United States Government Accountability Office

GAO

Testimony
Before the Subcommittee on Information Policy, Census, and National Archives, Committee on Oversight and Government Reform

For Release on Delivery
Expected at 2 p.m. EDT
Tuesday, March 11, 2008

PRIVACY

Government Use of Data from Information Resellers Could Include Better Protections

Statement of Linda D. Koontz, Director
Information Management Issues

March 11, 2008

PRIVACY

Government Use of Data from Information Resellers Could Include Better Protections

GAO Accountability • Integrity • Reliability

Highlights

Highlights of GAO-08-543T, a testimony before Subcommittee on Information Policy, Census, and National Archives, Committee on Oversight and Government Reform

Why GAO Did This Study

Federal agencies collect and use personal information for various purposes from information resellers—companies that amass and sell data from many sources. GAO was asked to testify on its April 2006 report on agency use of reseller data. For that report, GAO was asked to determine how the Departments of Justice, Homeland Security, and State and the Social Security Administration used personal data from resellers and to review the extent to which agencies' policies and practices for handling this information reflected the Fair Information Practices, a set of widely accepted principles for protecting the privacy and security of personal data. GAO was also asked to provide an update on the implementation status of its recommendations and to comment on provisions of the proposed Federal Agency Data Protection Act. In preparing this testimony, GAO relied primarily on its April 2006 report.

What GAO Recommends

GAO is not making additional recommendations at this time. However, in its 2006 report, GAO made recommendations to the Office of Management and Budget and the four agencies to address agency use of personal information from commercial sources. Agency officials generally agreed with the content of the report. Since then, 2 of the 4 agencies have taken steps to address its recommendations; however, OMB has not issued clarified guidance.

To view the full product, including the scope and methodology, click on GAO-08-543T. For more information, contact Linda Koontz at (202) 512-6240 or KoontzL@gao.gov.

What GAO Found

In fiscal year 2005, the Departments of Justice, Homeland Security, and State and the Social Security Administration reported that they used personal information obtained from resellers for a variety of purposes, including performing criminal investigations, locating witnesses and fugitives, researching assets held by individuals of interest, and detecting prescription drug fraud. The agencies planned spending approximately $30 million on contractual arrangements with resellers that enabled the acquisition and use of such information. About 91 percent of the planned fiscal year 2005 spending was for law enforcement (69 percent) or counterterrorism (22 percent).

Agency practices for handling personal information acquired from information resellers did not always fully reflect the Fair Information Practices. That is, for some of these principles, agency practices were uneven. For example, although agencies issued public notices when they systematically collected personal information, these notices did not always notify the public that information resellers were among the sources to be used. This practice is not consistent with the principle that individuals should be informed about privacy policies and the collection of information. Contributing to the uneven application of the Fair Information Practices are ambiguities in guidance from the Office of Management and Budget (OMB) regarding the applicability of privacy requirements to federal agency uses of reseller information. In addition, agencies generally lacked policies that specifically address these uses.

GAO made recommendations to OMB to revise privacy guidance and to the four agencies to develop specific policies for the use of personal information from resellers. The five agencies generally agreed with the report and described actions initiated to address the recommendations. Since GAO issued its report, agencies have taken steps to address the recommendations. For example, the Department of Homeland Security Privacy Office incorporated specific questions in its May 2007 Privacy Impact Assessment guidance concerning use of commercial data. In addition, the Department of Justice took steps to update its public notices to specify their use of data from information resellers. OMB, however, has not implemented GAO's recommendation to clarify guidance on use of commercial data.

