

---

**GAO**

**United States General Accounting Office**

To the Honorable Joseph I. Lieberman  
Ranking Minority Member  
Committee on Governmental Affairs  
U.S. Senate

---

September 2000

# INTERNET PRIVACY

## Agencies' Efforts to Implement OMB's Privacy Policy



---

---



**G A O**

Accountability \* Integrity \* Reliability

**United States General Accounting Office  
Washington, D.C. 20548**

**General Government Division**

B-284494

September 5, 2000

The Honorable Joseph I. Lieberman  
Ranking Minority Member  
Committee on Governmental Affairs  
United States Senate

Dear Senator Lieberman:

New information technologies offer many possibilities for the government to improve the quality and efficiency of its service to the American people. The Internet and Web sites are powerful tools for conveying information on topics relating to federal activities, objectives, policies, and programs. Web sites provide a simple and quick way for accessing information about the government and what it is doing on the people's behalf. However, the government cannot realize the full potential of the Internet until people are confident that the government will protect their privacy when they visit its Web sites. To ensure that individuals have notice about how their personal information is handled when they visit federal Web sites, in June 1999, the Office of Management and Budget (OMB) issued a memorandum (M-99-18) requiring federal agencies to post privacy policies on their Internet Web sites and provided guidance for doing so.

The OMB memorandum requires agencies to post privacy policies to their department or agency principal Web sites and to any other known, major entry points to their Web sites as well as any Web page where they collect substantial personal information from the public. The memorandum also requires agencies to post privacy policies that (1) clearly and concisely inform visitors to the Web sites what information the agency collects about individuals, why the agency collects it, and how the agency will use it; and (2) are clearly labeled and easily accessed when someone visits a Web site. Although the Privacy Act of 1974,<sup>1</sup> as amended, is the primary law regulating the federal government's collection and maintenance of personal information, the Privacy Act protects personal information maintained only in an agency's system of records.<sup>2</sup>

---

<sup>1</sup> Public Law No. 93-579, 5 U.S.C. § 552a.

<sup>2</sup> The Privacy Act defines a system of records as any group of records under the control of an agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual.

---

This report responds to your request for information on whether agencies were adhering to the OMB guidance. Specifically, you asked us to:

1. determine if agencies have clearly labeled and easily accessed privacy policies posted on their principal Web sites;
2. determine if agencies' privacy policies posted on their principal Web sites inform visitors about what information an agency collects, why the agency collects it, and how the agency will use the information;
3. determine how selected agencies have interpreted the requirement to post privacy policies at major entry points; and
4. determine if selected agencies have posted privacy policies on Web pages where the agency collects substantial personal information or, when applicable, notices that refer to the Privacy Act of 1974.

In addition, as agreed, we compared OMB's memorandum and its related guidance with selected statutory requirements that are generally applicable to federal agencies and with fair information principles as recently summarized by the Federal Trade Commission (FTC).<sup>3</sup> See appendix IV for additional information on the Privacy Act and implementing guidance and appendix V for more information on fair information principles.

---

## Scope and Methodology

To do our work for the first and second objectives, we reviewed the principal Web sites of 70 federal executive agencies—14 departments, 55 independent agencies, and the Executive Office of the President—on April 14, 2000, to determine if agencies had posted “clearly labeled and easily accessed” privacy policies (see app. II for a list of the 70 agencies). To determine if agency privacy policies addressed what information an agency Web site collects, why the agency collects it, and how the agency will use it, we answered those questions for two information practices addressed in OMB's guidance—information agencies collect and store automatically and information agencies collect when visitors to agency Web sites provide information voluntarily through e-mails and on-line forms. We did not verify whether agencies accurately portrayed this information or assess whether agencies complied with their posted policies. To do our work for the third objective, we selected six agencies to

---

<sup>3</sup> In its report to Congress, [Privacy Online: Fair Information Practices in the Electronic Marketplace](#), May 2000, FTC discussed fair information practices that are widely accepted principles of privacy protection. FTC summarized these practices into four principles: notice, choice, access, and security.

---

contact to discuss their interpretation of the requirement to post privacy policies at major entry points.<sup>4</sup> To do our work for the fourth objective, we reviewed the 31 high-impact agencies identified by the National Partnership for Reinventing Government (NPR), hereafter referred to as high-impact agencies, to determine if they had privacy policies posted on pages where personal information was collected.<sup>5</sup> We also contacted officials of nine high-impact agencies to discuss whether they should have posted privacy policies and, when applicable, Privacy Act notices on Web pages that we identified as collecting personal information.<sup>6</sup> In addition, we compared the OMB memorandum with applicable laws and implementing guidance and with the fair information principles as summarized by FTC in its May 2000 report.

We conducted our work from January through August 2000 in accordance with generally accepted government auditing standards. See appendix I for a more detailed discussion of our objectives, scope, and methodology. We requested comments on a draft of this report from the Director of OMB and on excerpts of a draft of this report from the six agencies where we performed additional work. OMB's comments are addressed at the end of this letter and reproduced in appendix VI. The six agencies also provided technical comments, which we incorporated into the report where applicable.

---

## Results in Brief

Of the 70 agencies' principal Web sites that we reviewed on April 14, 2000, 69 had privacy policies posted on their principal Web sites, and 1 did not. In addition, of the 69 agency Web sites, 2 had privacy policies that we determined were not clearly labeled and easily accessed. Thus, 67 of the 70 agency principal Web sites we reviewed had privacy policies that were

---

<sup>4</sup> We selected these agencies—Departments of Commerce, Defense, the Interior, and Justice and the Small Business Administration (SBA) and Social Security Administration (SSA)—because they had a large number of Web sites or frequent contact with the public.

<sup>5</sup> NPR identified 32 agencies as having high impact, that is—they have 90 percent of the federal government's contact with the public. The 32 high-impact agencies consist of components of departments, independent agencies, and 1 initiative—Acquisition Reform—that cuts across all services. Two of the high-impact agencies—the Veterans Health Administration and the Veterans Benefits Administration—are under the Department of Veterans Affairs. In doing our work, we did not distinguish between these agencies when we searched for pages that collected personal information. We searched the Department's Veterans Benefits and Services Web site ([www.va.gov/vbs/index.htm](http://www.va.gov/vbs/index.htm)) because both agencies linked to this site. Therefore, in this report, we counted these agencies as 1, that is—the Department of Veterans Affairs—and discuss only 31 high-impact agencies. (See app. III for a list of the high-impact agencies).

<sup>6</sup> We selected these nine high-impact agencies because they were the two independent agencies from objective three—SBA and SSA— and components of the four departments we selected for objective three that were identified as high-impact agencies by NPR— Bureau of the Census, Patent and Trademark Office, International Trade Administration, Acquisition Reform, Bureau of Land Management, National Park Service, and the Immigration and Naturalization Service.

---

clearly labeled and easily accessed. This appears to be considerable progress from a 1999 survey of selected federal home pages by a public interest group.<sup>7</sup>

Of the 70 agencies' principal Web sites we reviewed, 63 had privacy policies that addressed the automatic collection of information, and 46 of those agencies generally followed all 3 elements of the OMB memorandum's requirement for the agencies to disclose in their privacy policies what information they were automatically collecting, why they were collecting it, and how they planned to use it. Although the OMB guidance does not make clear that agencies should address whether or not they are using security and intrusion detection measures to collect information on visitors to their Web sites, of the 70 agencies, about half addressed this issue in their privacy policies. Of the 70 agencies, 67 had privacy policies that disclosed whether or not they collected information that visitors voluntarily provided, and 57 of these agencies explained how and why they would use that information.

Although OMB requires agencies to post privacy policies at major entry points to their Web sites, the privacy policy guidance does not define major entry point. However, using a sample of six agencies that had a large number of Web sites or frequent contact with the public—the Departments of Commerce, Defense, the Interior, and Justice and SBA and SSA—we found that these agencies generally used similar criteria to determine the major entry points to their Web sites. Generally, the selected agencies designated the home pages of their components as well as Web pages that receive a high number of visits. Of the 6 selected agencies that identified nearly 2,700 Web pages as major entry points, we found only 9 Web pages that did not have posted privacy policies.

The OMB memorandum requires agencies to post privacy policies on pages where they collect "substantial" personal information, but the guidance does not define substantial personal information. Therefore, to assess OMB's requirement, we developed our own criteria defining personal information and reviewed the Web sites of the 31 high-impact agencies for Web pages that collected any personal information. We defined personal information to include an individual's name, e-mail address, postal address, telephone number, Social Security number, or

---

<sup>7</sup> See [Policy vs. Practice: A Progress Report on Federal Government Privacy Notices on the World Wide Web](#), The Center for Democracy and Technology, April 1999. The results of the survey indicated that just over one-third of 46 federal agencies had privacy policies linked from their home pages, 8 agencies had privacy policies that were not on their home pages, and 22 agencies did not have privacy policies.

---

credit card number. Most high-impact agencies did not post privacy policies on all pages that we identified as collecting personal information. Of the 101 on-line forms that we identified as collecting personal information, 44 did not have privacy policies posted. Using a judgmentally selected sample of the high-impact agencies, we asked officials of nine of the high-impact agencies if privacy policies and Privacy Act notices should have been posted to pages that we identified as collecting personal information. For eight forms, officials from four of the high-impact agencies said that the forms we identified should have had privacy policies posted. In addition, officials of three high-impact agencies said that four forms should have had Privacy Act notices posted. The officials generally said that it was an oversight that the policies and notices had not been posted and that they would take corrective action.

In comparing the OMB memorandum and guidance to the Privacy Act and fair information principles, the OMB memorandum is narrower in scope than the Privacy Act and the fair information principles, and the act and principles also differ in some respect. According to OMB officials, the memorandum and guidance primarily address the fair information principle of notice. The Privacy Act, which applies to federal Web sites that maintain information in a system of records that is retrieved by a personal identifier, addresses the four fair information principles, although somewhat differently from how FTC summarizes the principles. For instance, although the Privacy Act gives individuals some choice about how their personal information is used by federal agencies, it also contains exceptions that limit the choice that an individual can exercise over agencies' use of personal information.

We are making recommendations to the Director of OMB, including that the Director consider, in consultation with other parties, such as agencies and the Chief Information Officers (CIO) Council,<sup>8</sup> how best to make certain modifications to the OMB privacy policy that would better ensure that individuals are provided clear and adequate notice about how their personal information is treated when they visit federal Web sites. We also recommend that the Director, working with others as appropriate, determine whether current oversight strategies are adequate to ensure agencies' adherence to Web site privacy policies and whether the policies will need further revision as Web practices continue to evolve.

---

<sup>8</sup> The CIO Council is the lead interagency forum for improving practices in the design, modernization, use, sharing, and performance of federal agency information resources. The CIO Council consists of CIOs and Deputy CIOs from selected federal agencies and liaisons of other executive councils; committees; and boards, including the Chair of the Information Technology Resources Board.

---

## Background

Federal agencies are required by law to protect an individual's right to privacy when they collect personal information. The Privacy Act of 1974, as amended—which is the primary law regulating the federal government's collection and maintenance of personal information—requires protection for personal information maintained in a federal agency's system of records.<sup>9</sup> In addition, OMB Circular A-130, Appendix I, provides guidance to agencies for implementing the Privacy Act.<sup>10</sup> Other laws, such as the Freedom of Information Act (FOIA),<sup>11</sup> the Computer Security Act,<sup>12</sup> and the Paperwork Reduction Act of 1995,<sup>13</sup> support agency compliance with the Privacy Act. Appendix IV provides more information on each of these laws.

According to the Paperwork Reduction Act, the Director of OMB is to provide overall leadership and coordination of federal information resources management within the executive branch. The Director is to issue policies, procedures, and guidelines to assist agencies in achieving integrated, effective, and efficient information resources management. In addition, OMB is to review agencies' policies, practices, and programs pertaining to security, protection, sharing, and disclosure of information in order to ensure compliance, with respect to privacy and security, with the Privacy Act, the Freedom of Information Act, the Computer Security Act, and related statutes.

In addition to statutory protections to protect an individual's right to privacy, a code of fair information practices exists. The fair information principles were first outlined in July 1973 in a report by a Department of Health, Education and Welfare advisory committee.<sup>14</sup> The report recommended the enactment of legislation establishing a code of fair information practices for all automated personal data systems and set out basic principles to safeguard requirements for automated personal data systems. This code predated the Privacy Act of 1974 by over a year and influenced the enactment of the Privacy Act. Most recently, in May 2000, when it conducted a survey of commercial Web sites, FTC summarized

---

<sup>9</sup> See footnote 1.

<sup>10</sup> See OMB Circular A-130, Appendix I, Federal Agency Responsibilities for Maintaining Records About Individuals.

<sup>11</sup> Public Law No. 89-487, 5 U.S.C. § 552.

<sup>12</sup> Public Law No. 100-235; 2 U.S.C. § 271 note, 272, 278g-3, 278g-4, 278h; 40 U.S.C. § 1441.

<sup>13</sup> Public Law No. 104-13, 44 U.S.C. § 35001 *et. seq.*, as amended by the Clinger-Cohen Act of 1996.

<sup>14</sup> See Records, Computers, and the Rights of Citizens, report of the Advisory Committee on Automated Personal Data Systems.



---

these practices into four core principles of privacy protection: notice, choice, access, and security. Some private sector organizations also have used these principles voluntarily as a means of protecting personal information they have collected.

In August 1997, a survey of federal Web sites showed, among other results, that only 11 of 31 federal agencies collecting personal information indicated to users how that information would be used.<sup>15</sup> In April 1999, another survey reported that just over one-third of 46 federal agencies had privacy policies linked from their home pages, 8 agencies had privacy policies that were not on their home pages, and 22 agencies did not have privacy policies.<sup>16</sup>

On June 2, 1999, OMB issued Memorandum M-99-18 directing executive departments and agencies to post clear privacy policies on their Web sites.<sup>17</sup> OMB developed its memorandum and guidance with input from agencies and the CIO Council. The OMB memorandum states that “federal agencies must protect an individual’s right to privacy when they collect personal information, which is required by the Privacy Act and OMB Circular No. A-130.” OMB’s memorandum contains four requirements that agencies are to follow concerning their on-line privacy policies. To follow the memorandum, agencies must post

- privacy policies to their department or agency principal Web site by September 1, 1999;
- privacy policies to any other known, major entry points to their Web sites by December 1, 1999, as well as any Web page where they collect substantial personal information from the public;
- policies that clearly and concisely inform visitors to the Web sites what information the agency collects about individuals, why the agency collects it, and how the agency will use it; and

---

<sup>15</sup> A Delicate Balance: The Privacy and Access Practices of Federal Government World Wide Web Sites, OMB Watch, August 1997.

<sup>16</sup> Policy vs. Practice: A Progress Report on Federal Government Privacy Notices on the World Wide Web, The Center for Democracy and Technology, April 1999.

<sup>17</sup> A Web site is a collection of files that covers a particular theme or subject and is managed by a particular person or organization. These files are called Web pages and are usually based on hypertext markup language (HTML) that may contain such elements as text, graphics, online audio, or video. A Web site can be entered from any number of Web pages or from a hyperlink. A hyperlink is a predefined link from one location to another. The link can jump within a particular location, to another location with the same computer or network site, or even to a location at a completely different physical site. Hyperlinks are commonly used on the Internet to provide navigation, reference, and depth where published text cannot. A hyperlink can be created from text, which typically appears as blue underlined text within an HTML page, or from a graphic.

- policies that are clearly labeled and easily accessed when someone visits a Web site.

Attached to the memorandum is guidance that contains five sections on the following situations: introductory language; information collected and stored automatically; information collected from e-mails and Web forms; security, intrusion, and detection language; and significant actions where information enters a system of records.<sup>18</sup> Each section but the last provides examples of model privacy language to assist agencies in drafting their privacy policies.

