vehicles and the Department's policy should apply to each. *Of the collection vehicles tested, only MSHA's collection vehicle complied with DOL's policy.*

Also identified was the Employment Standards Administration, Office of Federal Contract Compliance Programs'agreement with the Eastern Research Group, Inc. The purpose is to conduct the Equal Opportunity Survey to obtain employment information from Federal contractor establishments. The collection instrument, reportedly, is electronically secured and collects only the name of the person(s) responsible for the submission of the Equal Opportunity Survey. *OIG does not consider this collection to be related to any individual's Internet access or viewing habits.*

Interview Results - OIG interviewed the agencies' Webmasters and other responsible officials in the following agencies: ESA, ETA, MSHA, OSHA, OIG, and OASP. OASP is the responsible agency for the overall management of DOL's web sites as well as the agency that maintains the Department's web server and other agency web sites.

Interviews were performed to get agency perspectives on cookie usage, implementation of privacy statement policies, and use of data collection vehicles. Information from the interviews included:

- - Several instances of past persistent cookie usage were promptly addressed by officials when it was brought to their attention. In most cases, the persistent cookies were being created by new or updated versions of web server software with default settings to create them. Agency officials promptly instituted procedures for reviewing default settings upon all updates of software.

- - Agencies do not currently use persistent or session cookies to track personal identifying information. However, agencies can use persistent cookies but must justify the need and obtain OASP approval prior to their use.

- - All web developers indicated they were aware of the DLMS - 9, Chapter 1500, policy.

- - Agencies did not have specific policies or procedures in place to perform internal reviews for compliance, but all Webmasters and officials interviewed indicated they perform thorough examinations of their web sites.

- - Agencies' major points of entry are to include press releases, pamphlets and brochures, but officials were unable to say whether the agencies always follow the practice.

- - Not all agencies agreed with the Department's policy to cover web pages that can be

reached below agency and top program level pages. However, one agency, MSHA, indicated it uses the web server software to identify lower pages with significant entry traffic. MSHA noted that it also includes a link to a privacy statement on all web pages as a default setup for development.

- - The privacy statement being used by the agencies differs by agency. Most agencies use the DOL privacy statement as a model; however, some agencies have homegrown statements that may not be in full compliance with the model statement.

Recommendation

OIG recommends the Assistant Secretary for Policy clarify and strengthen its policy, DLMS - 9, Chapter 1500, to better facilitate consistent implementation across the Department's and agencies' web sites and perform related assessments of the agency web sites.

We appreciate the professionalism and assistance you and your staff provided in responding to this high priority congressional mandate. Should you have any questions related to this effort, please call Robert W. Curtis (693-7001) or Keith E. Galayda (693-5259).

Attachment