Memorandum

Date APR 16 2001

From Michael F. Mangano
Acting Inspector General

Subject Monitoring of Personally Identifiable Information on Users of Departmental Internet Sites (A-01-01-03000)

To Dennis P. Williams
Acting Assistant Secretary
for Management and Budget

Attached are two copies of our final report detailing the results of our review of the Department's monitoring of personally identifiable information on users of its web sites. This review was required by December 21, 2000, legislation prohibiting such monitoring. In accordance with the legislation, we are providing copies of our report to the House and Senate Committees on Appropriations.

We would appreciate your views and the status of any further action taken or contemplated on our recommendations within the next 60 days. If you have any questions, please contact me or have your staff contact Joseph E. Vengrin, Assistant Inspector General for Audit Operations and Financial Statement Activities, at (202) 619-1157.

To facilitate identification, please refer to Common Identification Number A-01-01-03000 in all correspondence relating to this report.

Attachment

Department of Health and Human Services

OFFICE OF INSPECTOR GENERAL

MONITORING OF PERSONALLY IDENTIFIABLE INFORMATION ON USERS OF DEPARTMENTAL INTERNET SITES

APRIL 2001
A-01-01-03000

Memorandum

Date APR 16 2001

From Michael F. Mangano
Acting Inspector General

Subject Monitoring of Personally Identifiable Information on Users of Departmental Internet Sites (A-01-01-03000)

To Dennis P. Williams
Acting Assistant Secretary
for Management and Budget

This final report provides the results of our review of the monitoring of personally identifiable information on users of Department of Health and Human Services (HHS) web sites. This review was required by December 21, 2000, legislation prohibiting such monitoring.

The objective of our review was to determine whether HHS operating divisions, or their third-party contractors, collected, reviewed, or created any aggregate list that included personally identifiable information relating to an individual's access to or use of their Internet sites. We also determined whether the HHS web sites designed for children were in compliance with the Children's Online Privacy Protection Act of 1998.

We found that four operating divisions collected personally identifiable information on individuals who browsed six of their respective web sites. This was accomplished by transmitting information commonly referred to as a persistent "cookie" to an individual's computer when the individual visited the web site. Contrary to departmental policy, the web sites in question had not obtained the Secretary's prior approval for using the cookies and did not warn the user that these techniques were in use. We also found that 21 of the Department's web sites designed for children did not contain a privacy statement or a link to a privacy statement as required by the Children's Online Privacy Protection Act.

We recommend that you amend current departmental policy to require frequent review of web sites to detect the use of persistent cookies. We also recommend that you direct the Chief Information Officers (CIO) of the operating divisions to (1) ensure that the persistent cookies we detected are immediately disabled, (2) ensure that web sites do not use persistent cookies without the proper waiver from the Secretary, (3) ensure that the web sites designed for children are in compliance with the Children's Online Privacy Protection Act of 1998, and (4) require all web site originators to certify to their respective CIOs that they are in compliance with applicable laws.

In response to our draft report, the Department generally concurred with our findings. With respect to our recommendations, the Department agreed to change existing policy

and has taken steps to correct instances of noncompliance. The Department pointed out that due to the numerous web sites, web site originators should certify to their respective CIOs as to compliance with applicable laws. We concur with this suggestion and have made the appropriate change to our recommendations.

BACKGROUND

Information on visitors to a web site can be collected by using "cookies." A cookie is a short string of text (not a program) that is sent from a web server to a web browser when the browser accesses a web page. The use of cookies allows the server to recognize returning users, track on-line purchases, or maintain and serve customized web pages. Domain cookies are those placed on a visitor's computer by the visited web site. Third-party cookies are those placed on a visitor's computer by a domain other than the site being visited.

Both domain and third-party cookies may be categorized as either session cookies or persistent cookies. Session cookies are used only during the browsing session and expire when the user quits the browser. Session cookies, which do not produce personal information on the user, are generally used for statistical purposes or to help make web sites more useful to visitors. Persistent cookies, on the other hand, specify expiration dates, remain stored on the clients' computers until the expiration dates, and can be used to track users' browsing behavior by identifying their Internet addresses whenever they return to a site. Webmasters can easily obtain information about users' browser types, last pages visited, and more depending on the users' software and the program being executed. Cookies are the preferred method of accruing data because the information persists from session to session and allows the web server to recognize a user as having previously visited from the same computer.