On December 17, 1999, the President issued a memorandum to heads of executive departments and agencies on the subject of electronic government. That memorandum discusses that as public awareness and Internet usage increase, the demand for on-line government interaction and simplified, standardized ways to access government information and services becomes increasingly important. That memorandum further recognizes that at the same time, the public must have confidence that their on-line communications with the government are secure and their privacy protected. That memorandum directs agencies to make available on-line by December 2000 the forms needed for the top 500 government services used by the public, and to make transactions with the federal government available for on-line processing of services by October 2003.

## Most Agencies Have Privacy Policies Posted on Their Principal Web Sites

The overwhelming majority of federal Web sites we reviewed, that is 69 of 70, followed the OMB requirement to post privacy policies on their principal Web sites. This appears to be considerable progress from a 1999 survey of selected federal home pages that reported that just over one-third of 46 federal agencies had privacy policies linked from their home pages, 8 agencies had privacy policies that were not on their home pages, and 22 agencies did not have privacy policies.<sup>19</sup> Because the OMB memorandum did not include a definition of “clearly labeled and easily accessed,” we needed to assert criteria. We considered an agency’s privacy policy to be clearly labeled and easily accessed if the policy was located on an agency’s home page, or if the agency’s home page had a hypertext link to the policy that included the word “privacy.”<sup>20</sup> Two of the 69 agencies had

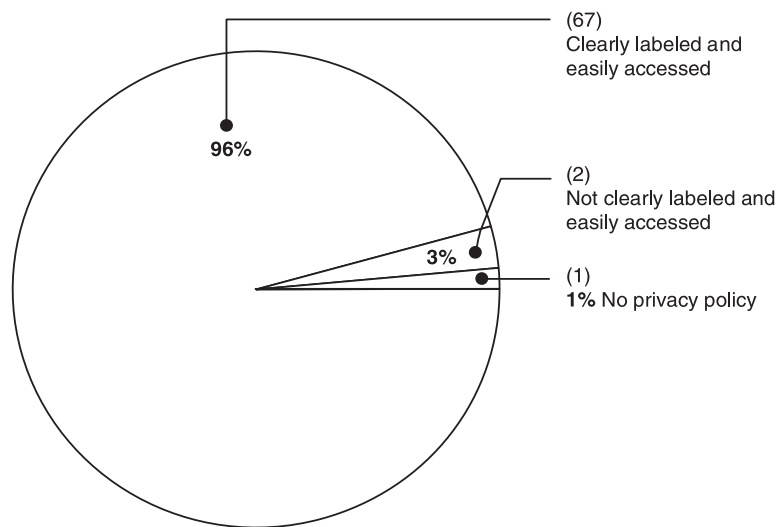
<sup>18</sup> The OMB privacy policy guidance actually uses two headings to describe situation 5— significant actions where information may be subject to the Privacy Act and significant actions where information enters a system of records.

<sup>19</sup> See footnote 16.

<sup>20</sup> We considered an agency’s home page to be the top-level page of the agency. For example, for the Department of Commerce, the agency home page is [www.doc.gov](http://www.doc.gov), and from this page visitors can access all other pages of the agency’s Web site.

privacy policies that did not meet our criteria for being clearly labeled and easily accessed. Specifically, one agency had its privacy policy located under a link “Web Site Policies and Notices,” and one agency had its privacy policy under “Help/Site Info.” Figure 1 shows the number and percentage of agencies we reviewed that had posted privacy policies on their principal Web sites on April 14, 2000.

**Figure 1: Number and Percentage of Agencies That Had Privacy Policies Posted on Their Principal Web Sites on April 14, 2000**



Source: GAO analysis.

## Most Agencies Informed Visitors About Information Collection Practices

To determine if agencies followed the requirement of OMB’s memorandum to inform visitors to their Web sites about what information agencies collect, why they collect it, and how they will use it, we reviewed whether agencies addressed in their policies that they were (1) collecting information automatically and (2) collecting information that visitors provide voluntarily using e-mail and on-line forms.<sup>21</sup> Of the 70 agencies we reviewed, 63 had privacy policies explaining that they automatically collected information when individuals visited their Web sites<sup>22</sup>, and 67 had privacy policies that explained that they collected information that visitors voluntarily provide through e-mail or on-line forms.

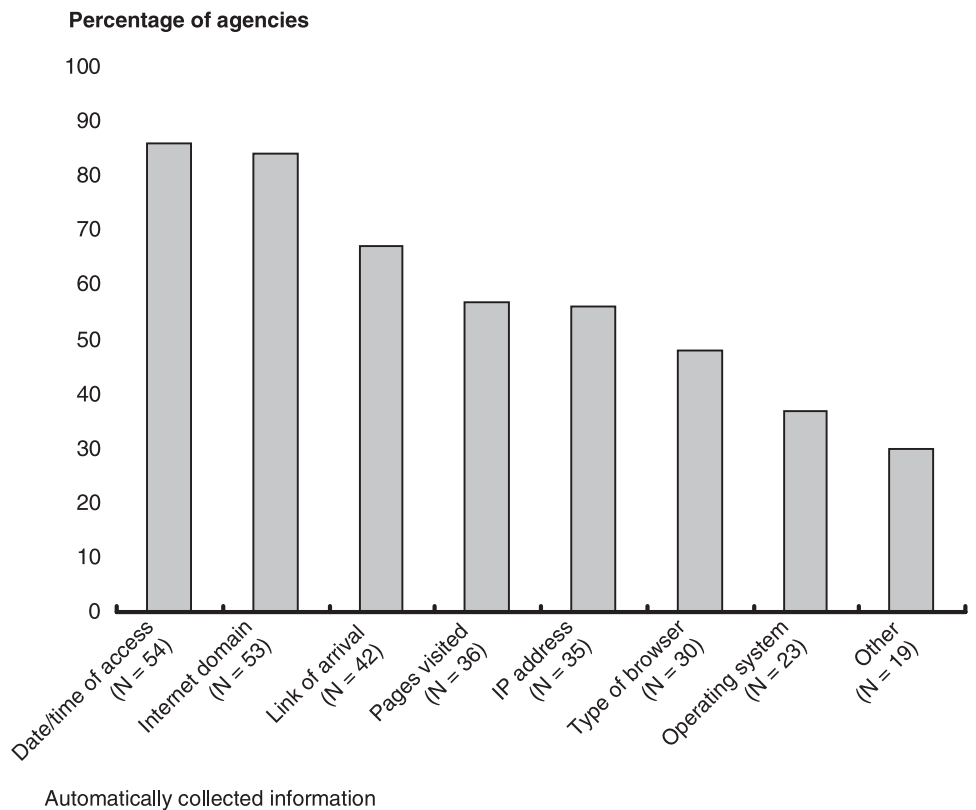
<sup>21</sup> Although OMB’s guidance includes a section on security, intrusion, and detection language, we included our work on that information practice in our discussion of automatically collected information.

<sup>22</sup> The 63 agencies explained that they collected information automatically through the use of logs.

## Many Agency Privacy Policies Addressed Information Collected Automatically

OMB’s guidance recognizes that in the course of operating Web sites, agencies may collect certain information automatically when individuals visit agency Web sites and that this information does not typically identify a visitor personally. In addition, the OMB guidance recognizes that agencies also may collect information automatically by using “cookies.”<sup>23</sup> The guidance provides examples of types of automatically collected information, such as the date or time that a visitor accesses the site, the Internet address of the link through which a visitor accesses the site, the addresses of the Web pages visited, and the type of browser a visitor uses to access the site. Figure 2 shows the types of automatically collected information and the number and percentage of agencies that explained in their privacy policies that they collected this information.

**Figure 2: Types of Automatically Collected Information Addressed in 63 Agency Privacy Policies**



Note: Of the 70 agencies we reviewed, 63 explained that they collected information automatically through the use of logs. Figure 2 shows in parentheses the number of agencies that collected each type of information.

<sup>23</sup> A cookie is a file that is placed on a Web user’s hard drive by a Web site. The cookie can monitor the user’s access of the site, usually without the user’s knowledge.

Source: GAO analysis.

Of the 63 agency privacy policies that explained that they collected information automatically from visitors to their Web sites, 46 followed all 3 of the elements that were contained in the OMB memorandum, that is— what information they collect, why they collect it, and how it will be used. According to an OMB official, OMB recognizes that often the why and how are difficult to distinguish. In doing our work, sometimes we also encountered difficulty in distinguishing between the why and the how. However, in most cases, our assessment was that agencies that addressed the why also addressed the how. Table 1 shows the number of agencies that addressed what, why, and how and the number that addressed all three.

**Table 1: Number of Agencies That Followed OMB’s Requirements to Disclose What, Why, and How for Automatically Collected Information**

<b>OMB requirement</b>	<b>Agencies that addressed automatic collection of information (n=63)</b>
What information is collected	56
Why the information is collected	54
How the information will be used	52
All three—what, why, and how	46

Source: GAO analysis of agency privacy policies posted on Web sites on April 14, 2000.

In addition although not required by the OMB memorandum or the attached guidance, we noted that 11 agencies’ privacy policies specifically addressed the issue of how long they would maintain automatically collected information or that they would destroy such information. For example, the Small Business Administration’s posted privacy policy stated that the agency regularly destroys automatically collected information in accordance with guidance set forth by the National Archives and Records Administration.

**Some Agencies Disclosed the Use of Cookies in Their Privacy Policies**

OMB’s June 1999 guidance is not clear on whether agencies should disclose whether or not they use cookies to collect information. The section of the guidance on information that is collected and stored automatically begins with this sentence: “In the course of operating a Web site, certain information may be collected automatically in logs or by cookies.” However, the section then notes that agencies may have the technical ability to collect information and later take additional steps to identify people, such as looking up Internet addresses linked to specific individuals. The paragraph closes by stating that agencies’ “policies should

make clear” whether or not they are collecting this type of information and whether they “will take further steps to collect more information.” If the reference to “this information” covers the use of logs and cookies and not just additional steps, such as looking up Internet addresses linked to individuals, then to follow the 1999 memorandum and guidance, agencies should be stating whether or not they use automatically collected information, including logs and cookies, in the privacy policies they post on their principal Web sites and major entry points.

On June 22, 2000, however, OMB issued a memorandum that limits the use of cookies and clarifies that if agencies use cookies they are to disclose the use. The June 2000 memorandum directs federal agencies and contractors not to use cookies on their Web sites, unless they provide “clear and conspicuous notice” 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 of the agency head.

Of the privacy policies that we reviewed on April 14, 2000, 11 stated that the agencies used cookies, and 17 policies stated that the agencies did not use cookies to collect information. Thus, of the 70 agencies, 28 addressed whether or not they used cookies. Of the 11 agencies that disclosed that they used cookies, 8 addressed all 3 elements of the OMB memorandum. Table 2 shows the number of agency privacy policies that addressed the use of cookies to automatically collect information and the number of agencies that addressed the OMB requirement to address what, why, and how.

**Table 2: Number of Agencies That Followed OMB Requirements to Address What, Why, and How for Cookies**

OMB requirement to disclose	Agencies that said they used cookies (n=11)
What information is collected	8
Why the information is collected	11
How the information will be used	10
Addressed all three—what, why and how	8

Source: GAO analysis of agency privacy policies posted on Web sites on April 14, 2000.

**Some Agencies Disclosed Whether or Not They Used Security and Intrusion Detection Measures to Collect Information**

Although the OMB guidance is not clear that agencies’ posted privacy policies should address whether or not they use security and intrusion detection measures to collect information on visitors to their Web sites, 36 of the 70 agencies, or about half, addressed this issue. The guidance recognizes that agencies may collect information to detect potentially

---

harmful intrusions to their Web sites and to take action once an intrusion is detected. The guidance states that in the event of authorized law enforcement investigations, and according to any required legal process, information from Internet Protocol (IP) logs and other sources may be used to help identify an individual.<sup>24</sup> However, the guidance does not explicitly state that agencies must identify in their privacy policies whether or not they use security and intrusion detection measures to collect information from visitors to their Web sites. In addition, although most of the discussion of model language in this section of the guidance concerns agencies' on-line management of security threats, the last sentence of the guidance states: "In the event of authorized law enforcement investigations, and pursuant to any required legal process, information from those logs and other sources may be used to help identify an individual." It is unclear whether this sentence refers specifically to law enforcement investigations stemming from an agency's detection of intrusion to the security of its Web site or whether the sentence refers to potential uses of personal information for law enforcement or any other legal process purposes that are not related to the intrusion of an agency's Web site.

---

**Many Agency Privacy Policies Addressed Information Provided by Visitors**

OMB's guidance also recognizes another information practice that agencies use—the collection of information voluntarily provided by individuals through e-mails and on-line forms when they visit an agency's Web site. According to the OMB guidance, many Web sites receive personal, identifiable information voluntarily from individuals via e-mails or on-line forms, and some statement is appropriate about how agencies treat identifiable information when an individual provides it.

Of the 67 agencies whose privacy policies on their principal Web sites explained that they collected personal information voluntarily submitted by visitors to their Web sites, 57 disclosed how and why such information would be used.<sup>25</sup> In determining whether the agencies' policies adhered to OMB's guidance, we were often unable to make a clear distinction between why and how. For example, a typical explanation that we judged to address both how and why information would be used was: "we may use this information to respond to your request." The privacy policies of 46 of the 67 agencies specifically explained that this information could be

---

<sup>24</sup> An IP is a set of procedures in telecommunications connections that the terminals or nodes use to send signals back and forth and that track the address of nodes, route outgoing messages, and recognize incoming messages. An IP log collects and stores incoming messages.

<sup>25</sup> We did not analyze whether an agency Web site explained what information it collected because we assumed that visitors would know what information they were providing to an agency.

---

collected through e-mail, and 18 of the 67 agencies explained that this information could be collected through on-line forms.

Although not specifically required, OMB's sample language suggests that agencies include statements on the length of time they maintain information collected and whether they share information with third parties. OMB suggests, when applicable, that a general and helpful comment would be: "we only use information included in an e-mail for the purpose provided and that the information will be destroyed after this purpose has been fulfilled."

OMB also provides sample language from FTC's privacy policy, which includes:

"The material you submit may be seen by various people. We may enter the information you send into our electronic database, to share with our attorneys and investigators involved in law enforcement or public policy development. We may also share it with a wide variety of other government agencies enforcing consumer protection, competition, and other laws. You may be contacted by the FTC or any of those agencies. In other limited circumstances, including requests from Congress or private individuals, we may be required by law to disclose information you submit."

Of the 70 agencies, only 5 addressed how long they would maintain information collected, and 49 explained whether or not they would share the information with others. Of the 49 agencies, 26 stated they would not share information with third parties, and 23 stated they would. Of the 23 agencies that disclosed they would share information with third parties, in most instances, the third parties were other federal agencies.<sup>26</sup>

---

## Selected Agencies Generally Used Similar Criteria to Define Major Entry Point

The OMB guidance requires agencies to post privacy policies at major entry points to their Web sites. The guidance, however, does not define a major entry point. Nevertheless, we found that the six selected agencies we reviewed used similar criteria in designating a Web page as a major entry point. In reviewing the major entry points that agencies identified, we found very few instances in which agencies had not posted privacy

---

<sup>26</sup> All but four agencies stated that they share the information only with other federal agencies. The instances the four agencies described in their privacy policies were as follows: one agency stated that it shares information with "trade associations, bilateral development banks, or any agency that shares [its] mission"; another agency stated that it may share information with "product manufacturers, distributors, or retailers, but no names or other personal information will be disclosed without explicit permission"; a third agency stated that personally identifiable information "is used generally to respond to your request but may have other uses which are identified on each form"; finally, an agency stated that at the point of collection, it will inform the visitor "how information that personally identifies [the visitor] will be used, including whether such information may be transmitted to third parties."



policies on those Web pages or posted policies that were not clearly labeled and easily accessed.

