DOE/IG-0493

# AUDIT REPORT

## INTERNET PRIVACY

FEBRUARY 2001

U.S. DEPARTMENT OF ENERGY
OFFICE OF INSPECTOR GENERAL
OFFICE OF AUDIT SERVICES

February 9, 2001

MEMORANDUM FOR THE SECRETARY

FROM: Gregory H. Friedman (Signed)
Inspector General

SUBJECT: INFORMATION: Report on "Internet Privacy"

## BACKGROUND

Recently enacted appropriations law required agency Inspectors General to report within 60 days on the collection of information about individuals accessing agency web sites. With limited exceptions, the Department of Energy is prohibited from collecting personal information from individuals accessing its public web sites, and must post conspicuous privacy notices containing clear and unambiguous explanations of any permissible data collection activities and their purpose. The most prominent example of an impermissible collection method is through the use of "persistent cookies." Persistent cookies are small files containing unique identifiers that a web server places on a site visitor's computer that can be used to retrieve information about the user. These files remain embedded in a user's hard drive and can facilitate information collection until they expire or are removed.

The objective of our audit was to determine whether the Department's method of collecting data from its public web site visitors was consistent with applicable Federal regulations.

## RESULTS OF AUDIT

Based on the results of our audit, we concluded that the Department cannot assure that the privacy of its web site visitors is properly protected in all instances. The Department's data collection methods were not uniformly consistent with applicable regulations. Our review of 93 web sites sponsored by the Department or its contractors disclosed that approximately 12 percent impermissibly employed persistent cookies to collect information from site visitors. Further, approximately 30 percent of the web sites we reviewed did not satisfy Federal disclosure requirements.

These Internet site privacy control weaknesses occurred because the Department lacked clear and current implementing guidance and did not provide consistent oversight of web development and operation. It is important to note that Federal guidance in this area continues to evolve.

## MANAGEMENT REACTION

The Office of the Chief Information Officer agreed with our recommendations and agreed to take immediate corrective action.

Attachment

cc: Under Secretary for Nuclear Security/Administrator for Nuclear Security

# INTERNET PRIVACY

## TABLE OF CONTENTS


**Overview**

Introduction and Objective.....1

Conclusions and Observations.....1

**Data Collection and Disclosure Concerns**

Details of Finding .....3

Recommendations and Comments.....7

**Appendices**

1. Web Sites Using Persistent Cookies.....9
2. Web Sites with Inadequate or Missing Privacy Notices .....10
3. Scope and Methodology .....12
4. Prior Reports.....14

# OVERVIEW

## INTRODUCTION AND OBJECTIVE

On December 15, 2000, the *Treasury and General Government Appropriations Act of 2001* (Act) was enacted. Section 646 of the Act specifically requires the Inspector General to report on any activity related to the collection of information from individuals accessing Departmental Internet sites. Activities related to internal data collection efforts and agreements with third parties to collect personally identifiable data must be reported to Congress no later than 60 days after enactment.

The Privacy Act and implementing Federal guidance prohibits the involuntary collection or review of personally identifiable information relating to an individual's access to or use of any Internet (web) site of a Federal department or agency. The prohibition on the gathering and monitoring of personal information also applies to Government contractors and other related third parties. With limited exception, the Department is prohibited from collecting information from individuals that access its web sites through the use of techniques that are not disclosed and are not readily apparent to the user. In most instances, Office of Management and Budget (OMB) regulations prohibit the Department from using data collection techniques such as "persistent cookies." Persistent cookies are small files containing unique identifiers that a web server places on a site visitor's computer that can be used to retrieve information about the user. These files remain embedded in a user's hard drive and can facilitate information collection until they expire or are removed. Collection of data using this technique is permitted only when the organization demonstrates a "compelling need" and such use is specifically approved by the Secretary.

The objective of our audit was to determine whether the Department's method of collecting data from users of its publicly accessible web sites was consistent with Federal privacy regulations.

## CONCLUSIONS AND OBSERVATIONS

The Department's method of collecting data from users of its publicly accessible web sites was not always consistent with Federal regulations. Specifically, some web sites were collecting data by unapproved or undisclosed means and a number of web sites did not display conspicuously located, clearly written privacy notices. Departmental and OMB guidance expressly prohibit the collection of data through the use of unapproved or undisclosed methods. These regulations

require that web sites conspicuously post privacy notices containing clear and unambiguous language that explains data collection techniques and the ultimate use of visitor data. Web site privacy control weaknesses occurred in a number of instances because the Department lacked clear and current implementing guidance and did not provide consistent oversight of site development and operation. As a result, the Department cannot ensure that the privacy of its site visitors is properly protected in all instances as required by Federal privacy regulations.