The Federal Agency Data Protection Act was introduced on December 18, 2007. The legislation, among other things would require that agencies (1) conduct privacy impact assessments for their uses of commercial data, and (2) promulgate regulations concerning the use of commercial data brokers. GAO considers these requirements to be consistent with the results and the recommendations made to the agencies in its 2006 report

Abbreviations

DEA	Drug Enforcement Administration
DHS	Department of Homeland Security
DOJ	Department of Justice
FBI	Federal Bureau of Investigation
OECD	Organization for Economic Cooperation and Development
OIG	Office of the Inspector General
OMB	Office of Management and Budget
PIA	privacy impact assessments
SSA	Social Security Administration
State	Department of State
TSA	Transportation Security Administration

Mr. Chairman and Members of the Subcommittee:

I appreciate the opportunity to discuss critical issues surrounding the federal government's purchase of personal information[1] from businesses known as information resellers. As you are aware, the ease and speed with which people's personal information can be collected by information resellers from a wide variety of sources and made available to government and other customers has accelerated with technological advances. In recent years, security breaches at large information resellers such as ChoicePoint and LexisNexis have raised questions about how resellers and their federal customers handle people's personal information—and especially whether their practices are fully consistent with widely accepted practices for protecting the privacy and security of personal information.

Federal agency use of personal information is governed primarily by the E-Government Act of 2002 and the Privacy Act of 1974. The E-Government Act of 2002 strives to enhance protection for personal information in government information systems by requiring that agencies conduct privacy impact assessments (PIA). A PIA is an analysis of how personal information is collected, stored, shared, and managed in a federal system. The Privacy Act of 1974[2] requires that the use of personal information be limited to predefined purposes and involve only information germane to those purposes. The provisions of the Privacy Act, in turn, are largely based on a set of principles for protecting the privacy and security of personal information, known as the Fair Information Practices, which were

[1]For purposes of this report, the term personal information is defined as any information about an individual maintained by an agency, including (1) any information that can be used to distinguish or trace an individual's identity, such as name, Social Security number, date and place of birth, mother's maiden name, or biometric records, and (2) any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information.

[2]The Privacy Act of 1974, Pub. L. No. 93-579, 88 Stat. 1896 (codified as amended at 5 U.S.C. § 552a) provides safeguards against an invasion of privacy through the misuse of records by federal agencies and allows citizens to learn how their personal information is collected, maintained, used, and disseminated by the federal government.

first proposed in 1973 by a U.S. government advisory committee.[3] These principles, now widely accepted, include

1. collection limitation,
2. data quality,
3. purpose specification,
4. use limitation,
5. security safeguards,
6. openness,
7. individual participation, and
8. accountability.[4]

These principles, with some variation, are used by organizations to address privacy considerations in their business practices and are also the basis of privacy laws and related policies in many countries, including the United States, Germany, Sweden, Australia, and New Zealand, as well as the European Union.

As agreed, my testimony today will be based primarily on the agency information contained in a report we issued in April 2006.[5] For that report, we analyzed fiscal year 2005 contracts and other vehicles for the acquisition of personal information from information resellers by the Departments of Justice (DOJ), Homeland Security (DHS), and State (State) and the Social Security Administration (SSA). We compared relevant agency guidelines and management policies and

[3]Congress used the committee's final report as a basis for crafting the Privacy Act of 1974. See U.S. Department of Health, Education, and Welfare, *Records, Computers, and the Rights of Citizens: Report of the Secretary's Advisory Committee on Automated Personal Data Systems* (Washington, D.C.; July 1973).

[4]Descriptions of these principles are shown in table 1.

[5]GAO, *Personal Information: Agency and Reseller Adherence to Key Privacy Principles*, GAO-06-421 (Washington, D.C.: Apr. 4, 2006).

procedures to the Fair Information Practices. We also updated the implementation status of recommendations contained in our 2006 report and analyzed provisions of the proposed Federal Agency Data Protection Act.[6] Our work was performed in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Today, after a brief summary of the laws that govern agency use of personal information, I will summarize the information contained in our 2006 report on how the selected agencies used the personal information that they purchased from resellers and the extent to which the agencies had policies and practices that reflected the Fair Information Practices. I will also provide an update on steps taken by the agencies to address the recommendations contained in our 2006 report. Finally, I will comment on specific privacy related provisions of the proposed Federal Agency Data Protection Act.

Results in Brief

In fiscal year 2005, DOJ, DHS, State, and SSA reported that they planned to spend a combined total of approximately $30 million[7] to purchase personal information from resellers. The vast majority—approximately 91 percent—of the planned spending was for purposes of law enforcement (69 percent) or counterterrorism (22

[6]H.R. 4791, Federal Agency Data Protection Act, 110th Cong., introduced by Representative Wm. Lacy Clay, December 18, 2007.