OMB’s guidance states that federal agency Web sites are highly diverse and have many different purposes. An OMB official said that in most cases, major entry points might be the home pages of the major components of an agency. For example, the official said that the home page for the Department of Justice’s Federal Bureau of Investigation could most likely be considered a major entry point for the Department.

We reviewed the Web sites of 6 of the 70 agencies because they had large numbers of Web sites or had frequent contact with the public. The four departments—Commerce, Defense, Interior, and Justice—generally defined their criteria, or part of their criteria for a major entry point, as being the home pages of their major components, bureaus, or operating units. In addition, three of the four departments and two independent agencies—SBA and SSA—used the number of visits to their Web pages as a basis for determining which pages should be designated as major entry points. For example, the Department of Justice had three criteria for defining a major entry point: (1) the home page of one of its components, (2) a Web page that routinely receives a higher number of visits than a component’s home page, or (3) a Web page that receives more than 2,000 visits per week. The Department of Justice was the only agency that defined a specific number of visits as being a criterion for determining a major entry point. Table 3 shows the number of Web pages that the agencies identified as major entry points as of May 1, 2000, and the criteria that they used to define a major entry point.

**Table 3: Criteria Selected Agencies Identified as Using to Determine Major Entry Points**

Agency	Number of major entry points identified	Criteria agency identified as using to determine its major entry points		
		Home pages of major components	Most visited Web pages	Other
Commerce <sup>a</sup>	17	x	x	
Defense	2,401	x		
Interior	11	x	x	
Justice	112	x	x	x <sup>b</sup>
Small Business Administration	7	x	x	x <sup>c</sup>
Social Security Administration	143		x	x <sup>d</sup>
<b>Total</b>	<b>2,691</b>			

Note: Because the Department of Defense reported a large number of major entry points, we reviewed a random sample of 59 of the Department-identified 2,401 major entry points and found that none were missing privacy policies. On the basis of our analysis of these results, we estimate that if there are any major entry points at the Department of Defense without posted privacy policies, the number does not exceed 5 percent of all the Department’s major entry points.

---

<sup>a</sup>According to a Department of Commerce official, the Department left the identification of Web pages most frequently visited to its operating units. The official said that the Department did not have major entry point information for its operating units readily available. The 17 Web sites the Department identified were for its major components and for a few Web sites that Department officials knew received a high number of visits.

<sup>b</sup>According to a Department of Justice official, the agency also designates Web pages that receive more than 2,000 visits per week as major entry points.

<sup>c</sup>According to an SBA official, the agency defines a major entry point as a Web page that receives a high number of visits and collects personal information from visitors.

<sup>d</sup>According to an SSA official, the agency uses a combination of Web page visits and customer feedback to determine major entry points.

Source: Agency-reported information in response to our request for information.

Most of the Web pages that the six agencies identified as major entry points had privacy policies posted.<sup>27</sup> Two agencies—the Department of Commerce and the Department of Justice—had only nine pages identified as major entry points that either did not have privacy policies posted or, using the criteria previously asserted, did not have clearly labeled and easily accessed policies posted. A Department of Justice official said that the agency is considering changing its criteria for designating a Web page as a major entry point. The official said that due to the high number of visits to the agency’s Web pages, the 2,000 visits per week criterion is too low. The official said that under revised criteria, the pages that we found that lacked privacy policies would no longer be considered major entry points and would not need to have privacy policies posted.

---

## Substantial Personal Information Not Defined, so It Is Difficult to Determine if Agencies Followed OMB’s Memorandum

The OMB memorandum requires agencies to post privacy policies on pages where they collect “substantial” personal information from visitors to their Web sites. However, neither the memorandum nor the attached guidance provides a definition of substantial personal information. OMB officials said that they left the interpretation of this requirement to each agency’s discretion. Without a definition, however, it is difficult to assess whether agencies followed this OMB requirement. Therefore, we developed our own criteria for personal information. We defined personal information to include an individual’s name, e-mail address, postal address, telephone number, Social Security number, or credit card number.<sup>28</sup>

---

<sup>27</sup> We reviewed all the Web pages that five of the six agencies identified as being major entry points. Because the Department of Defense reported a large number of major entry points, we reviewed a random sample of 59 major entry points and found that none were missing privacy policies. On the basis of our analysis of these results, we estimate that if there are any major entry points at the Department of Defense without posted privacy policies, the number does not exceed 5 percent of all the Department’s major entry points. Appendix I provides more details on our methodology.

<sup>28</sup> FTC defined personal identifying information to include these same elements in its report to Congress, *Privacy Online: Fair Information Practices in the Electronic Marketplace*, May 2000.

---

To do this portion of our work on the memorandum's requirement for agencies to post privacy policies on Web pages where they collected substantial personal information, we selected the 31 high-impact agencies, which comprise 1 department, 21 components of departments, 8 independent agencies, and a crosscutting initiative—acquisition reform. For those agencies, we searched the Web sites for up to five pages that collected any personal information. Of the 31 high-impact agencies we reviewed, most did not have privacy policies posted on Web pages that we identified as collecting personal information. During our review of nine selected high-impact agencies, officials from those agencies said that some of the on-line forms should have had privacy policies.<sup>29</sup> In addition, they said that a few of the on-line forms should have had Privacy Act notices because the information collected was being maintained in systems of records.

---

### Nearly Half of the Web Pages That We Identified as Collecting Personal Information Did Not Have Privacy Policies Posted

We recognized that the OMB memorandum did not require agencies to post privacy policies on all Web pages that collect any personal information but rather on pages collecting substantial personal information. However, lacking a basis for judging what would constitute substantial personal information, we used personal information as defined above as our asserted criteria. On this basis, we found that nearly half of the Web pages that we identified as collecting personal information did not have privacy policies posted. In addition, privacy policies were not consistently posted on Web pages that collected personal information for similar purposes or on pages that collected similar types of personal information. Of the 31 high-impact agencies we reviewed, 28 had Web pages that allowed visitors to voluntarily provide personal information through an on-line form. For this purpose, we considered any Web page that requested a visitor to enter information onto the Web page to be an on-line form. This is distinguished from the visitor using an e-mail link to provide information.<sup>30</sup> Of these 28 high-impact agencies, 10 had privacy policies on all the on-line forms that we identified.<sup>31</sup> The remaining 18 high-

---

<sup>29</sup> We selected these nine high-impact agencies because they were either the same as agencies we selected for reviewing major entry points or were components of the departments we included in reviewing major entry points.

<sup>30</sup> Although the report discusses personal information that visitors voluntarily submit through on-line forms, we also reviewed how many high-impact agencies collected personal information, specifically a visitor's e-mail address, when he or she sent an e-mail to the agency. Of the 31 high-impact agencies, 30 had at least 1 page on which visitors could send e-mail. Of these pages, seven had the agencies' privacy policies posted on that page. Although most high-impact agencies did not have privacy policies posted on these pages, we also noted that 26 of the 30 agencies explained how they handled e-mail in the privacy policies posted on their agencies' home pages.

<sup>31</sup> If an on-line form did not have a privacy policy posted on that page but did have one on an intermediary page that an individual would likely view before arriving at the form, we considered this

---

impact agencies did not have privacy policies posted on at least 1 page that visitors could use to provide personal information.<sup>32</sup> For the 28 high-impact agencies, we identified 101 on-line forms that visitors could use to submit personal information.<sup>33</sup> Of these forms, 57 had privacy policies posted, and 44 did not.<sup>34</sup>

On-line forms that the high-impact agencies used to collect information for similar purposes did not consistently have privacy policies posted. The high-impact agencies collected personal information through the on-line forms that we identified for various purposes, including allowing visitors to order publications; apply for permits, benefits, or jobs; and subscribe to electronic mailing lists. All the on-line forms that visitors could use to apply for jobs and benefits had privacy policies posted. However, not all forms that visitors could use to place an order contained privacy policies. For example, we identified 14 forms that collected personal information for the purpose of placing an order. Of these, two had privacy policies posted on the page, and two had privacy policies posted on an intermediary page that an individual would likely view before arriving at the form. However, 10 forms did not have privacy policies posted. Nine agencies had not posted privacy policies on pages that collected personal information that was used to place an order. Table 4 illustrates the purposes for which the high-impact agencies collected information and whether or not privacy policies were posted.

---

as having a privacy policy posted. Of the 10 high-impact agencies with privacy policies posted on all the on-line forms we identified, 6 had the policies located on an intermediary page that an individual would likely view before arriving at the form.

<sup>32</sup> For purposes of this analysis, if a high-impact agency posted a Privacy Act notice, we counted this as the agency having a privacy policy posted.

<sup>33</sup> For each high-impact agency we reviewed, we identified up to five Web pages that could collect personal information from visitors using on-line forms.

<sup>34</sup> Of the 57 on-line forms, 21 had privacy policies located on an intermediary page that an individual would likely view before arriving at the form.

**Table 4: Number of High-Impact Agencies' On-Line Forms With Posted Privacy Policies by Purpose of Collection**

Purpose of collection of personal information	Number of on-line forms			
	Total	With privacy policies posted <sup>a</sup>		Without privacy policies posted
		On the Web page	On a prior Web page <sup>b</sup>	
Provide feedback, comments, guestbook	16	9	1	6 <sup>c</sup>
Place an order	14	2	2	10 <sup>c</sup>
Request services	13	3	4	6
Apply for permit or patent	11	3	5	3
Apply for benefits	10	6	4	0
Subscribe to mailing list	7	4	1	2
Ask a question about agency program	7	5	1	1
Apply for a job	4	3	1	0
Register for meetings or training	4	0	0	4
Report adverse event or formal complaint	3	1	0	2 <sup>c</sup>
Make a FOIA request	2	0	0	2
Other	10	0	2	8
<b>Total</b>	<b>101</b>	<b>36</b>	<b>21</b>	<b>44</b>

<sup>a</sup>For purposes of this analysis, if a high-impact agency posted a Privacy Act notice, we counted this as the agency having posted a privacy policy. Of the 101 on-line forms, we identified 19 on-line forms that had Privacy Act notices posted.

<sup>b</sup>"On a prior Web page" refers to on-line forms that had privacy policies posted on an intermediary page that an individual would likely view before arriving at the form.

<sup>c</sup>One of the on-line forms had a privacy policy posted, but it was not clearly labeled. We counted this as the form not having a privacy policy posted.

Source: GAO analysis of data from Web sites of the high-impact agencies.

Furthermore, on-line forms with information being collected for similar purposes did not consistently have privacy policies posted even within a single high-impact agency. For example, two offices within the same high-impact agency had on-line forms that visitors could use to submit feedback on the Web site. One of the forms had a privacy policy posted, and the other did not.

By far, the largest number of forms that we identified collected contact information. We defined contact information to include at least two of the following: an individual's name, e-mail address, postal address, or telephone number. For the 31 high-impact agencies, 70 of the 101 on-line forms we identified collected contact information. Of these 70 forms, 38 did not have privacy policies posted. Other forms collected information, such as a Social Security or credit card number. Of the 101 on-line forms

we reviewed, 17 asked visitors to provide a Social Security number, among other information.<sup>35</sup> All but one of these forms had privacy policies posted. Of the 101 on-line forms we reviewed, 8 collected credit card numbers; 5 of the 8 forms did not have privacy policies posted. Table 5 describes the number of forms with posted privacy policies by the type of personal information collected.

**Table 5: Number of High-Impact Agencies' On-line Forms With Posted Privacy Policies by Type of Personal Information Collected**

Type of personal information collected on on-line form	Number of on-line forms			
	Total number of on-line forms	With privacy policies posted <sup>a</sup>		Without privacy policies posted <sup>c</sup>
		On the Web page	On a prior Web page <sup>b</sup>	
Social Security number	17	9	7	1
Credit card number	8	0	3	5
Contact information only <sup>d</sup>	70	22	10	38
E-mail address only	6	5	1	0
<b>Total</b>	<b>101</b>	<b>36</b>	<b>21</b>	<b>44</b>

<sup>a</sup>For purposes of this analysis, if a high-impact agency posted a Privacy Act notice, we counted this as the having a privacy policy posted. Of the 101 on-line forms, we identified 19 on-line forms that had Privacy Act notices posted.

<sup>b</sup>“On a prior Web page” refers to on-line forms that had privacy policies posted on an intermediary page that an individual would likely view before arriving at the form.

<sup>c</sup>Three of the on-line forms had privacy policies posted that were not clearly labeled. We counted these as not having privacy policies posted.

<sup>d</sup>We defined contact information to include at least two of the following items: an individual's name, e-mail address, postal address, or telephone number but not credit card or Social Security numbers.

Source: GAO analysis of data from Web sites of high-impact agencies.

**Some Web Pages Lacked Privacy Policies, and Others Lacked Required Privacy Act Notices**

If an agency plans to maintain personal information in a system of records, under the Privacy Act, it is required to include a notice on the form it uses to collect personal information or on a separate form that can be retained by the individual. The Privacy Act states that the notice should include the following items: (1) the authority that allows the request of the information and a statement on whether providing the information is mandatory or voluntary; (2) the principal purpose or purposes for which the information is to be used; (3) the routine uses that may be made of the information; and (4) the effects on the individual, if any, of not providing all or any part of the requested information. The OMB privacy policy guidance, in a section relating to “significant actions where information enters a system of records,” states that if a Privacy Act notice would be required in the paper-based world, agencies should post a Privacy Act notice on the Web page or

<sup>35</sup> Of the 17 on-line forms, 7 had privacy policies located on an intermediary page that an individual would likely view before arriving at the form.

---

through a clearly labeled hyperlink.<sup>36</sup> The guidance also states that to date, agencies have not collected a large amount of personal information on the Internet that agencies are maintaining as systems of records.

To determine if pages that we identified needed either the OMB required privacy policies or Privacy Act notices posted, we contacted officials at nine judgmentally selected high-impact agencies.<sup>37</sup> The 9 high-impact agencies had 30 on-line forms that we identified that visitors could use to provide personal information. Of these forms, 12 had privacy policies, 8 had Privacy Act notices, and 10 had neither privacy policies nor Privacy Act notices posted. We discussed the forms that did not have privacy policies posted with officials of those high-impact agencies. For eight forms, officials from four of the high-impact agencies said that the forms we identified should have had privacy policies posted. The officials generally said that it was an oversight that the policies had not been posted and that they would take corrective action. In addition, officials of three high-impact agencies said that four forms, two of which had privacy policies posted, should have had Privacy Act notices posted because, according to agency officials, these forms collected information that the agencies were maintaining in systems of records. The forms collected personal information for the purposes of making park reservations, participating in a wild horse and burro adoption program, ordering publications, and obtaining a log-in name and password for submitting an on-line resume. Officials for these agencies said that it was an oversight that these forms did not have Privacy Act notices posted and that the agencies were in the process of taking corrective action.

For the nine high-impact agencies, table 6 shows the number of forms that did not have either privacy policies or Privacy Act notices posted and the number of those forms that agencies identified as needing privacy policies or Privacy Act notices.

---

<sup>36</sup> As discussed in appendix IV, because the intended meaning of the phrase “significant actions” is not defined in the memorandum and is thus unclear, an agency could interpret this as distinguishing between significant and nonsignificant actions. Under the Privacy Act, however, personally identifiable information is covered by the act if it is in a system of records; the act does not distinguish between significant and nonsignificant information.

<sup>37</sup> The selected high-impact agencies included the Bureau of the Census, Patent and Trademark Office, and International Trade Administration within the Department of Commerce; the Acquisition Reform initiative within the Department of Defense; Bureau of Land Management and National Park Service within the Department of the Interior; Immigration and Naturalization Service within the Department of Justice; SBA and SSA.