(Signed)
Office of Inspector General

# DATA COLLECTION AND DISCLOSURE CONCERNS

**Persistent Cookies and Inadequate Privacy Notices**

The Department's method of collecting data from users of its publicly accessible web sites was not always consistent with Federal regulations. Some web sites were collecting data from site visitors by unapproved or undisclosed methods while other sites did not adequately advise users of the web site as to the ultimate use of the information collected. Specifically, some Departmental elements had not fully complied with Presidential and OMB guidance restricting the use of persistent cookies. Also, a number of Departmental web sites did not display conspicuously located, or did not provide clearly written web site privacy policies.

Web Sites with Persistent Cookies

Despite prohibitions imposed by Federal and Departmental sources, a number of the Department's publicly accessible web sites were collecting data through an unapproved method. Our review of 93 web sites sponsored by the Department or its contractors disclosed that approximately 12 percent (11) of those sites used persistent cookies to collect information from site visitors. These cookies were written to the web site visitor's hard disk and were potentially capable of collecting data without the user's knowledge for periods ranging from 10 to 37 years. None of the persistent cookies discovered during our review met the OMB requirements for an exception to their use and none had been approved by the Secretary as required. Persistent cookies identified by testing a sample of the Department's web sites are listed in Appendix 1.

Web site managers gave a variety of reasons as to why persistent cookies were being used on their web sites. Some said they were unaware their web site was performing this function. Others indicated they were aware that persistent cookies were being used but not aware that the practice was prohibited. Several others expressed awareness of the requirements but chose to use the data collection method because they believed that there was a valid requirement for the information. One web site manager told us that she knew of the requirement for direct approval from the Secretary, but chose instead to seek approval from the head of her own organization. All sites that acknowledged a specific purpose for using persistent cookies told us that the data collected was used strictly to enhance web site operation and was not sold or provided to others.

Privacy Notices

A number of the Department's publicly accessible web sites did not satisfy Federal and Departmental requirements to provide a clear and unambiguous notice to users as to the extent of data collection and the ultimate use of such data. We noted that about 30 percent, or 28 of the 93 web sites reviewed did not satisfy Federal disclosure requirements. Specifically, privacy notices were either absent, not conspicuously located, or lacked sufficient detail to appraise users of the extent and the ultimate use of the data collected. The lack of such notices may erode public trust in the Government as visitors to the Department's web sites will not know what to expect regarding personal privacy. Appendix 2 details web sites with inadequate privacy notices identified during our review of sampled web pages.

## Federal Web Site Privacy Requirements

The Privacy Act and implementing Federal guidance published by OMB prohibits the involuntary collection or review of personally identifiable information relating to an individual's access to or use of any web site of the Department. The prohibition on gathering personal information also applies to Government contractors and other related third parties. With limited exception, the Department is prohibited from collecting information from individuals that access its web sites through the use of techniques that are not disclosed and are not readily apparent to the user.

Data Collection Methods

In most instances, Federal web sites are prohibited from collecting data from web site visitors using techniques that are not readily apparent to the user. Generally, OMB specifically prohibits the use of data collection techniques through the use of "persistent cookies." Collection of data in this manner is usually transparent to the web site visitor, and as such, is permitted only in limited circumstances. Specifically, collection of data using this technique is permitted only when the organization demonstrates a "compelling need," the method is fully disclosed, and the practice is approved by the Secretary.

Privacy Notices

Presidential and OMB guidance require that Federally-operated or sponsored web sites feature a Privacy Notice that explains what members of the public may expect regarding personal privacy while visiting the site. Such web site privacy notices must be conspicuously posted and flow from page to page within the site. In addition, the notice should contain clear and unambiguous language explaining the extent, method, and ultimate use of personal data collected from web site visitors. OMB M-99-18 contains model language for web site Privacy Notices.