Legislation enacted December 21, 2000,[1] prohibits Federal agency monitoring of personal information on an individual's use of the Internet. Agencies may not:

- collect, review, or create any aggregate list that includes personally identifiable information relating to an individual's access to or use of any Federal Government Internet site or

- enter into any agreement with a third party (including another Government agency) to collect, review, or obtain any aggregate list that includes personally identifiable information relating to an individual's access to or use of any governmental or nongovernmental Internet site.

---

[1] Section 501 of Public Law 106-346, Department of Transportation and Related Agencies Appropriations Act, 2001, as amended by Public Law 106-554, enacted December 21, 2000, Appendix C, section 644 of H.R. 5658.

Exceptions include the voluntary submission of personally identifiable information and monitoring for law enforcement, regulatory, or supervisory purposes, as well as for certain system security purposes.

The legislation requires Inspectors General to report to the Congress, no later than 60 days after the date of enactment, on their respective agencies' compliance activities.[2]

On January 8, 2001, the Department's Office of Information Resource Management (IRM) issued policies that prohibit the use of persistent cookies on HHS web sites, including those operated by contractors, unless:

- the site gives clear and conspicuous notice that persistent cookies are in use;
- there is a compelling need to gather the data on the site;
- appropriate and publicly disclosed privacy safeguards exist for handling any information derived from the cookies; and
- the HHS Secretary gives personal, prior approval for their use.

Under the Children's Online Privacy Protection Act of 1998, a web site with a separate area designed for children must post a privacy notice on its home page and a link to that notice at each children's site. The link to the privacy notice must be clear and prominent. A link in small print at the bottom of the page, or one that is indistinguishable from other links on the web site, is not considered clear and prominent.

OBJECTIVE, SCOPE, AND METHODOLOGY

The objective of this review was to determine whether HHS operating divisions, or their third-party contractors, collected, reviewed, or created any aggregate list that included personally identifiable information relating to an individual's access to or use of their Internet sites. We also determined whether the HHS web sites designed for children were in compliance with the Children's Online Privacy Protection Act of 1998.

To accomplish our objective, we:

- reviewed applicable laws and regulations;
- browsed a judgmental sample of 81 of the Department's web sites available to the public through its home page, including links within those 81 sites encompassing thousands of web pages (see appendix II for a list of the sites visited);

---

[2] Public Law 106-554, Consolidated Appropriations Act, 2001, Appendix C, section 646 of H.R. 5658.

- determined whether the sites transmitted persistent cookies to our personal computers;

- interviewed personnel at the Health Care Financing Administration to confirm their policies and procedures regarding Internet privacy;

- requested that the Department address what steps it has taken or is contemplating to ensure that all HHS web sites and links do not (1) transmit persistent cookies to an individual's personal computer or (2) capture personal information in text files or other database formats without the individual's knowledge or consent; and

- reviewed sites for appropriate privacy statements or links to privacy statements.

We did not examine individual web servers to determine if personally identifiable information was captured and retained without the use of cookies.

We conducted our review in accordance with generally accepted government auditing standards. The review was conducted at the Office of Inspector General's Regional Office of Audit Services in Boston, Massachusetts, during January and February 2001.

FINDINGS

In its February 9, 2001, response to our request for information, the Department indicated that it had provided each operating division with recently issued IRM policies governing the use of persistent cookies. However, these policies were not always followed. We found that 4 of the 12 operating and staff divisions that we reviewed used persistent cookies to collect personally identifiable information on individuals who browsed 6 of their respective web sites. The cookies were used without the appropriate waivers from the Secretary and the user notifications required by the Department's policies. These web sites are shown below:

Operating Division	Web Site
Agency for Healthcare Research and Quality	http://www.guideline.gov
Health Resources and Services Administration	http://organdonor.gov
Indian Health Service	http://www.ihs.gov
Indian Health Service	http://my.ihs.gov
National Institutes of Health	http://hsroad.gov
National Institutes of Health	http://www.nih.gov

The Agency for Healthcare Research and Quality noted that it had applied for a waiver from the Secretary. At the time of our review, however, the waiver had not been approved, and visitors to the site were not notified that persistent cookies were being transmitted. In addition, the Centers for Disease Control and Prevention and the Office of the Secretary informed us that they had obtained waivers from the Secretary to use persistent cookies on certain of their web sites.[3] Appendix I lists the operating and staff divisions reviewed and the number of web sites that used persistent cookies.