**Table 6: Number of On-line Forms Reviewed That Collect Personal Information That Selected High-Impact Agencies Identified as Needing Privacy Policies or Privacy Act Notices**

High-impact agency	Number of on-line forms				Number of on-line forms without privacy policies or Privacy Act notices that agencies identified as needing them	
	Total	With privacy policies posted <sup>a</sup>	With Privacy Act notices posted	Without privacy policies or Privacy Act notices	Privacy policies	Privacy Act notices
Department of Commerce						
Bureau of the Census	4	3 <sup>b</sup>	1 <sup>c</sup>	0	0	1 <sup>b</sup>
Patent and Trademark Office	5	0	1 <sup>c</sup>	4	4 <sup>d</sup>	0
International Trade Administration	4	3	0	1	1 <sup>d</sup>	0
Department of Defense						
Acquisition Reform initiative	1	0	1	0	0	0
Department of the Interior						
Bureau of Land Management	3	0	1 <sup>c</sup>	2	0	2
National Park Service	3	1 <sup>e</sup>	1 <sup>c</sup>	1	1 <sup>d</sup>	1 <sup>e</sup>
Department of Justice						
Immigration and Naturalization Service	1	1	0	0	0	0
Small Business Administration	5	3	0	2	2 <sup>f</sup>	0
Social Security Administration	4	1	3 <sup>g</sup>	0	0	0
<b>Total</b>	<b>30</b>	<b>12</b>	<b>8</b>	<b>10</b>	<b>8</b>	<b>4</b>

<sup>a</sup>Seven of the on-line forms in this column had privacy policies posted on an intermediary page that an individual would likely view before arriving at the form.

<sup>b</sup>One of these forms had a privacy policy posted, but agency officials agreed that the form should have had a Privacy Act notice posted on the page. Officials said that there was a Privacy Act notice but that it was not posted directly on the page that collected personal information for log-in purposes, however, it was located on a subsequent page.

<sup>c</sup>The Privacy Act notice did not include language that addressed all of the elements required by the Privacy Act.

<sup>d</sup>The agency has subsequently posted privacy policies on these on-line forms.

<sup>e</sup>This form had a privacy policy posted and agency officials agreed that the form should have had a Privacy Act notice posted.

<sup>f</sup>An SBA official stated that subsequent to our audit work, the agency has revised its posted privacy policy to incorporate references to the Privacy Act and the Code of Federal Regulation's Part 102 (Record Disclosure and Privacy) into its posted privacy policy. In addition, the official stated that the agency's major home pages now include a "privacy" button that links visitors to the agency's revised privacy policy and that SBA plans to install a privacy link on all SBA Web pages.

<sup>g</sup>These three forms also had privacy policies, but because they also had Privacy Act notices, we included them in this column.

Source: GAO analysis of data obtained from Web sites and officials of high-impact agencies.



---

We also noted that four of the eight Privacy Act notices that we found on pages that collected personal information did not include language that addressed all of the elements required by the Privacy Act.

Under the Paperwork Reduction Act, OMB has responsibility to oversee agencies' adherence to the Privacy Act. For OMB's memorandum and guidance, which extends privacy policies to on-line information collections that are not covered by the Privacy Act, OMB officials said that they spot-check whether agencies post privacy policies.

**Officials Cited Reasons for Not Posting Privacy Act Notices**

Agency officials said they did not need to post Privacy Act notices on all their forms that collected personal information because they were not maintaining the information in systems of records that they were retrieving by personal identifier. Officials said that the forms we identified for the Small Business Administration, Patent and Trademark Office, and the International Trade Administration were primarily for collecting information on businesses. The personal information collected was primarily for contact purposes. In addition, they said that the information is not retrieved from their databases by personal information but by company name or patent number. Three agencies—the Bureau of the Census, the Immigration and Naturalization Service, and the National Park Service—had forms that requested name and contact information for ordering publications. Again, agency officials told us that Privacy Act notices were not required. For example, the Privacy Act Officer for the Department of the Interior said that the National Park Service on-line order form does not require a Privacy Act notice because the personal information is used only to address an envelope to mail publications, after which the information is immediately destroyed.

In addition, during our review, we observed that a few hyperlinks on some of the Web sites of the high-impact agencies took us to on-line forms of other nonfederal Web sites. Neither the OMB memorandum nor the attached guidance addresses this situation. The Web sites of some high-impact agencies alerted us when we were exiting the site. For example, the Immigration and Naturalization Service had a message that informed visitors that they were leaving the agency's site. Also, the posted privacy policy of the National Park Service explained that when visitors linked to another Web site, they would no longer be subject to the agency's privacy policy and that they would be subject to the privacy policy of a different site.

---

## Comparison of OMB Guidance to the Privacy Act and Fair Information Principles

As we mentioned earlier, in addition to the statutory requirements that protect an individual's right to privacy, fair information practices exist. Most recently, in its May 2000 report to Congress,<sup>38</sup> FTC summarized these practices into four core principles of privacy protection: notice, choice, access, and security. According to FTC, under notice, data collectors must disclose their information practices before collecting personal information from individuals. Under choice, individuals must be given options concerning whether and how personal information collected from them may be used for purposes beyond those for which the information was provided. Under access, individuals should be able to view and contest the accuracy and completeness of data collected about them. And under security, data collectors must take reasonable steps to ensure that information collected from individuals is accurate and secure from unauthorized use. According to OMB officials, the privacy policy guidance was primarily intended to address the first of the four principles—notice. For personal information subject to the Privacy Act, an individual is provided choice as to whether there will be a subsequent disclosure of his or her personally identifiable information that is contained in an agency's system of records, unless the disclosure is authorized by law. Under the Privacy Act, an agency is authorized to share information contained in its system of records with other parties, such as law enforcement agencies and Congress. Thus, individuals cannot have complete choice over the disclosure of their personal information. The remaining two principles—access and security—are generally covered by the Privacy Act. See appendix IV for additional information on the Privacy Act and implementing guidance and appendix V for more information on fair information principles.

Table 7 compares various information practices covered by OMB's Memorandum M-99-18 and its attached guidance, the Privacy Act, and the fair information principles as summarized by FTC in May 2000.

---

<sup>38</sup> See footnote 3.

**Table 7: Comparison of OMB Guidance with Privacy Act and Fair Information Principles**

Practice	Covered under		
	OMB M-99-18 and guidance	Privacy Act <sup>a</sup>	Fair information principles
Posting of privacy policy	X		X
Clear notice of information practices	X	X	X
Use of information collected			
What	X	X <sup>b</sup>	X
Why	X	X <sup>b</sup>	
How	X	X <sup>b</sup>	X
How collected	X		X
Agency to disclose			
Choice to individuals		X <sup>c</sup>	X
Access to individuals		X	X
Security to individuals		X	X
Notification of whether information is shared with other entities		X	X
Notification of whether information is maintained in a system of records	X	X	

<sup>a</sup>If an agency is maintaining personally identifiable information about an individual in a system of records, the information is subject to the Privacy Act; thus, the agency is to inform the individual supplying the information of (1) the authority that authorizes the collection of information and whether disclosure is mandatory or voluntary; (2) the principal purpose for which the information is intended to be used; (3) the routine uses that may be made of the information; and (4) the effects on the individual, if any, of not providing all or any part of the requested information. This information is to be provided on the form that is used to collect the information or a separate form that can be retained by the individual. Further, the agency must publish a notice of the existence of a system of records in the Federal Register.

<sup>b</sup>Although the disclosure of what information an agency collects, why it collects the information, and how it uses the information is not specifically required by the Privacy Act in these terms, on the basis of our assessment of the information required by the Privacy Act, it covers such disclosure.

<sup>c</sup>Under the Privacy Act, no agency can disclose any record that is contained in a system of records to any person or another agency without the consent of the individual to whom the record pertains, unless the disclosure is authorized by law.

Source: GAO analysis of OMB memorandum and its related guidance, the Privacy Act, and fair information principles as recently summarized by FTC.

## Conclusions

Protecting an individual’s right to privacy has been a long-standing concern of the federal government, as evidenced by the Privacy Act of 1974 and other laws and implementing guidance. However, the Privacy Act was passed long before the development of the current advances in information technology. By issuing its 1999 guidance, OMB took an important step in bringing the federal government’s protection of an individual’s privacy in line with current technological advancements by providing guidance to agencies for addressing the collection of on-line personal information through the on-line posting of privacy policies. However, the memorandum and attached guidance are unclear in several respects and contain undefined language.

---

OMB's memorandum requires that agencies' principal Web sites should have clearly labeled and easily accessed privacy policies that inform visitors about what information the agencies collect on their Web sites, why they collect it, and how they will use it. The overwhelming majority of principal Web sites we reviewed had clearly labeled and easily accessed privacy policies. This result contrasts with the results of surveys conducted by public interest groups in August 1997 and April 1999 that reported only about one-third or fewer of agencies surveyed had posted privacy policies on their principal Web sites. It is more difficult to determine if agencies are following the memorandum when specific information collection or use practices are considered. For example, three-quarters of the principal Web sites that disclosed that they automatically collected information from visitors also explained what information they collected, why they collected it, and how they used the information. Although OMB's memorandum clearly requires agencies to include these three elements in their privacy policy statements, an OMB official said that OMB recognizes that it is often difficult to distinguish between why information was collected and how it would be used. In doing our work, we also encountered some difficulty in distinguishing between why information was collected and how it would be used.

The memorandum and guidance also do not clearly state whether agencies must address in their privacy policies each of the information practices identified in the guidance, including information collected and stored automatically. On the specific issue of whether they used cookies to automatically collect information, a little more than a third of principal Web sites disclosed whether or not they did so. However, OMB's guidance when the memorandum was issued did not clearly direct such complete disclosure. OMB published a memorandum in June 2000 that clarifies this requirement. On the issue of whether agencies' Web sites used security and detection measures, only about half of the 70 principal Web sites addressed that they used such measures. Again, however, the OMB guidance did not clearly state that agencies were required to say whether or not they used such measures.

Because agencies are being tasked with conducting more business on-line, the importance of posting privacy policies that clearly inform visitors as to how the information they provide will be treated becomes more important. It becomes especially important because, given the mechanics of the Internet, visitors can enter virtually any Web page directly from any number of Web pages, including pages from outside an agency. Therefore, Web pages that collect personally identifiable information could be the first place a visitor enters a Web site. In such a case, the visitor's only

---

opportunity to learn of an agency's privacy policy would be from the page collecting the personal information.

Almost half of the forms we identified that collected personal information did not have privacy policies posted. However, because OMB's guidance requires privacy policies to be posted on agencies' Web pages where "substantial" personal information is collected but does not define what is meant by substantial information, we could not determine whether the forms we found that lacked privacy policies should have had them under OMB's memorandum. It is not clear, for instance, in OMB's guidance whether such information as Social Security numbers and credit card numbers qualify as substantial personal information. We found a few instances when such information was collected from on-line forms without posted privacy policies. Finally, although we reviewed only a few selected agencies to determine if Privacy Act notices should have been posted, we identified four instances where agency officials said that they should have posted Privacy Act notices because they were collecting personal information that they were maintaining in systems of records. In addition, some of the agencies that had Privacy Act notices on pages that collected personal information did not address all of the required elements of the Privacy Act. For OMB's memorandum and guidance, which extend privacy policies to on-line information collections that are not covered by the Privacy Act, OMB officials said that they spot-check whether agencies post privacy policies.

We also found a few instances where agencies seemed to be providing useful information in their privacy policies to Web site visitors that was not required by OMB's memorandum but suggested by its guidance. We found that a few agencies' privacy policies included information about how long information provided by visitors would be maintained and whether it would be shared with others. In addition, federal agencies sometimes provided links on their Web sites that took visitors to other federal agencies and, in some instances, to private organizations. During our work, we noted that the privacy policies of some agencies clearly alerted visitors when they were leaving the agencies' Web site, or the visitors received a message when they were leaving the agency's Web site.

---

## Recommendations

We recommend that the Director of OMB consider, in consultation as appropriate with parties such as the CIO Council, how best to help agencies better ensure that individuals are provided clear and adequate notice about how their personal information is treated when they visit federal Web sites. This should include:

- 
- defining what is meant by substantial personal information;
  - clarifying other sections of the guidance, including if agency privacy policies should specifically disclose whether or not they use security and intrusion detection measures; and
  - determining whether a distinction should continue to be made between why an agency collects information and how the information will be used; if the distinction is maintained, provide additional guidance on how agencies should make that distinction.

We also recommend that the Director of OMB, working, as appropriate, with agencies, Inspectors General, or the CIO Council, determine whether current oversight strategies are adequate to ensure agencies' adherence to Web site privacy policies and whether the policies will need further revision as Web practices continue to evolve. As part of this oversight, we recommend that the Director (1) ensure that the agencies we found that had not posted Privacy Act notices where required, do so, and (2) determine the extent to which the lack of Privacy Act notices is a problem on federal Web sites.

---

## Agency Comments and Our Evaluation

We provided a draft of this report for review and comment to the Director of OMB.

In a letter dated August 30, 2000 (see app. VI), OMB's Deputy Director for Management said that the report addresses a subject that is "very important to this Administration—the protection of personal privacy online." However, the Deputy Director said that the findings presented in the report do not adequately reflect the "significant progress that the federal agencies have made in this area." Specifically, the Deputy Director for Management said that executive branch agencies implemented the OMB memorandum with great success and that "agencies have now adopted privacy policies at the most important Web pages on their sites, with a virtually perfect record at agency principal Web sites and at major points of entry."

We believe our draft report provided a balanced assessment of agencies' implementation of OMB's memorandum and guidance at the time of our review. For example, we pointed out in our report that the overwhelming majority of federal Web sites we reviewed posted privacy policies on their principal Web sites, that is, the home pages of their Web sites. We also provided information from an April 1999 survey of agencies' Web sites' privacy notices so that readers could gauge the progress agencies have made. However, we also reported that the content of the privacy policies posted on the principal Web sites did not always address the required

---

elements of the OMB memorandum. Consequently, we did not believe any changes were needed to our final report.

It also is not clear to us that the agency principal Web sites and major entry points are necessarily the most important pages on agencies' Web sites regarding the collection of personal information. Given the mechanics of the Internet, which allow visitors to enter a Web site from any number of pages or a hyperlink, visitors can bypass both principal Web sites and major entry points and go directly to a page that collects personal information. Because the first place a visitor could enter a Web site (and perhaps the only opportunity the visitor has to learn of an agency's privacy policy) may be a Web page that collects personal information, as OMB's memorandum recognizes, it is important for agencies to post privacy policies on these pages to notify an individual about how his or her personal information will be treated. Nearly half of the Web pages that we identified as collecting personal information did not have posted privacy policies. Therefore, although we agree that agencies have made commendable progress in following OMB's memorandum, we believe that OMB's guidance on when agencies should post privacy policies on Web pages that collect personal information could benefit from clarification, especially because the memorandum requires privacy policies on pages where agencies collect substantial personal information, which is not defined.

In response to recommendations made in our draft report, the Deputy Director for Management stated that OMB's guidance was developed with input from agencies and the CIO Council and that OMB would elicit responses from these entities about the specific recommendations and the need for an overall oversight strategy. We believe such input and consultation are beneficial and, indeed, are incorporated into our recommendations to OMB.

We also provided excerpts of the report to the six agencies where we performed additional work on major entry points and Web pages that we identified as collecting personal information. The agencies provided technical comments, which we incorporated into the report where applicable.

---

We will send copies of this report to Senator Fred Thompson, Chairman, Senate Committee on Governmental Affairs; Representative Dan Burton, Chairman, House Committee on Government Reform; Representative

---

Henry A. Waxman, Ranking Minority Member, House Committee on Government Reform; and the Honorable Jacob J. Lew, Director, OMB. Copies will also be made available to others upon request.