**Factors Affecting the Web Site Privacy Control Structure**

Web site privacy control weaknesses occurred because the Department lacked clear and current implementing guidance and consistent oversight of web site development and operation. Despite the sensitivity of privacy related issues, the Department had not provided clear and current internal implementing guidance for Federal web privacy requirements. Web privacy oversight was performed only on an ad hoc basis and a consistent process for maintaining oversight of web site development and operation had not been developed. In addition, we noted that the Department had not developed specific privacy related performance goals as required by the Government Performance and Results Act of 1993.

Departmental Implementing Guidance

Even though web privacy issues had become the subject of intense Presidential and public attention, the Department did not provide sufficient guidance and did not publish or maintain directives in this area. Web privacy issues first became prominent during May 1998 when the President issued a memorandum directing protection of the privacy of citizens accessing Federal web sites. While Departmental officials indicate that guidance was issued to address the President's concern, they were unable to specify the extent of the guidance and could not furnish us with a copy of such direction. Despite the issuance of memorandums from OMB in January 1999 and June 2000 specifying required web privacy related actions, the Department did not move to publish a memorandum implementing such guidance until July 2000.

The Department had not issued new or modified existing directives to address web privacy related requirements. Departmental officials told us that they elected to rely on guidance issued through memorandums to program elements instead of incorporating Internet privacy requirements in Departmental directives. These same officials acknowledged that directives would have been more effective and that guidance issued through memorandums did not work its way down to the working level in many instances. In addition, the Department has allowed both of its directives addressing privacy issues, DOE Orders 1800.1A and 200.1, to lapse. Officials from the Office of the Chief Information Officer (CIO) acknowledged that the lack of direction in the privacy area was of concern, but that a severe shortage of resources relegated this issue to a low priority level.

Web Site Development and Operation Oversight

The Department does not maintain visibility over web site development and operation and performs privacy related oversight activities only on an ad hoc basis. Officials from the Office of the CIO told us that because of the Department's decentralized information technology management structure, they maintain little information regarding the Department's publicly accessible web sites. They indicated that the Department did not maintain an inventory of web sites and could not provide information on web site sponsorship, content, or operation. The Department also told us that its oversight of privacy related issues for web sites amounted to a single employee, on an ad hoc basis, randomly testing web sites for the presence of persistent cookies. Reviews to assess compliance with restrictions on data use and the sufficiency of privacy notices was not contemplated because of staffing constraints.

Performance Goals

While the Department had developed high level performance goals with respect to information technology management, specific web site privacy related performance goals required by the Government Performance and Results Act of 1993 had not been developed. Privacy-related performance goals contained in the Fiscal Year 2000 plan related solely to reducing the backlog of Freedom of Information request cases. Performance goals related to information technology management also did not contain specific goals related to web site development or privacy issues. Without specific goals, the Department lacks a basis to measure and demonstrate its performance in this highly sensitive area.

**Privacy Is Not Assured**

The Department cannot provide reasonable assurance to visitors of its publicly accessible web sites that their privacy is properly protected as required by Federal regulations. Because of the problems noted, the Department cannot consistently assure members of the public that personally identifiable information is being properly collected or used for authorized purposes. Clearly, the trend is to deliver greater quantities of service via the web and maintaining public trust in the right to security of personally identifiable information is of critical importance as the Government moves into the E-commerce arena.

**RECOMMENDATIONS**

We recommend that the Chief Information Officer take the following actions to enhance Internet privacy in the Department:

1. Require cognizant Program Offices to review all publicly accessible web sites for compliance with Federal privacy requirements and formally report results to the Secretary within 90 days.

2. Require cognizant Program Offices to catalog publicly accessible web sites, to include public field and contractor web sites, and periodically test them for compliance with Federal privacy requirements.

3. Develop and implement formal guidance regarding requirements and responsibilities for web privacy.

4. Develop Internet privacy specific performance measures as required by the Government Performance and Results Act of 1993.

**MANAGEMENT REACTION**

The Office of the Chief Information Officer (OCIO) agrees with the recommendations of this audit. The sampling done by the Inspector General indicates that there continues to be a few web sites that have not come into full compliance with the privacy requirements established by the OMB and communicated to sites by the OCIO. Immediate action will be taken to correct this. It should be noted that the audit contains no indication of malicious or inappropriate use of data resulting from the existence of persistent cookies on the sites identified in the report, and the OCIO does not have any other indicators of misuse of data. All web sites use commercial software products to improve information transactions on the site for the benefit of the user. Many of these products contain cookie features (including persistent cookies) that appear to be commonly used in private sector web sites. In all cases that the OCIO has reviewed, the responsible officials were not aware of the cookie feature and were certainly not using it inappropriately. It should also be noted that Government-wide policy in this area continues to evolve. A significant change occurred in September 2000 with a clarification from OMB that session cookies did not present a privacy concern. Until that point, the use of session cookies violated OMB policy even though session cookies did not present a privacy concern and were in fact often critical to a web site's ability to be useful and timely to any individual accessing the site.