Of the 81 web sites we visited, 56 (including the 6 that used persistent cookies without proper waivers) contained either the Department's standard privacy policy notice or a direct link to the notice. This notice, dated July 30, 1999, states that:

> "We collect no information about you, other than information automatically collected and stored (see below), when you visit our web site unless you choose to provide that information to us.
>
> "Information Automatically Collected and Stored:
>
> > "When you browse through any web site, certain personal information about you can be collected. We automatically collect and **temporarily** [emphasis added] store the following information about your visit:
> > - the name of the domain you use to access the Internet (for example, aol.com, if you are using an America Online account, or stanford.edu, if you are connecting from Stanford University's domain);
> > - the date and time of your visit;
> > - the pages you visited; and
> > - the address of the web site you came from when you came to visit."

We also reviewed 23 web sites designed for children to determine whether they were in compliance with the privacy statement requirements of the Children's Online Privacy Protection Act. The Department's home page has a "For Kids" link to the operating divisions' web sites for children and a "Kid's Privacy Notice." This notice, http://www.hhs.gov/kids/ privacy.html, is clear and prominently placed. We determined, however, that 21 of the web sites for children either did not contain a link to the privacy notice or had a link that was neither clear nor prominent.

---

[3] The Centers for Disease Control and Prevention received waivers to use persistent cookies on four web sites and the Office of the Secretary, on one web site.

RECOMMENDATIONS

We recommend that you amend current IRM policy to require frequent review of web sites to detect the use of persistent cookies. We also recommend that you direct the CIOs of the operating divisions to:

(1) ensure that the persistent cookies we detected on the Department's web sites are immediately disabled,

(2) ensure that web sites do not use persistent cookies without the proper waiver from the Secretary,

(3) ensure that the web sites designed for children are in compliance with the Children's Online Privacy Protection Act of 1998, and

(4) require all web site originators to certify to their respective CIOs that they are in compliance with applicable laws.

DEPARTMENT'S RESPONSE

The Department agreed that periodic reviews of web sites were appropriate and planned to modify current policy to reflect reviews on a quarterly basis. The Department has already taken steps to ensure that the CIOs responsible for the noncompliant sites we identified either apply for the appropriate waiver or modify the web sites to bring them into compliance. Finally, the Department pointed out that due to the over 8 million active web pages on the Department's Internet, web site originators should certify to their respective CIOs that they have complied with applicable laws. We concur with this suggestion and have revised the recommendations accordingly. Appendix III contains the full text of the Department's comments.

OPERATING AND STAFF DIVISIONS REVIEWED

Operating/Staff Division	Number of Web Sites	
	Persistent Cookies Found Without Waivers	Waivers Granted for Persistent Cookies
Administration on Aging	-	-
Administration for Children and Families	-	-
Agency for Healthcare Research and Quality[1]	1	-
Centers for Disease Control and Prevention	-	4
Food and Drug Administration	-	-
Health Care Financing Administration[2]	-	-
Health Resources and Services Administration	1	-
Indian Health Service	2	-
National Institutes of Health[2]	2	-
Office of the Secretary	-	1
Program Support Center	-	-
Substance Abuse and Mental Health Services Administration	-	-

[1] Applied for waiver from the Secretary.

[2] Some web sites maintained by a third-party contractor.