Key contributors to this report are listed in appendix VII. If you have any questions, please call me on (202) 512-8676 or Linda Libician on (214) 777-5709.

Sincerely yours,



Michael Brostek  
Associate Director, Federal Management  
and Workforce Issues



---

---

---

# Contents

---

Letter	1
<hr/>	
Appendix I	36
Objectives, Scope, and Methodology	
To Determine if Agencies Posted Clearly Labeled Privacy Policies on Principal Web Sites	36
To Determine if Agencies' Privacy Policies Addressed What Information Agencies Collect, Why They Collect It, and How They Will Use It	37
To Determine How Selected Agencies Interpreted Major Entry Point	39
To Determine if Selected Agencies Had Privacy Policies Posted on Web Pages Where They Collect Substantial Personal Information	39
To Compare OMB's Memorandum With Selected Statutory Requirements and With Fair Information Principles	42
<hr/>	
Appendix II	43
The Names and Internet Addresses of the 70 Executive Branch Agencies Reviewed	
<hr/>	
Appendix III	45
The Names and Internet Addresses of the High-Impact Agencies Reviewed	

---

<b>Appendix IV</b>		47
<b>Applicable Laws and</b>	Privacy Act	47
<b>Implementing</b>	Other Selected Statutes	48
<b>Guidance for</b>	OMB Circular No. A-130	49
<b>Protecting Personal</b>	OMB Privacy Policies for Federal Web Sites	51
<b>Information</b>	Analysis	54
	Conclusion	55
<hr/>		
<b>Appendix V</b>		57
<b>Comparison of Fair</b>	Fair Information Practice Principles	57
<b>Information Principles</b>	The Privacy Act	58
<b>to the Privacy Act and</b>	Analysis	59
<b>Other Laws</b>	Conclusion	62
<hr/>		
<b>Appendix VI</b>		63
<b>Comments From the</b>	GAO Comments	65
<b>Office of Management</b>		
<b>and Budget</b>		
<hr/>		
<b>Appendix VII</b>		66
<b>GAO Contacts and</b>		
<b>Staff</b>		
<b>Acknowledgments</b>		
<hr/>		
<b>Tables</b>	Table 1: Number of Agencies That Followed OMB's Requirements to Disclose What, Why, and How for Automatically Collected Information	11
	Table 2: Number of Agencies That Followed OMB Requirements to Address What, Why, and How for Cookies	12
	Table 3: Criteria Selected Agencies Identified as Using to Determine Major Entry Points	15
	Table 4: Number of High-Impact Agencies' On-Line Forms With Posted Privacy Policies by Purpose of Collection	19

---

**Contents**

---

Table 5: Number of High-Impact Agencies' On-line Forms With Posted Privacy Policies by Type of Personal Information Collected	20
Table 6: Number of On-line Forms Reviewed That Collect Personal Information That Selected High-Impact Agencies Identified as Needing Privacy Policies or Privacy Act Notices	22
Table 7: Comparison of OMB Guidance with Privacy Act and Fair Information Principles	25

---

**Figures**

Figure 1: Number and Percentage of Agencies That Had Privacy Policies Posted on Their Principal Web Sites on April 14, 2000	9
Figure 2: Types of Automatically Collected Information Addressed in 63 Agency Privacy Policies	10

---

---

# Objectives, Scope, and Methodology

This review focuses on whether federal agencies were following Office of Management and Budget (OMB) Memorandum M-99-18 entitled Privacy Policies on Federal Web Sites, and attached guidance entitled Guidance and Model Language for Federal Web Site Privacy Policies. Our objectives were to

- determine if agencies had clearly labeled and easily accessed privacy policies posted on their principal Web sites;
- determine if agencies' privacy policies posted on principal Web sites informed visitors about what information an agency collects, why the agency collects it, and how the agency will use the information;
- determine how selected agencies interpreted the requirement of the OMB guidance to post privacy policies at major entry points; and
- determine if selected agencies have posted privacy policies on Web pages where the agency collects substantial personal information or, when applicable, posted notices that refer to the Privacy Act of 1974.<sup>1</sup>

In addition, as agreed, we compared the OMB privacy policy memorandum with selected statutory requirements that are generally applicable to federal agencies in protecting the privacy of information and with fair information principles, as defined by the Federal Trade Commission (FTC) in its May 2000 report.<sup>2</sup>

## To Determine if Agencies Posted Clearly Labeled Privacy Policies on Principal Web Sites

To determine if agencies had privacy policies posted on their principal Web sites, we reviewed the Web sites of 70 agencies—14 departments, 55 independent agencies, and the Executive Office of the President—on April 14, 2000. We compiled a list of federal executive agencies using two publications—the United States Government Manual (1995/96 edition) published by the National Archives and Records Administration and the Federal Yellow Book (summer 1999 edition) published by Leadership Directories Inc., and we used the Library of Congress' Web site (<http://lcweb.loc.gov/global/executive/fed.html>). We excluded boards, commissions, and committees that were not listed as independent agencies. OMB officials indicated that some of the agencies included in our review might not consider themselves to be “executive branch” agencies that are directly subject to the June 1999 OMB guidance. Because we did not know definitively which agencies should be excluded, and because the

<sup>1</sup> Public Law No. 93-547, 5 U.S.C. 552a. The Privacy Act of 1974 is the primary law regulating the federal government's collection and maintenance of personal information.

<sup>2</sup> In its report to Congress, Privacy Online: Fair Information Practices in the Electronic Marketplace, May 2000, FTC summarized widely accepted principles concerning fair information practices into four principles of privacy protection—notice, choice, access, and security.

---

OMB guidance is consistent with the notice principle incorporated into the Privacy Act and the fair information principles, we believe it is reasonable to determine whether even those agencies not directly subject to the OMB guidance are nevertheless following it. We know that one agency—the U.S. Postal Service—does not believe that it should be on our list of agencies that are to follow the OMB memorandum. According to U. S. Postal Service officials, executive orders and OMB instructions generally do not apply to it. However, the officials said that although the Postal Service is not required to follow OMB’s privacy policy memorandum, it voluntarily adheres to it. We may have included other agencies in this review that are not required to follow OMB’s guidance.

To assess if an agency’s privacy policy was “clearly labeled and easily accessed” on the agency’s principal Web site, (i.e., its home page), we asserted the criterion that an agency’s home page should include either the privacy policy or a hyperlink to the privacy policy.<sup>3</sup> If there was such a link to the agency’s privacy policy, we asserted the criterion that the link should contain the word “privacy.” In cases where there was no agency privacy policy posted directly on the home page of the principal Web site nor a clearly labeled link on that home page, we searched the agency Web site for evidence of a privacy policy posted elsewhere. In these cases we connected to Web pages through other links with labels such as “notices,” “site map,” “about this site,” “help,” or, when available, used the Web site’s search feature with the word “privacy.”

---

## To Determine if Agencies’ Privacy Policies Addressed What Information Agencies Collect, Why They Collect It, and How They Will Use It

To determine if agencies’ privacy policies address what information agencies collect, why they collect it, and how they will use it, we reviewed the privacy policies of the 70 agencies for two information practices—automatically collected information and information provided by individuals through e-mails and on-line forms when they visited an agency’s Web site. We did not verify whether agencies accurately portrayed their information collection practices or whether agencies complied with their posted privacy policies.

For automatically collected information we determined if agencies addressed this practice in their privacy policies. If agencies addressed automatically collected information, we noted what specific information the agencies collected, including Internet domain, type of browser used to

---

<sup>3</sup> A hyperlink is a predefined link from one location to another. The link can jump within a particular location, to another location with the same computer or network site, or even to a location at a completely different physical site. Hyperlinks are commonly used on the Internet to provide navigation, reference, and depth where published text cannot. A hyperlink can be created from text, which typically appears as blue underlined text within an HTML page, or from a graphic.

access the Web site, user's operating system, date and time of access, pages visited, link of arrival, and Internet Protocol (IP) address.<sup>4</sup> To determine if agencies' privacy policies addressed why they were automatically collecting information, we looked for a general statement that addressed why information was collected. Some examples of language we looked for included "for statistical purposes," "for summary statistics," and "to determine the number of visitors." To determine if agencies addressed how they were using this information, we looked for a general statement that addressed how they used the information. We also looked for an action taken as a result of collecting information, and examples of language we looked for included "to improve our site" and "to identify problem areas." In addition, we looked for more specific descriptions of how an agency might use information, such as how long it would maintain automatically collected information. Also, we identified whether agencies' privacy policies addressed the use of cookies to collect information.<sup>5</sup> If privacy policies addressed cookies, we used the same criteria mentioned earlier to determine if the privacy policies addressed what information was collected, why it was collected, and how it would be used. In addition, we noted if the policies specifically addressed whether or not agencies disclosed the use of security and intrusion detection measures to collect information about visitors to their Web sites.

For the second information practice—information provided by individuals through e-mails and on-line forms who visited the agency Web site—we determined if agencies' privacy policies addressed this practice. We determined whether or not agencies' privacy policies addressed why the information was collected and how it would be used—for example, "to respond to specific requests." We also noted if the privacy policies identified how long agencies would maintain the collected information and if personal information would be shared with third parties, which OMB's guidance suggests is appropriate. We made the assumption that if visitors were voluntarily submitting information, they would know what information was being collected.

---

<sup>4</sup> An IP address is a string of numbers that the Internet uses to locate individual computers.

<sup>5</sup> A cookie is a file that is placed on a Web user's hard drive by a Web site. The cookie can monitor the user's access of the site, usually without the user's knowledge.



---

## To Determine How Selected Agencies Interpreted Major Entry Point

To determine how selected agencies have interpreted the requirement of the OMB guidance to post privacy policies at major entry points, we contacted officials at 6 of the 70 agencies—the Departments of Commerce, Defense, Justice, and the Interior; the Small Business Administration (SBA); and the Social Security Administration (SSA). We selected these agencies because they had large numbers of Web sites or had frequent contact with the public. We interviewed officials at each of the selected agencies to obtain their criteria for determining which Web pages to designate as major entry points. From these officials, we obtained a list of their major entry points as of May 1, 2000. For five of the six agencies, we visited each Web page the agencies identified as being a major entry point to determine if privacy policies were posted. Because the Department of Defense identified a large number of major entry points, we selected and reviewed a random sample of 59 of their approximately 2,400 major entry points. Our sample was designed to detect, at a 95-percent probability level, if 5 percent or more of the Department-identified major entry Web pages did not have a posted privacy policy. All of the major entry points in our sample had privacy policies posted. These results from our review of this sample indicate, with a high degree of assurance, that the Department consistently posted privacy policies on its identified major entry points.

Because we judgmentally selected the six agencies when we did our review of privacy policies posted at major entry points, we are not able to generalize the results of our work to all federal agencies.

---

## To Determine if Selected Agencies Had Privacy Policies Posted on Web Pages Where They Collect Substantial Personal Information

To determine if selected agencies have posted privacy policies on Web pages where they collect substantial personal information or, when applicable, notices that refer to the Privacy Act of 1974, we first had to define what constituted “substantial” personal information because the OMB memorandum and its guidance did not define it. Therefore, to assess OMB’s requirement that agencies post privacy policies on Web pages where they collect substantial personal information, we developed our own criterion—personal information. To do so, we reviewed the definition of personal information from studies conducted by FTC on private sector Web sites. For purposes of this review, we defined personal information to include an individual’s name, e-mail address, postal address, telephone number, Social Security number, or credit card number.<sup>6</sup> FTC calls this type of information personal identifying information because it can be used to locate or identify an individual.

---

<sup>6</sup> Our definition of personal information is consistent with the elements of personal information identified by FTC in its report to Congress, [Privacy Online: Fair Information Practices in the Electronic Marketplace](#), which was published in May 2000.

Using our definition of personal information, we reviewed the Web sites at agencies designated by the National Performance Review (NPR) as high-impact agencies. According to NPR, these high-impact agencies provide 90 percent of the federal government's contact with the public as well as a wide range of services. NPR identified 32 high-impact agencies. The high-impact agencies consist of components of departments, independent agencies, and one crosscutting issue—acquisition reform. To distinguish them from the 70 agencies we reviewed under our prior objectives, we refer to these as the high-impact agencies. Two of the high-impact agencies are the Veterans Health Administration and Veterans Benefits Administration under the Department of Veterans Affairs. In doing our work, we did not distinguish between these agencies when we searched for pages that collected personal information. We searched the Department's Veterans Benefits and Services Web site ([www.va.gov/vbs/index.htm](http://www.va.gov/vbs/index.htm)) because both agencies linked to this site. Therefore, we counted them as a single high-impact agency, the Department of Veterans Affairs, and limited our review to 31 high-impact agencies. One of NPR's identified high-impact agencies, the Department of Defense's Acquisition Reform, is not an agency, but an initiative under the Office of the Secretary that cuts across all services. However, because NPR identified it as an agency, we retained it on our list of 31 high-impact agencies. We reviewed the Office of the Deputy Under Secretary of Defense for Acquisition Reform's Web site.

For the 31 high-impact agencies, we reviewed the home page of each agency's Web site to determine if there was a posted privacy policy or a link to a privacy policy statement. We then reviewed the privacy policy of each high-impact agency's home page to determine if it addressed the collection of personal information through e-mail and forms. We judgmentally reviewed each of the 31 high-impact agencies' Web sites to locate one instance of e-mail and up to 5 instances of on-line forms that collected personal information.

If we could not locate on-line forms where individuals could submit personal information, we used a site search engine, when available, to search using the word "form." If we found fewer than five on-line forms, a second staff member searched the Web site for additional forms. The e-mail link and the on-line forms that we identified for each high-impact agency may or may not be representative of other e-mail links or on-line forms on the agencies' Web sites.

For each page where we found an e-mail and an on-line form, we noted whether there was a privacy policy or a Privacy Act notice directly on the

page or if there was a clearly labeled link, using the same criteria we used when reviewing principal Web sites, to a privacy policy on the page. We also noted if the high-impact agency had posted privacy policies, or a link to privacy policies, on an intermediary page that an individual would have to view before arriving at the form. In these instances, there was a hyperlink to a privacy policy on the home page of the form or one of the pages an individual would view once he or she had selected a link to input information on the form. Without the specific address of the on-line form, the visitor could not access the on-line form without passing through a prior page. Also, the Privacy Act, which requires agencies to include a privacy notice on forms that collect Privacy Act covered information, permits agencies to meet this requirement by including the notice on a separate page that an individual can detach and retain.

We documented the personal information that a visitor could provide on the Web page. We noted whether the visitor could provide name, e-mail address, postal address, telephone number, Social Security, number and credit card information. In some cases, the form would state that certain information was optional. We collected the information regardless of whether it was optional for the visitor to provide or not. We also noted the purpose for which the agency collected the personal information.

To determine if pages that we identified needed either the OMB required privacy policies or Privacy Act notices posted, we contacted officials at nine judgmentally selected high-impact agencies. The selected high-impact agencies include: Bureau of the Census, Patent and Trademark Office, and International Trade Administration within the Department of Commerce; the Acquisition Reform initiative within the Department of Defense; Bureau of Land Management and National Park Service within the Department of the Interior; Immigration and Naturalization Service within the Department of Justice; SBA; and SSA. We selected these high-impact agencies because they were either the same agencies or components of the agencies we reviewed for the major entry point work. We asked officials of the selected high-impact agencies if the on-line forms we identified as not having privacy policies posted were collecting information that the agencies were maintaining in systems of records, thereby requiring Privacy Act notices. If officials said that they were not maintaining the information collected in systems of records, we discussed if they considered the Web page as needing privacy policies posted as required under the OMB memorandum. In addition, for the selected high-impact agencies, if they had Privacy Act notices posted on forms that we identified, we also

---

determined if the notices contained the elements required under the Privacy Act.<sup>7</sup>

To help ensure accuracy and consistency in our assessments of the agencies' Web pages, a second staff member independently reviewed each Web page.