**AUDITOR COMMENTS**

Management's comments are responsive to our recommendations.

# Appendix 1

**WEB SITES USING PERSISTENT COOKIES**

| Web Site | Web Address |
|---|---|
| Environmental Management Site Closure | http://apps.em.doe.gov/closure |
| Bonneville Power Administration | www.bpa.gov |
| Brookhaven National Laboratory | www.bnl.gov/bnl.html |
| Central Internet Database | http://cid.em.doe.gov |
| "My ES&H Page" | http://tis.eh.doe.gov/portal/home.htm |
| Federal Energy Regulatory Commission | www.ferc.fed.us |
| Environmental Management – IPABS | http://ipabs-is.em.doe.gov/ipabs |
| Long Term Stewardship Information Center | http://lts.apps.em.doe.gov |
| Departmental Risk Center | www.riskcenter.doe.gov |
| Environmental Management Scholar Search | http://scholarships.em.doe.gov |
| Waste Isolation Pilot Plant | www.wipp.carlsbad.nm.us/wipp.htm |

Notes:

1. During our audit, we notified web site managers when persistent cookies were observed. Some web sites have since either removed the persistent cookies or changed them to session cookies.

2. The persistent cookies listed above were identified through a review of 93 judgmentally selected Internet sites.

# Appendix 2

**WEB SITES WITH INADEQUATE OR MISSING PRIVACY NOTICES**

| Web Site | Web Address | No Privacy Policy | Insufficient Privacy Policy |
|---|---|---|---|
| Advanced Computing Laboratory | www.acl.lanl.gov | | X |
| Albuquerque Operations Office | www.doeal.gov | | X |
| Argonne National Laboratory | www.anl.gov | | X |
| Brookhaven National Laboratory | www.bnl.gov/bnl.html | | X |
| Chief Financial Officer | www.cfo.doe.gov | | X |
| Defense Programs | www.dp.doe.gov | | |
| Denver Regional Office | www.eren.doe.gov/dro | X | |
| Fermi National Accelerator Laboratory | www.fnal.gov | | X |
| General Counsel | www.gc.doe.gov | | X |
| Idaho Operations Office | www.id.doe.gov | | X |
| Independent Oversight and Performance Assurance | www.tis.doe.gov/iopa | | X |
| INEEL | www.inel.gov | | X |
| Long Term Stewardship Information Center | http://lts.apps.em.doe.gov | | X |
| Kansas City Plant | www.os.kcp.com | | X |
| Lawrence Berkeley Laboratory | www.lbl.gov | | X |
| Lawrence Livermore National Laboratory | www.llnl.gov | | X |
| Los Alamos National Laboratory | www.lanl.gov | X | |
| New Brunswick Laboratory | www.nbl.doe.gov | X | |
| Oak Ridge Institute for Science and Education | www.orau.gov/orise.htm | X | |
| Oak Ridge National Laboratory | www.ornl.gov | X | |
| Oak Ridge Operations | www.oakridge.doe.gov | X | |

**WEB SITES WITH INADEQUATE OR MISSING PRIVACY NOTICES**

| Web Site | Web Address | No Privacy Policy | Insufficient Privacy Policy |
|---|---|---|---|
| | | | |
| Oakland Operations Office | www.oak.doe.gov | X | |
| Pantex Plant | www.pantex.com | X | |
| Princeton Plasma Physics Laboratory | www.pppl.gov | X | |
| Sandia National Laboratory | www.sandia.gov | | X |
| Stanford Linear Accelerator Center | www.slac.stanford.edu | | X |
| Jefferson Laboratory | www.jlab.org | X | |
| Waste Isolation Pilot Plant | www.wipp.carlsbad.nm.us/wipp.htm | | X |
| BWXT Y-12 | www.y12.doe.gov/.index.html | | X |
| Y-12 Security Complex | www.y12.doe.gov/.index.html/y12.html | | X |

Notes:

1. The Internet sites with inadequate privacy notices were identified through a review of 93 judgmentally selected web sites.