WEB SITES REVIEWED

http://aspe.hhs.gov
http://aspe.os.dhhs.gov
http://cancernet.nci.nih.gov/occdocs/kidsHome.html
http://directory.psc.gov
http://grants.nih.gov
http://hsroad.gov
http://learning.hhs.gov
https://my.ihs.gov
http://ndms.dhhs.gov
http://odphp.osophs.dhhs.gov
http://ohrp.osophs.dhhs.gov/
http://oig.hhs.gov
http://organdonor.gov
http://ori.dhhs.gov
http://raceandhealth.hhs.gov
http://salud.nih.gov
http://science-education.nih.gov/newsnapshots/index.html
https://sdn.cdc.gov
http://search.nih.gov
http://smokefree.gov
http://telehealth.hrsa.gov
http://www.4woman.gov/
http://www.acf.dhhs.gov
http://www.afterschool.gov
http://www.ahrq.gov
http://www.aoa.gov
http://www.atsdr.cdc.gov
http://www.atsdr.cdc.gov/child/
http://www.bhpr.hrsa.gov
http://www.bphc.hrsa.gov
http://www.cdc.gov/nceh/kids/99kidsday/default.htm
http://www.cdc.gov/tobacco/sgr/sgr4kids/sgrmenu.htm
http://www.cdc.gov/global/
http://www.cdc.gov
http://www.cdc.gov/nceh/cddh/kids/kdhpage.htm
http://www.cdc.gov/ncipc/bike/kids.htm
http://www.cdc.gov/niosh/adoldoc.html
http://www.childstats.gov
http://www.consumer.gov
http://www.DrugAbuseStatistics.samhsa.gov
http://www.fda.gov/oc/opacom/kids/default.htm
http://www.fda.gov
http://www.fedstats.gov
http://www.fedworld.gov
http://www.firstgov.gov
http://www.foodsafety.gov/~dms/cbook.html
http://www.guideline.gov
http://www.hab.hrsa.gov
http://www.hcfa.gov
http://www.health.org/features/kidsarea/index.htm
http://www.health.org.gov/gpower
http://www.healthfinder.gov
http://www.hhs.gov/kids/morekids.html
http://www.hhs.gov/kids/
http://www.hhs.gov/families/kids.htm
http://www.hhs.gov
http://www.hrsa.gov
http://www.ihs.gov/publicinfo/publications/mcgruff/index.asp
http://www.ihs.gov
http://www.info.gov
http://www.insurekidsnow.gov
http://www.mchb.hrsa.gov
http://www.medicare.gov
http://www.mentalhealth.org
http://www.ncvhs.hhs.gov
http://www.nida.nih.gov/GoestoSchool/NIDAg2s.html
http://www.nidr.nih.gov/news/pubs/snaksmrt/main.htm
http://www.niehs.nih.gov/reform/puzzles.htm
http://www.niehs.nih.gov/external/a2z/home.htm
http://www.niehs.nih.gov/kids/
http://www.nih.gov
http://www.omhrc.gov/
http://www.psc.dhhs.gov
http://www.psc.gov
http://www.ruralhealth.hrsa.gov
http://www.samhsa.gov
http://www.surgeongeneral.gov
http://www2.cdc.gov/nchstp_od
http://www2.cdc.gov/wfrs
http://www2.ihs.gov/heritage
http://www4.od.nih.gov/

DEPARTMENT OF HEALTH & HUMAN SERVICES

Office of the Secretary

Washington, D.C. 20201

RECEIVED
2001 MAR 15 AM 10:47
OFFICE OF INSPECTOR GENERAL

MAR 14 2001

MEMORANDUM TO : Michael F. Mangano
Acting Inspector General

FROM : Dennis P. Williams
Acting Assistant Secretary
for Management and Budget

SUBJECT: Comment on Draft Report on Monitoring of Persistent Cookies (A-01-01-03000)

IG
EAIG
PDIG
DIG-AS ✓
DIG-EI
DIG-OI
DIG-MP
OCIG
ExecSec
Date Sent 3/15/01

Thank you for the opportunity to review and comment on your draft report of findings on the Monitoring of Personally Identifiable Information on Users of Departmental Internet Sites dated March, 2001.

We generally concur with your statement of the problem, background, objective, scope, methodology, and findings as contained in your report. We offer the following comments on the recommendations:

We agree that periodic review of the Department's Internet Websites and pages to test for compliance with existing law is appropriate. We believe that the CIOs of the Staff and Operating Divisions should perform and certify that they have done so to the Office of Information Resources Management on a quarterly basis, and will modify our current policy to so state.

When we make this change, we shall use the opportunity presented by its announcement to remind the Department's CIOs of their obligation to comply with the legal requirements regarding both persistent cookies and Websites designed for children. Rather than waiting for your final report to be issued, we further will pass along the specific instances of non-compliance that you have identified to the affected CIOs in the next few days and ask that they either request a waiver as may be appropriate or modify them to bring them into compliance.

It is pertinent to note that, at last count, the Department had over eight million active Webpages on the Internet. Policing so many existing items for compliance is therefore a very large and problematic undertaking, to be done as effectively as possible, but of necessity, in a gradual manner that may not accommodate an immediate review of each active page. Instead we suggest you recommend the originator of the Webpage to certify to the respective CIO that they have complied. The CIO can perform the review and the IG can audit these requests for validation of compliance.

Thank you for your assistance in our efforts to manage the Department's compliance with these requirements.

If you have any questions, please contact Mr. Bill Sykes of my staff at 202-690-6713.