---

## **To Compare OMB's Memorandum With Selected Statutory Requirements and With Fair Information Principles**

To compare OMB's memorandum and its related guidance with selected statutory requirements that are generally applicable to federal agencies, we researched and reviewed selected statutes and implementing guidance that generally apply to federal agencies in protecting the privacy of information they collect. To compare the OMB memorandum and its related guidance to fair information principles as recently summarized by FTC in its May 2000 report, we reviewed FTC's report and other literature about the fair information principles. We also interviewed OMB officials to obtain their opinion as to how the OMB privacy policy memorandum compared to fair information principles.

We performed our work between January and August 2000, in accordance with generally accepted government auditing standards.

---

<sup>7</sup> The Privacy Act requires agencies to inform individuals whom it asks to supply information the following information on the form which it uses to collect the information: (1) the authority which authorizes the solicitation of the information and whether disclosure is mandatory or voluntary; (2) the principal purpose or purposes for which the information is intended to be used; (3) the routine uses which may be made of the information; and (4) the effects on the individual, if any, of not providing all or any part of the requested information.

# The Names and Internet Addresses of the 70 Executive Branch Agencies Reviewed

<b>Agency</b>	<b>Internet address</b>
Executive Office of the President	<a href="http://www.whitehouse.gov">www.whitehouse.gov</a>
<b>Department</b>	
Agriculture	<a href="http://www.usda.gov">www.usda.gov</a>
Commerce	<a href="http://www.doc.gov">www.doc.gov</a>
Defense	<a href="http://www.defenselink.mil">www.defenselink.mil</a>
Education	<a href="http://www.ed.gov">www.ed.gov</a>
Energy	<a href="http://www.doe.gov">www.doe.gov</a>
Health and Human Services	<a href="http://www.dhhs.gov">www.dhhs.gov</a>
Housing and Urban Development	<a href="http://www.hud.gov">www.hud.gov</a>
Interior	<a href="http://www.doi.gov">www.doi.gov</a>
Justice	<a href="http://www.usdoj.gov">www.usdoj.gov</a>
Labor	<a href="http://www.dol.gov">www.dol.gov</a>
State	<a href="http://www.state.gov">www.state.gov</a>
Transportation	<a href="http://www.dot.gov">www.dot.gov</a>
Treasury	<a href="http://www.treas.gov">www.treas.gov</a>
Veterans Affairs	<a href="http://www.va.gov">www.va.gov</a>
<b>Independent agency</b>	
African Development Foundation	<a href="http://www.adf.gov">www.adf.gov</a>
Central Intelligence Agency	<a href="http://www.cia.gov">www.cia.gov</a>
Commodity Futures Trading Commission	<a href="http://www.cftc.gov">www.cftc.gov</a>
Consumer Product Safety Commission	<a href="http://www.cpsc.gov">www.cpsc.gov</a>
Corporation for National Service	<a href="http://www.cns.gov">www.cns.gov</a>
Defense Nuclear Facilities Safety Board	<a href="http://www.dnfsb.gov">www.dnfsb.gov</a>
Environmental Protection Agency	<a href="http://www.epa.gov">www.epa.gov</a>
Equal Employment Opportunity Commission	<a href="http://www.eeoc.gov">www.eeoc.gov</a>
Export-Import Bank of the United States	<a href="http://www.exim.gov">www.exim.gov</a>
Farm Credit Administration	<a href="http://www.fca.gov">www.fca.gov</a>
Federal Communications Commission	<a href="http://www.fcc.gov">www.fcc.gov</a>
Federal Deposit Insurance Corporation	<a href="http://www.fdic.gov">www.fdic.gov</a>
Federal Election Commission	<a href="http://www.fec.gov">www.fec.gov</a>
Federal Emergency Management Agency	<a href="http://www.fema.gov">www.fema.gov</a>
Federal Housing Finance Board	<a href="http://www.fhfb.gov">www.fhfb.gov</a>
Federal Labor Relations Authority	<a href="http://www.flra.gov">www.flra.gov</a>
Federal Maritime Commission	<a href="http://www.fmc.gov">www.fmc.gov</a>
Federal Mediation and Conciliation Service	<a href="http://www.fmcs.gov">www.fmcs.gov</a>
Federal Mine Safety and Health Review Commission	<a href="http://www.fmshrc.gov">www.fmshrc.gov</a>
Federal Reserve System – Board of Governors	<a href="http://www.bog.frb.fed.us">www.bog.frb.fed.us</a>
Federal Retirement Thrift Investment Board	<a href="http://www.frtib.gov">www.frtib.gov</a>
Federal Trade Commission	<a href="http://www.ftc.gov">www.ftc.gov</a>
General Services Administration	<a href="http://www.gsa.gov">www.gsa.gov</a>
Inter-American Foundation	<a href="http://www.iaf.gov">www.iaf.gov</a>
Merit Systems Protection Board	<a href="http://www.mspb.gov">www.mspb.gov</a>
National Aeronautics and Space Administration	<a href="http://www.nasa.gov">www.nasa.gov</a>
National Archives and Records Administration	<a href="http://www.nara.gov">www.nara.gov</a>
National Capital Planning Commission	<a href="http://www.ncpc.gov">www.ncpc.gov</a>
National Credit Union Administration	<a href="http://www.ncua.gov">www.ncua.gov</a>
National Endowment for the Arts	<a href="http://www.arts.endow.gov">www.arts.endow.gov</a>
National Endowment for the Humanities	<a href="http://www.neh.fed.us">www.neh.fed.us</a>
National Labor Relations Board	<a href="http://www.nlrb.gov">www.nlrb.gov</a>
National Mediation Board	<a href="http://www.nmb.gov">www.nmb.gov</a>

**Appendix II**  
**The Names and Internet Addresses of the 70 Executive Branch Agencies Reviewed**

<b>Agency</b>	<b>Internet address</b>
National Science Foundation	www.nsf.gov
National Transportation Safety Board	www.nts.gov
Nuclear Regulatory Commission	www.nrc.gov
Occupational Safety and Health Review Commission	www.oshrc.gov
Office of Government Ethics	www.usoge.gov
Office of Personnel Management	www.opm.gov
Office of Special Counsel	www.osc.gov
Overseas Private Investment Corporation	www.opic.gov
Peace Corps	www.peacecorps.gov
Pension Benefit Guaranty Corporation	www.pbgc.gov
Postal Rate Commission	www.prc.gov
Railroad Retirement Board	www.rrb.gov
Securities and Exchange Commission	www.sec.gov
Selective Service System	www.sss.gov
Small Business Administration	www.sba.gov
Social Security Administration	www.ssa.gov
Tennessee Valley Authority	www.tva.gov
Trade and Development Agency	www.tda.gov
United States Agency for International Development	www.usaid.gov
United States Commission on Civil Rights	www.usccr.gov
United States International Trade Commission	www.usitc.gov
United States Postal Service <sup>a</sup>	www.usps.com

<sup>a</sup>According to U.S. Postal Service officials, the agency is not required to follow OMB's privacy policies memorandum but voluntarily adheres to the memorandum.

Source: Agency Web pages.

# The Names and Internet Addresses of the High-Impact Agencies Reviewed

High-impact agency	Internet address
Department of Agriculture	
Animal and Plant Health Inspection Service	<a href="http://www.aphis.usda.gov">www.aphis.usda.gov</a>
Food Safety and Inspection Service	<a href="http://www.fsis.usda.gov">www.fsis.usda.gov</a>
Food and Nutrition Service	<a href="http://www.fns.usda.gov">www.fns.usda.gov</a>
Forest Service	<a href="http://www.fs.fed.us">www.fs.fed.us</a>
Department of Commerce	
Bureau of the Census	<a href="http://www.census.gov">www.census.gov</a>
U.S. & Foreign Commercial Trade/ International Trade Administration <sup>a</sup>	<a href="http://www.usatrade.gov">www.usatrade.gov</a>
Patent and Trademark Office	<a href="http://www.uspto.gov">www.uspto.gov</a>
National Weather Service	<a href="http://www.nws.noaa.gov">www.nws.noaa.gov</a>
Department of Defense	
Acquisition Reform <sup>b</sup>	<a href="http://www.acq.osd.mil/ar/ar.htm">www.acq.osd.mil/ar/ar.htm</a>
Department of Education	
Office of Financial Assistance <sup>c</sup>	<a href="http://www.ed.gov">www.ed.gov</a>
Department of Health and Human Services	
Food and Drug Administration	<a href="http://www.fda.gov">www.fda.gov</a>
Administration for Children and Families	<a href="http://www.acf.dhhs.gov">www.acf.dhhs.gov</a>
Health Care Financing Administration	<a href="http://www.hcfa.gov">www.hcfa.gov</a>
Department of the Interior	
National Park Service	<a href="http://www.nps.gov">www.nps.gov</a>
Bureau of Land Management	<a href="http://www.blm.gov">www.blm.gov</a>
Department of Justice	
Immigration and Naturalization Service	<a href="http://www.ins.usdoj.gov">www.ins.usdoj.gov</a>
Department of Labor	
Occupational Safety and Health Administration	<a href="http://www.osha.gov">www.osha.gov</a>
Department of State	
Bureau of Consular Affairs	<a href="http://travel.state.gov">travel.state.gov</a>
Department of Transportation	
Federal Aviation Administration	<a href="http://www.faa.gov">www.faa.gov</a>
Department of the Treasury	
Customs Service	<a href="http://www.customs.ustreas.gov">www.customs.ustreas.gov</a>
Internal Revenue Service	<a href="http://www.irs.ustreas.gov">www.irs.ustreas.gov</a>
Financial Management Service	<a href="http://www.fms.treas.gov">www.fms.treas.gov</a>
Department of Veterans Affairs <sup>d</sup>	
Veterans Health Administration	<a href="http://www.va.gov/About_VA/Orgs/vha/index.htm">www.va.gov/About_VA/Orgs/vha/index.htm</a>
Veterans Benefits Administration	<a href="http://www.vba.va.gov">www.vba.va.gov</a>

**Appendix III**  
**The Names and Internet Addresses of the High-Impact Agencies Reviewed**

<b>High-impact agency</b>	<b>Internet address</b>
Independent Agency	
Environmental Protection Agency	www.epa.gov
Federal Emergency Management Agency	www.fema.gov
General Services Administration	www.gsa.gov
National Aeronautics and Space Administration	www.nasa.gov
Office of Personnel Management	www.opm.gov
Small Business Administration	www.sba.gov
Social Security Administration	www.ssa.gov
United States Postal Service <sup>e</sup>	www.usps.com

<sup>a</sup>We reviewed the Web site of the U.S. Commercial Service, an office within the International Trade Administration.

<sup>b</sup>One of the high-impact agencies, the Department of Defense's acquisition reform, is not an agency, but an initiative under the Office of the Secretary that cuts across all services. We reviewed the Web site for the Office of the Deputy Under Secretary of Defense for Acquisition Reform.

<sup>c</sup>The NPR site lists this agency as the Office of Financial Assistance but the agency's Web site refers to the agency's name as the Office of Student Financial Assistance.

<sup>d</sup>Two of the high-impact agencies--the Veterans Health Administration and the Veterans Benefits Administration—are under the Department of Veterans Affairs. In doing our work, we did not distinguish between these agencies when we searched for pages that collected personal information. We searched the Department's Veterans Benefits and Services Web site ([www.va.gov/vbs/index.htm](http://www.va.gov/vbs/index.htm)) because both agencies linked to this site. Therefore, in this report, we counted these agencies as one, that is--the Department of Veterans Affairs--and discuss only 31 high-impact agencies.

<sup>e</sup>According to U.S. Postal Service officials, the agency is not required to follow OMB's privacy policy memorandum, but it voluntarily adheres to the memorandum.

Source: National Partnership for Reinventing Government Internet Web site located at [www.npr.gov/library/announc/hiapage3.html](http://www.npr.gov/library/announc/hiapage3.html).



# Applicable Laws and Implementing Guidance for Protecting Personal Information

Federal agencies are required by law to protect an individual's right to privacy when they collect personal information. The Privacy Act is the primary law regulating the federal government's collection and maintenance of personal information.<sup>1</sup> Other laws of general application that apply to the protection of personal information collected by the federal government are the Freedom of Information Act (FOIA),<sup>2</sup> the Computer Security Act of 1987,<sup>3</sup> the Paperwork Reduction Act of 1995,<sup>4</sup> and the Computer Matching and Privacy Protection Act of 1988.<sup>5</sup> Appendixes I and III of OMB Circular No. A-130 on the management of federal information resources also provide guidance to executive departments and agencies on protecting personal information.<sup>6</sup> On June 2, 1999, OMB issued Memorandum M-99-18 directing agencies to post privacy policies on federal Web sites. On June 22, 2000, OMB issued Memorandum M-00-13 providing additional guidance relating to the collection of information by federal Web sites. This appendix discusses the Privacy Act and other laws mentioned above that protect personal information, OMB Circular No. A-130, OMB Memorandum M-99-18 and its attached guidance, and OMB Memorandum M-00-13.

## Privacy Act

The Privacy Act places limitations on the collection, use, and dissemination of personally identifiable information maintained by an agency about an individual and contained in an agency's system of records. The Privacy Act defines a "system of records" as any group of records under the control of an agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual. Under the act, an agency cannot disclose any information about an individual contained in a system of records to another person or agency without the prior consent of the individual, unless the disclosure is authorized by law. The Privacy Act authorizes 12 exceptions under which an agency may disclose information in its records. For example, the act authorizes an agency to disclose a

<sup>1</sup> P. L. 93-579, 5 U.S.C. § 552a.

<sup>2</sup> P. L. 89-487, 5 U.S.C. §552.

<sup>3</sup> P. L. 100-235; 15 U.S.C. §§271 note, 272, 278g-3, 278g-4, 278h; 40 U.S.C. §1441.

<sup>4</sup> P. L. 104-13, 44 U.S.C. §3501 *et. seq.*, as amended by the Clinger-Cohen Act of 1996.

<sup>5</sup> P. L. No. 100-503; 5 U.S.C. §§552a(o),- (p), (q), (r), and (s).

<sup>6</sup> Appendix I, "Federal Agency Responsibilities for Maintaining Records about Individuals," provides guidance to agencies for implementation of the Privacy Act; and Appendix III, "Security of Federal Automated Information Resources," among other things, establishes a minimum set of controls to be included in federal automated information security programs and assigns federal agency responsibilities for the security of automated information.

---

record for a routine use, pursuant to an order of a court of competent jurisdiction, or to either House of Congress.<sup>7</sup> The Privacy Act grants individuals the right of access to agency records maintained on themselves; the right to amend that record if it is inaccurate, irrelevant, untimely, or incomplete; and the right to sue the government for violations of the act. The Privacy Act requires an agency to notify an individual when it is collecting information on a form that is to be entered in a system of records of such information as the authority authorizing the solicitation of the information, the principal purpose for which the information is intended to be used, and the routine uses that may be made of the information. When an agency is establishing or revising a system of records, it is required to publish in the Federal Register a notice including such information as the name and location of the system, the categories of individuals on whom records are maintained in the system, and each routine use of the records contained in the system.

---

## Other Selected Statutes

FOIA, as amended, provides that the public has a right of access to federal agency records, except for those records that are protected from disclosure by nine stated exemptions. Two exemptions in FOIA protect personal privacy interests from disclosure. The first exemption allows the federal government to withhold information about individuals in personnel and medical files when the disclosure would constitute a clearly unwarranted invasion of personal privacy. The second exemption allows the federal government to withhold records or information compiled for law enforcement purposes, but only to the extent that the production of such law enforcement records or information could reasonably be expected to constitute an unwarranted invasion of personal privacy.