# Appendix 3

**SCOPE**

The scope of this audit was limited by a 60-day time constraint imposed by the Act. The audit was performed between December 18, 2000 and February 2, 2001. The audit was conducted at Headquarters and covered a review of the controls in place to ensure that the Department's collection of data associated with its publicly accessible web sites was consistent with Federal and Departmental guidance. The scope of the audit was also constrained by the absence of information relating to the total population of the Department's publicly accessible web sites and web hosting contracts.

**METHODOLOGY**

To satisfy the audit objective, we:

- Reviewed Federal and Departmental regulations, guidance, and correspondence for ensuring web site privacy;
- Reviewed Departmental strategic plans and performance goals for compliance with the Government Performance and Results Act of 1993;
- Tested a judgmental sample of Departmental web sites and analyzed the use of cookies and the placement and content of privacy policy notices;
- Interviewed cognizant officials in the Office of CIO and other Department personnel responsible for web sites and privacy issues;
- Interviewed Departmental personnel to determine whether there were any formal complaints or "Hotline" calls related to web site privacy; and,
- Reviewed third party web hosting contracts to determine whether they adequately addressed privacy issues.

The audit was performed to satisfy the requirements of Section 646 of the *Treasury and General Government Appropriations Act of 2001* (P.L. 106-554). The audit was conducted in accordance with generally accepted Government auditing standards for performance audits and included tests of internal controls and compliance with laws and regulations to the extent necessary to satisfy the audit objective. We did not rely on computer processed data to accomplish our audit objective. Because our audit was limited, it would not

necessarily have disclosed all internal control deficiencies that may have existed. Due to time constraints imposed by the Act, a formal exit conference was not held with management officials. Management was, however, given an opportunity to review the report in draft form and offer comments.

## PRIOR REPORTS
## BY THE U. S. GENERAL ACCOUNTING OFFICE

- *Internet Privacy: Agencies' Efforts to Implement OMB's Privacy Policy,* GGD-00-191. Although progress has been made at Federal web sites, privacy policies were not as yet sufficiently or adequately posted. OMB guidance found in M-99-18 is unclear regarding cookies as well as other terms. The Report also suggested insufficient oversight as a cause of the problem.

- *Internet Privacy: Comparison of Federal Agency Practices with FTC's Fair Information Principles,* AIMD-00-296R. This Report was generated from a Senate request. It compared Federal practices regarding privacy with guidelines set by FTC. OMB had serious problems accepting this comparison, as FTC guidelines are for the commercial market, not the public sector.

- *Internet Privacy: Federal Agency Use of Cookies,* GAO-01-147R. GAO reviewed 65 Federal web sites and found undisclosed persistent cookies at 9 of them. One of those was a Department web site at Ames Laboratory.

IG Report No. : DOE/IG-0493

## CUSTOMER RESPONSE FORM

The Office of Inspector General has a continuing interest in improving the usefulness of its products. We wish to make our reports as responsive as possible to our customers' requirements, and, therefore, ask that you consider sharing your thoughts with us. On the back of this form, you may suggest improvements to enhance the effectiveness of future reports. Please include answers to the following questions if they are applicable to you:

1. What additional background information about the selection, scheduling, scope, or procedures of the audit would have been helpful to the reader in understanding this report?

2. What additional information related to findings and recommendations could have been included in this report to assist management in implementing corrective actions?

3. What format, stylistic, or organizational changes might have made this report's overall message more clear to the reader?

4. What additional actions could the Office of Inspector General have taken on the issues discussed in this report which would have been helpful?

Please include your name and telephone number so that we may contact you should we have any questions about your comments.

Name _____ Date _____

Telephone _____ Organization _____

When you have completed this form, you may telefax it to the Office of Inspector General at (202) 586-0948, or you may mail it to:

Office of Inspector General (IG-1)
Department of Energy
Washington, DC 20585

ATTN: Customer Relations

If you wish to discuss this report or your comments with a staff member of the Office of Inspector General, please contact Wilma Slaughter at (202) 586-1924.

The Office of Inspector General wants to make the distribution of its reports as customer friendly and cost effective as possible. Therefore, this report will be available electronically through the Internet at the following alternative address:

U. S. Department of Energy Office of Inspector General Home Page
http://www.ig.doe.gov

Your comments would be appreciated and can be provided on the Customer Response Form attached to the report.