The Paperwork Reduction Act of 1995 requires the Office of Information and Regulatory Affairs within OMB to provide central guidance for and oversight of federal agencies' information management activities, including activities under the Privacy Act. The Paperwork Reduction Act of 1995 also requires federal agencies to ensure compliance with the Privacy Act and coordinate management of the requirements of FOIA, the Privacy Act, the Computer Security Act, and related information management laws.

The Computer Security Act of 1987, as amended, provides for improving the security and privacy of sensitive information in federal computer systems. The act defines "sensitive information" to include any unclassified information that, if lost, misused, or accessed or modified

---

<sup>7</sup> The Privacy Act defines "routine use" as the use of a record for a purpose that is compatible with the purpose for which it was collected.

without authorization, could adversely affect the national interest, conduct of federal programs, or the privacy to which individuals are entitled under the Privacy Act. The Computer Security Act requires federal agencies to identify their computer systems that contain sensitive information, establish training programs to increase security awareness and knowledge of security practices, and establish a plan for the security and privacy of each computer system with sensitive information. The Computer Security Act also requires the National Institute of Standards and Technology to develop standards and guidelines for the security and privacy of sensitive information in federal computer systems.

The Computer Matching and Privacy Protection Act of 1988 amended the Privacy Act to establish procedural safeguards regarding an agency's use of Privacy Act records in performing certain types of computerized matching programs. The act requires that agencies enter into written agreements specifying the terms under which matches are to be performed. It also provides due process rights for individuals to prevent agencies from taking adverse actions unless they have independently verified the results of a match and given the subject 30 days' advance notice. The act covers matches for the purpose of establishing or verifying initial or continuing eligibility for federal benefits programs or for recouping payments or delinquent debts under federal benefits programs. Appendix 1 to OMB Circular No. A-130 provides guidance to agencies on computer matching programs.

---

## **OMB Circular No. A-130**

OMB Circular No. A-130 establishes policies for the management of federal information resources, as required by the Paperwork Reduction Act of 1980,<sup>8</sup> as amended. The Circular sets forth a number of general policies concerning the protection of personal privacy by the federal government:

- The individual's right of privacy must be protected in federal government information activities involving personal information.<sup>9</sup>
- Agencies shall consider the effects of their actions on the privacy rights of individuals and ensure that appropriate legal and technical safeguards are implemented.<sup>10</sup>
- Agencies have a responsibility to provide information to the public consistent with their missions. Agencies shall discharge this responsibility by providing (a) information as required by law. . . ; and (b) access to

---

<sup>8</sup> P. L. 96-511.

<sup>9</sup> OMB Circular No. A-130, Sec. 7g (Feb. 1996).

<sup>10</sup> OMB Circular No. A-130, Sec. 8a1(i) (Feb. 1996).

agency records under provisions of FOIA and the Privacy Act, subject to the protections and limitations provided for in these Acts.<sup>11</sup>

- Agencies shall limit the collection of information that identifies individuals to that which is legally authorized and necessary for the proper performance of agency functions.<sup>12</sup>
- Agencies shall provide individuals, upon request, access to records about them maintained in Privacy Act systems of records, and permit them to amend such records as are in error consistent with the provisions of the Privacy Act.<sup>13</sup>

In addition, Appendix I to OMB Circular No. A-130 describes agency responsibilities relating to the Privacy Act, as amended by the Computer Matching and Privacy Protection Act of 1988, for maintaining records about individuals. In this regard, Appendix 1 requires the head of the agency to review the following:

- every 2 years, a random sample of agency contracts that provide for the maintenance of a system of records to ensure the contract makes the Privacy Act provision binding on the contractor and his or her employees;
- every 4 years, the routine use disclosures associated with each system of records to ensure the recipient's use of such records are compatible with the purpose for which the disclosing agency collected the information; and
- biennially, agency training practices in order to ensure that agency personnel are familiar with the act and the agency's implementing regulation.<sup>14</sup>

In addition, Appendix III to OMB Circular No. A-130 describes a minimum set of controls to be included in federal automated information security programs; assigns federal agency responsibilities for the security of automated information; and links agency automated information security programs and agency management control systems established in accordance with OMB Circular No. A-123.

---

<sup>11</sup> OMB Circular No. A-130, Sec. 8a5 (Feb. 1996).

<sup>12</sup> OMB Circular No. A-130, Sec. 8a9(b) (Feb. 1996).

<sup>13</sup> OMB Circular No. A-130, Sec. 8a9(d) (Feb. 1996).

<sup>14</sup> See Section 3 of Appendix 1 to OMB Circular No. A-130 for a complete list of reviews an agency is to conduct relating to the Privacy Act.

---

## OMB Privacy Policies for Federal Web Sites

### OMB Memorandum M-99-18

On June 2, 1999, OMB issued Memorandum M-99-18 directing agencies to post privacy policies on their principal Web sites by September 1, 1999. The memorandum also directed agencies to add privacy policies to any known major entry points, as well as to any Web page where substantial personal information is collected from the public by December 1, 1999. The OMB memorandum states “each privacy policy must inform visitors to the site of the following: (1) what information the agency is collecting about individuals; (2) why the agency is collecting the information; and (3) how the agency will use the information.” The OMB memorandum also states that privacy policies must be clearly labeled and easily accessed when an individual visits a Web site.

The OMB memorandum states “federal agencies must protect an individual’s right to privacy when they collect personal information which is required by the Privacy Act and OMB Circular No. A-130.” The memorandum also states “new information technologies offer exciting possibilities for improving the quality and efficiency of government service to the American people” and further states “we cannot realize the potential of the Web until people are confident we protect their privacy when they visit our sites.” The memorandum informed agencies that it was attaching guidance containing model privacy language to assist them in reviewing their existing privacy policies or to use in creating privacy policies.

### Guidance Attached to OMB Memorandum M-99-18

The guidance attached to OMB Memorandum M-99-18 states “every federal Web site must include a privacy policy statement, even if the site does not collect any information resulting in creating a Privacy Act record.” The guidance also states that “federal agencies’ Web sites are highly diverse, have many different purposes, and that agencies must tailor their statement to the information practices of each individual Web site.” The guidance advises agencies on how to prepare privacy policy statements for five different situations: (1) introductory language; (2) information collected and stored automatically; (3) information collected from e-mails and Web forms; (4) security, intrusion, and detection language; and (5) significant actions where information enters a system of records.<sup>15</sup> Finally,

---

<sup>15</sup> The OMB privacy policy guidance uses two headings to describe situation 5—“significant actions where information may be subject to the Privacy Act” and “significant actions where information enters a system of records.” For purposes of consistency in this appendix, we use the heading “significant actions where information enters a system of records.”

the guidance provides examples of model privacy language to assist agencies in drafting their policies.

Concerning the posting of introductory language on agency Web sites, the guidance describes Web sites as “the front door” for many contacts by individuals, and advises agencies to inform individuals about the agencies’ privacy policies concerning the collection and use of information. As examples, the guidance contains language from the White House and the Social Security Administration Web sites. The privacy policy posted on the White House’s Web site states it will not collect any personal information from individuals visiting the Web site unless they choose to provide that information. The Social Security Administration’s Web site informs visitors that under its privacy policy, it will not collect any personally identifiable information from them such as their names, addresses, or Social Security numbers, when they visit its Web site unless they willingly provide such information.

Concerning information that is collected and stored automatically, OMB’s guidance notes that in the course of operating a Web site, certain information may be collected automatically. The OMB guidance advises agencies to make clear to individuals whether they are collecting information automatically and whether they plan to collect more information. The OMB guidance provides language from the White House Web site, which informs visitors that its policy is to collect the Internet domain name, the type of browser and operating system visitors use to access the site, the date and time the site was accessed, and the pages visited. The White House Web site also informs visitors that although it uses the information to make its site more useful to visitors, its policy is not to track or record information about individuals and their visits.

On June 22, 2000, OMB issued Memorandum M-00-13, entitled “Privacy Policies and Data Collection on Federal Web Sites.” The June 22 memorandum refers to the earlier OMB Memorandum, M-99-18, and the need for agencies to comply with this earlier guidance; however, the June 22, 2000, memorandum provides additional guidance relating to the collection of information by federal Web sites using cookies.<sup>16</sup> The guidance attached to OMB Memorandum M-99-18 states that agencies could use automatic means to collect information in logs or cookies. The June 22, 2000 memorandum states that cookies should not be used at federal Web sites unless clear and conspicuous notice is given and the following conditions are met: (1) there is a compelling need to gather the

---

<sup>16</sup> Cookies are files placed on a Web user’s hard drive by a Web site to track the activities of users.

data on the site, (2) the agency takes appropriate and publicly disclosed privacy safeguards for handling information derived from cookies, and (3) the head of the agency has personally approved the use of cookies.

Concerning information collected from e-mails and Web pages, the OMB guidance notes that many Web sites receive identifiable information from e-mails or Web forms and advises agencies to state how they treat the identifiable information. The OMB guidance states “if true, the agency should inform visitors it uses the information included in an e-mail for the purposes for which it was provided and that the information will be destroyed after this purpose has been fulfilled.” The OMB guidance provides sample language to this effect from the FTC privacy policy posted at its Web site. The FTC privacy policy also informs individuals that the material they submit may be seen by various people in the agency and may also be shared with other government agencies enforcing protection, competition, and other laws. The FTC policy informs individuals that in other limited circumstances, such as requests from Congress or private individuals, FTC may be required by law to disclose information submitted by e-mail.

Concerning security, intrusion, and detection language, the OMB guidance notes that many Webmasters use information collected on a site to detect potentially harmful intrusion and to take action once an intrusion is detected. The OMB guidance further notes that in the event of authorized law enforcement investigations, and pursuant to any required legal process, information from those logs and other sources may be used to help identify an individual. The OMB guidance contains language from the Department of Defense’s (DOD) privacy policy posted on its Web site that states “for site security purposes, and to ensure that this service remains available to all users, this government computer system employs software programs to monitor network traffic to identify unauthorized attempts to upload or change information, or otherwise cause damage.” The DOD privacy policy further states “except for authorized law enforcement investigations, no other attempts are made to identify individual users or their usage habits.”

Concerning significant actions where information enters a system of records, the OMB guidance states “to date, a large fraction of federal Web pages have not collected significant amounts of identifiable information in ways that are entered directly into systems of records covered by the Privacy Act.” The OMB guidance informs agencies that in systems of records where traditional paper collections of information are supplemented or replaced by electronic forms offered through a Web site,

---

the rules of the Privacy Act continue to apply. The guidance also states that for those situations where a Privacy Act notice would be required in the paper-based world, it would be appropriate to post a relevant Privacy Act notice on the Web page, or through a well-marked hyperlink.

---

## Analysis

OMB Memorandum M-99-18 and the attached guidance provide supplemental information to agencies to reflect their collection of personal information by new technologies that were not in existence when the Privacy Act became law in 1974. The OMB memorandum recognizes that agencies are required by the Privacy Act to protect an individual's right to privacy when they collect personal information. However, the OMB memorandum and guidance introduce undefined terms, the meaning of which is unclear, and which are not used in the Privacy Act.

OMB Memorandum M-99-18 and the attached guidance introduce two new terms, "substantial personal information" and "significant actions," which are not found in the Privacy Act and OMB Circular No. A-130 and are not defined in OMB Memorandum M-99-18 and its attachment. The OMB memorandum directs agencies to post privacy policies on their principal Web sites and major entry points, as well as any Web pages that collect substantial personal information. However, the attached guidance states that agencies must include a privacy policy statement on every Web site, even if the sites do not collect personal information that would be entered into a system of records that is covered under the Privacy Act. Under the Privacy Act, the controlling authority for information covered by the act is whether it falls within the definition of a system of records, and not whether it is considered to be substantial personal information. Because the term "substantial personal information" is not defined in the OMB memorandum and is not contained in the Privacy Act, it is unclear how agencies decide what personal information is or is not substantial.

The guidance attached to the OMB memorandum also includes a section discussing an agency's Privacy Act obligations in an electronic environment and indicates that the rules of the Privacy Act continue to apply where traditional paper collections of information are supplemented or replaced by electronic forms offered through a Web site. However, the heading for this section indicates that it relates only to "significant actions where information enters a system of records." Since the intended meaning of the phrase "significant actions" is not defined in the memorandum and is thus unclear, an agency could interpret this requirement as distinguishing between significant and nonsignificant actions. Under the Privacy Act, however, personally identifiable information is covered by the act if it is in a system of records. The Privacy



Act does not distinguish between significant or nonsignificant information for the purpose of determining whether information is subject to the Privacy Act.

More generally, the OMB memorandum does not explicitly address the relationship between the requirements of posting Web site privacy policies and an agency's obligations under the Privacy Act. The OMB memorandum directs agencies to post privacy policies that inform individuals about the information the agency is collecting about them, why it is collecting the information, and how it will be used. However, neither the memorandum nor the guidance refers to the more expansive requirements in the Privacy Act for an agency that maintains a system of records to notify individuals who supply information, on a form, of the following:

1. the authority authorizing the solicitation of the information, and whether disclosure of such information is mandatory or voluntary;
2. the principal purpose or purposes for which the information is intended to be used;
3. the routines uses which may be made of the information; and
4. the effects on the individual, if any, for not providing all or any part of the requested information.

The only discussion directly addressing an agency's obligation under the Privacy Act is in the section in the attached guidance entitled "significant actions where information enters a system of records"; and, as noted earlier, the scope of the section is unclear. Accordingly, given the differences between the privacy policy statement required by OMB's memorandum and the notice required by the Privacy Act, we believe that the OMB memorandum may cause agencies confusion.

---

## Conclusion

The Privacy Act of 1974, as amended, requires protection for personal information maintained in a federal agency's systems of records. Other laws, such as FOIA, the Computer Security Act, and the Paperwork Reduction Act support agency compliance with the Privacy Act. On June 2, 1999, OMB issued Memorandum M-99-18 directing federal agencies to post privacy policies on federal Web sites. However, OMB Memorandum M-99-18 and its attached guidance are unclear and introduce two new terms—substantial personal information and significant actions—that are not found in the Privacy Act and OMB Circular No. A-130 and are not defined in the OMB memorandum and guidance. Furthermore, the new terms do

---

not appear to have equivalent terms in the act. These terms and other apparent differences between the OMB Memorandum and the Privacy Act could be confusing to agencies.

# Comparison of Fair Information Principles to the Privacy Act and Other Laws

The Fair Information Practice Principles were first articulated in July 1973 when a Department of Health, Education and Welfare (HEW) Advisory Committee on Automated Personal Data Systems issued a report to the Secretary of HEW entitled “Records, Computers, and the Rights of Citizens.” In this report, the Advisory Committee recommended the enactment of legislation establishing a Code of Fair Information Practice for all automated personal data systems and set forth five basic principles to safeguard requirements for automated personal data systems. The Code of Fair Information Practice predated the Privacy Act of 1974<sup>1</sup> by over a year, and influenced the enactment of the Privacy Act. The Privacy Act is the primary law regulating the federal government’s collection and maintenance of personal information. This appendix discusses fair information practices principles and compares those principles contained in a May 2000 Federal Trade Commission Report to Congress<sup>2</sup> to the requirements imposed by the Privacy Act of 1974, as amended, and other laws of general application that apply to the protection of personal information collected by the federal government.

## Fair Information Practice Principles

The 1973 HEW Advisory Report recommended the enactment of legislation to establish a code of fair information practices for all automated personal data systems containing the following five basic principles:

- There must be no personal data record-keeping systems whose very existence is secret.
- There must be a way for an individual to find out what information about him or her is in a record and how it is used.
- There must be a way for an individual to prevent information about him or her that was obtained for one purpose from being used or made available for other purposes without his or her consent.
- There must be a way for an individual to correct or amend a record of identifiable information about him or her.
- Any organization creating, maintaining, using, or disseminating records of identifiable personal data must assure the reliability of the data for their intended use and must take precautions to prevent misuse of the data.

Since the 1973 report was issued, the fair information practice principles have been used by governmental agencies in the United States, Canada, and Europe. Private sector organizations also have used these principles

<sup>1</sup> Pub. L. No. 93-579, 88 Stat, 1896 (Dec. 31, 1974) (5 U.S.C. § 552a).

<sup>2</sup> Privacy Online: Fair Information Practices In the Electronic Marketplace, Federal Trade Commission report to Congress, May 2000.

---

voluntarily as a means of protecting personal information they have collected. In its May 2000 Privacy Online report, FTC identified the following core principles of privacy protection:

- Notice: Data collectors must disclose their information practices before collecting personal information from consumers.
- Choice: Consumers must be given options with respect to whether and how personal information collected from them may be used for purposes beyond those for which the information was provided.
- Access: Consumers should be able to view and contest the accuracy and completeness of data collected about them.
- Security: Data collectors must take reasonable steps to ensure that information collected from consumers is accurate and secure from unauthorized use.<sup>3</sup>

In its May 2000 report, FTC surveyed commercial Web sites and applied the above principles to them.

---

## The Privacy Act

The Privacy Act places limitations on the collection, use, and dissemination of personally identifiable information about an individual maintained by an agency and contained in an agency's system of records. The Privacy Act defines a "system of records" as any group of records under the control of an agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual. Under the act, an agency cannot disclose any information about an individual contained in a system of records to another person or agency without the prior consent of the individual, unless the disclosure is authorized by law. The Privacy Act authorizes 12 exceptions where an agency may disclose personally identifiable information in an agency's records. For example, the act authorizes an agency to disclose a record for a routine use,<sup>4</sup> pursuant to an order of a court of competent jurisdiction, or to either House of Congress. The Privacy Act grants individuals the right of access to agency records pertaining to themselves; the right to amend that record if it is inaccurate, irrelevant, untimely, or incomplete; and the right to sue the government for violations of the act. The Privacy Act requires an agency to inform an individual from whom it is collecting information that is to be entered in a system of records on the form used to collect the information or on a separate form to be retained by the individual of: (1) the authority

---

<sup>3</sup> Privacy Online, p. 4.

<sup>4</sup> The Privacy Act defines "routine use" as the use of a record for a purpose that is compatible with the purpose for which it was collected.

---

authorizing the solicitation of the information and whether disclosure of such information is mandatory or voluntary, (2) the principal purpose for which the information is intended to be used, (3) the routine uses which may be made of the information, and (4) the effects on the individual for not providing all or any part of the information. When an agency is establishing or revising a system of records, it is required to publish in the Federal Register a notice including such information as the name and location of the system, the categories of individuals on whom records are maintained in the system, and each routine use of the records contained in the system.

---

## Analysis

The core principles from the July 1973 Advisory Report entitled “Records, Computers, and the Rights of Citizens” are identified as the source for the concepts embodied in the Privacy Act of 1974.<sup>5</sup> Although the Privacy Act and other laws do generally reflect most of the fair information practice principles, as discussed below, two major aspects of the act—the system of records requirement and the statutory exceptions for disclosure—result in differences in the application of the Privacy Act and the fair information principles, particularly with respect to the choice principle.

Notice is the first principle articulated in the FTC report. Under the notice principle, data collectors must disclose their information practices before collecting personal information from consumers. With regard to this principle, the FTC May 2000 report states the following:

“... consumers should be given clear and conspicuous notice of an entity’s information practices before any personal information is collected from them, including: identification of the entity collecting the data, the uses to which the data will be put, and the recipients of the data; the nature of the data collected and the means by which it is collected; whether provision of the requested data is voluntary or required; and the steps taken by the data collector to ensure the confidentiality, integrity and quality of the data.”<sup>6</sup>

Personal information subject to the fair information practice principle may not be subject to the Privacy Act, because only personally identifiable information that is contained in an agencies’ system of records is subject to the Privacy Act. However, for personal information contained in an agency’s system of records, the Privacy Act contains notice requirements similar to those stated in the notice principle. As discussed above, under the Privacy Act, an agency is required to provide notice in two situations. An agency is required to notify an individual of specific information when

---

<sup>5</sup> Personal Privacy in an Information Society: The Report of the Privacy Protection Study Commission, July 1977, p. 501.

<sup>6</sup> Privacy Online, p. 14.

---

it is collecting information, on a form, that is to be entered in a system of records. Additionally, the Privacy Act requires an agency to publish in the Federal Register a notice concerning the establishment or revision of the existence and character of a system of records.

The choice principle, the second principle articulated in the FTC report, provides that consumers must be given options with respect to whether and how personal information collected from them may be used for purposes beyond the use for which the information was provided. The FTC May 2000 report states:

“Under the choice principle, data collectors must afford consumers an opportunity to consent to secondary uses of their personal information, such as the placement of a consumer’s name on a list for marketing additional products or the transfer of personal information to entities other than the data collector.”<sup>7</sup>

Under the Privacy Act, an individual is provided some choice as to whether there will be a subsequent disclosure of his or her personally identifiable information that is contained in an agency’s system of records. In this regard, the Privacy Act provides that an agency cannot disclose a record contained in a system of records to any person, or to another agency, without the prior written consent of the individual to whom the record pertains, unless the disclosure is authorized by law. Thus, for any disclosure not authorized by law, the Privacy Act provides an individual with a choice as to whether his or her personal information will be disclosed. However, with respect to any disclosure that is authorized by law, the individual has no choice concerning an agency’s authority to disclose the individual’s personally identifiable information. The act authorizes an agency to disclose personally identifiable information contained in an agency’s system of records in the following 12 situations:

- to those officers and employees of the agency who maintain the record and have a need for the record in the performance of their duties;
- if required under 5 U.S.C. §552 (the Freedom of Information Act);
- for a routine use as defined in the act;
- to the Bureau of the Census for purposes of planning or carrying out a census, survey, or related activity pursuant to the provisions of Title 13;

---

<sup>7</sup>Privacy Online, p. 15.

- 
- to a recipient who has provided the agency with advance adequate written assurance that the record will be used solely as a statistical research or reporting record, and the record is to be transferred in a form that is not individually identifiable;
  - to the National Archives and Records Administration as a record that has sufficient historical or other value to warrant its continued preservation by the United States Government, or by evaluation by the Archivist of the United States to determine whether the record has such value;
  - to another agency or instrumentality of any governmental jurisdiction within or under the control of the United States for a civil or criminal law enforcement activity, if the activity is authorized by law, and the head of the agency or instrumentality has made a written request to the agency maintaining the record specifying the particular portion desired and the law enforcement activity for which the record is sought;
  - to a person pursuant to a showing of compelling circumstances affecting the health or safety of an individual;
  - to either House of Congress, or to the extent of matter within its jurisdiction, any committee or subcommittee thereof, any joint committee of Congress, or subcommittee of any such joint committee;
  - to the Comptroller General, or any of his authorized representatives, in the course of the performance of the duties of the General Accounting Office;
  - pursuant to an order of a court of competent jurisdiction; or
  - to a consumer reporting agency.

The access principle is the third principle articulated in the FTC report. Under this principle, access refers to an individual's ability to both access data about him or herself—i.e., to view the data in an entity's file—and to contest that data's accuracy and completeness.<sup>8</sup> The access principle is contained in the Privacy Act. Under the Privacy Act, any agency that maintains a system of records is required upon a request by an individual to allow the individual to gain access to his or her record, to review the record, copy any or all of it, and request an amendment of the record if it is incorrect.

---

<sup>8</sup> [Privacy Online](#) p. 16.

Security is the last principle articulated in the FTC May 2000 report. The FTC report describes security as a data collector's obligation to protect personal information against unauthorized access, use or disclosure, and loss or destruction.<sup>9</sup> The implementation of the security principle lies with the data collector. The Privacy Act also contains requirements to protect personally identifiable information contained in an agency's systems of records. Specifically, the Privacy Act requires an agency to establish appropriate administrative, technical, and physical safeguards to ensure the security and confidentiality of records and to protect against anticipated threats or hazards to their security or integrity that could result in substantial harm, embarrassment, inconvenience, or unfairness to any individual on whom information is maintained. The Privacy Act also requires an agency to maintain for most systems of records an accounting of the date, nature and purpose of each disclosure of a record, and the name and address of the person or agency to whom the disclosure is made.<sup>10</sup> In addition, other laws, such as the Paperwork Reduction Act of 1995<sup>11</sup> and the Computer Security Act of 1987,<sup>12</sup> require agencies to protect sensitive and critical information. Under the Paperwork Reduction Act, the Office of Management and Budget is responsible for developing security guidance and overseeing agency practices. Under the Computer Security Act, the National Institute of Standards and Technology is responsible for developing technical and providing related guidance.

---

## Conclusion

The five core principles contained in a July 1973 Department of HEW Advisory Committee Report entitled "Records, Computers, and the Rights of Citizens" influenced the enactment of the Privacy Act of 1974. Although the Privacy Act and other federal laws do generally contain most of the fair information practice principles, the system of records requirement and the statutory exceptions for disclosure in the Privacy Act result in differences in the application between the Privacy Act and the fair information practice principles.

---

<sup>9</sup>Privacy Online: p. 18.

<sup>10</sup> The Privacy Act exempts from the accounting requirement those disclosures authorized by the act that are made to officers and employees of the agency who maintain the record and have a need for it in the performance of their duties and disclosures required by the Freedom of Information Act. See 5 U.S.C. § 552a(c).

<sup>11</sup> Pub. L. No. 104-13, 44 U.S.C. § 3501 et. seq., as amended by the Clinger-Cohen Act of 1996.

<sup>12</sup> Pub. L. No. 100-235; 15 U.S.C. §§ 271 note, 272, 278g-3, 278-4, 278h; 40 U.S.C. § 1441.



# Comments From the Office of Management and Budget



EXECUTIVE OFFICE OF THE PRESIDENT  
OFFICE OF MANAGEMENT AND BUDGET  
WASHINGTON, D.C. 20503

DEPUTY DIRECTOR  
FOR MANAGEMENT

August 30, 2000

Michael Brostek  
Associate Director of Federal Management  
and Workforce Issues  
General Accounting Office  
Washington, DC 20548

Dear Mr. Brostek:

Thank you for the opportunity to comment on GAO's draft report, "Internet Privacy: Agencies' Efforts to Implement OMB's Privacy Policies."

This report addresses a subject that is very important to this Administration – the protection of personal privacy online. We appreciate the work that GAO has performed in the area of federal website privacy. However, we believe that the recitation of the numerous findings in the report do not adequately reflect the significant progress that the federal agencies have made in this area.

Last spring, in response to questions and concerns raised by the public about federal agency use of personal information collected online, OMB Director Jack Lew issued Memorandum M99-18 -- Privacy Policies on Federal Websites. In that memorandum, OMB directed federal agencies to post privacy policies on key web pages on agency websites. The executive branch agencies implemented the OMB memorandum with great success. As the draft GAO report illustrates, agencies have now adopted privacy policies at the most important web pages on their sites, with a virtually perfect record at agency principal websites and at major points of entry.<sup>1</sup> This success is all the more impressive because it occurred when agencies were also occupied with intensive Y2K preparations.

In short, we are pleased that OMB was able to respond in short order to a concern about privacy protection on government websites, and that privacy policies now appear governmentwide on web pages where public users may have the most questions. We recognize that work is not complete in this area and continue to work with agencies to improve compliance where necessary.

---

<sup>1</sup> When GAO conducted its review of the principal websites at 70 agencies, 69 of them had a privacy policy posted. In addition, GAO identified 2,692 major points of entry on six agencies' websites -- *all but 9* had privacy policies posted.

See comment 1.

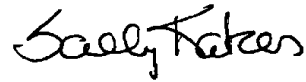
See comment 2.

The draft GAO report contains a number of recommendations for OMB. Several recommendations pertain to clarifying the OMB guidance. The draft report also recommends that we develop an oversight strategy for ensuring agencies' adherence to OMB's website privacy policies, including the requirement to post Privacy Act notices on websites when applicable.

The OMB guidance was developed with input from agencies and the CIO Council, and efforts to ensure compliance involved these entities as well. We expect to present the GAO recommendations to the agencies and the CIO Council in order to elicit their response about the specific recommendations and the need for an overall oversight strategy.

We look forward to continuing our work in this area and appreciate your interest in our progress.

Sincerely,



Sally Katzen  
Deputy Director for Management

---

The following are GAO's comments on the Office of Management and Budget's (OMB) letter.

---

## GAO Comments

1. Although OMB states that our report illustrates that agencies have a virtually perfect record adopting privacy policies at major points of entry, our review focused only on the major entry points of six selected agencies. Thus, the results cannot be generalized to all federal agencies.

2. OMB states that all but 9 of 2,692 Web pages that agencies considered to be major entry points had privacy policies posted. However, we did not review all the Web pages identified by all six agencies as major entry points. As we point out in our report, although we reviewed all the major entry points identified by 5 of the agencies, we reviewed only a sample of 59 of the 2,401 Web pages identified by the Department of Defense. We estimate that if there are any major entry points at the Department of Defense without privacy policies posted, the number does not exceed 5 percent of all the Department's major entry points. Thus, there could be as many as 120 Web pages that do not have privacy policies posted.

# GAO Contacts and Staff Acknowledgments

---

## GAO Contacts

Michael Brostek (202) 512-8676

Linda J. Libician (214) 777-5709

---

## Acknowledgments

In addition to the individuals named above, Judith Collins, Susan Michal-Smith, David Plocher, James Rose, Kiki Theodoropoulos, James W. Turkett, and Leigh White, made key contributions to this report.

---

---

---

### **Ordering Copies of GAO Reports**

**The first copy of each GAO report and testimony is free. Additional copies are \$2 each. Orders should be sent to the following address, accompanied by a check or money order made out to the Superintendent of Documents, when necessary. VISA and MasterCard credit cards are accepted, also. Orders for 100 or more copies to be mailed to a single address are discounted 25 percent.**

**Order by mail:**

**U.S. General Accounting Office  
P.O. Box 37050  
Washington, DC 20013**

**or visit:**

**Room 1100  
700 4<sup>th</sup> St. NW (corner of 4<sup>th</sup> and G Sts. NW)  
U.S. General Accounting Office  
Washington, DC**

**Orders may also be placed by calling (202) 512-6000 or by using fax number (202) 512-6061, or TDD (202) 512-2537.**

**Each day, GAO issues a list of newly available reports and testimony. To receive facsimile copies of the daily list or any list from the past 30 days, please call (202) 512-6000 using a touch-tone phone. A recorded menu will provide information on how to obtain these lists.**

### **Viewing GAO Reports on the Internet**

**For information on how to access GAO reports on the INTERNET, send e-mail message with "info" in the body to:**

**info@www.gao.gov**

**or visit GAO's World Wide Web Home Page at:**

**http://www.gao.gov**

### **Reporting Fraud, Waste, and Abuse in Federal Programs**

**To contact GAO FraudNET use:**

**Web site: <http://www.gao.gov/fraudnet/fraudnet.htm>**

**E-Mail: [fraudnet@gao.gov](mailto:fraudnet@gao.gov)**

**Telephone: 1-800-424-5454 (automated answering system)**

---

---

---

**United States  
General Accounting Office  
Washington, D.C. 20548-0001**

**Bulk Rate  
Postage & Fees Paid  
GAO  
Permit No. G100**

**Official Business  
Penalty for Private Use \$300**

**Address Correction Requested**

---