[7]This figure may include uses that do not involve personal information. Except for instances where the reported use was primarily for legal research, agency officials were unable to separate the dollar values associated with use of personal information from uses for other purposes (for example, LexisNexis and West provide news and legal research in addition to public records). The four agencies obtained personal information from resellers primarily through two general-purpose governmentwide contract vehicles—the Federal Supply Schedule of the General Services Administration and the Library of Congress's Federal Library and Information Network.

percent). For example, components of DOJ (the largest user of resellers) used the information for criminal investigations, locating witnesses and fugitives, researching assets held by individuals of interest, and detecting fraud in prescription drug transactions. DHS acquired personal information to aid its immigration fraud detection and border screening programs. SSA and State purchased personal information from information resellers to detect and investigate fraud, verify identities, and determine benefits eligibility.

Agency practices for handling personal information acquired from information resellers reflected four of eight principles established by the Fair Information Practices. Agency practices generally reflected the *collection limitation*, *data quality*, *use limitation*, and *security safeguards* principles. For example, law enforcement agencies (including the Federal Bureau of Investigation and the U.S. Secret Service) generally reported that they corroborate information obtained from resellers to ensure that it is accurate when it is used as part of an investigation, reflecting the *data quality* principle that data should be accurate, current, and complete, as needed for the defined purpose. However, agencies did not always have practices for handling reseller information to fully address the *purpose specification*, *individual participation*, *openness*, and *accountability* principles. For example:

- Although agencies notified the public through *Federal Register* notices and published PIAs that they collected personal information from various sources, they did not always indicate specifically that information resellers were among those sources.
- Some agencies lacked robust audit mechanisms to ensure that use of personal information from information resellers was for permissible purposes, reflecting an uneven application of the *accountability* principle.

Contributing to agencies' uneven application of the Fair Information Practices were ambiguities in guidance from the Office of Management and Budget (OMB) on how privacy requirements apply to federal agency uses of reseller information. In addition, agencies generally lacked policies that specifically address these uses.

We made recommendations to OMB to revise privacy guidance and to the four agencies to develop specific policies for the use of personal information from resellers. The agencies generally agreed with the report and described actions initiated to address our recommendations. Since we issued our report, two of the four agencies have taken steps to address our recommendations. For example, the DHS Privacy Office incorporated specific questions in its May 2007 PIA guidance concerning use of commercial data. In addition, DOJ took steps to ensure that their system-of-records notices specifically reference their use of data from information resellers. OMB, however, has not implemented our recommendation to clarify guidance on use of commercial data.

On December 18, 2007, the Federal Agency Data Protection Act was introduced. This legislation, among other things would require that agencies (1) conduct PIAs for their uses of commercial data and (2) promulgate regulations concerning the use of commercial data brokers. We believe that these requirements are consistent with the results of our 2006 report and the recommendations we made to the agencies.

Background

Before advanced computerized techniques, obtaining people's personal information usually required visiting courthouses or other government facilities to inspect paper-based public records, and information contained in product registrations and other business records was not generally available at all. Automation of the collection and aggregation of multiple-source data, combined with the ease and speed of its retrieval, have dramatically reduced the time and effort needed to obtain such information. Information resellers provide services based on these technological advances.

We use the term "information resellers" to refer to businesses that vary in many ways but have in common collecting and aggregating personal information from multiple sources and making it available to their customers. These businesses do not all focus exclusively on aggregating and reselling personal information. For example, Dun &

Bradstreet primarily provides information on commercial enterprises for the purpose of contributing to decision making regarding those enterprises. In doing so, it may supply personal information about individuals associated with those commercial enterprises. To a certain extent, the activities of information resellers may also overlap with the functions of consumer reporting agencies, also known as credit bureaus—entities that collect and sell information about individuals' creditworthiness, among other things. To the extent that information resellers perform the functions of consumer reporting agencies, they are subject to legislation specifically addressing that industry, particularly the Fair Credit Reporting Act.

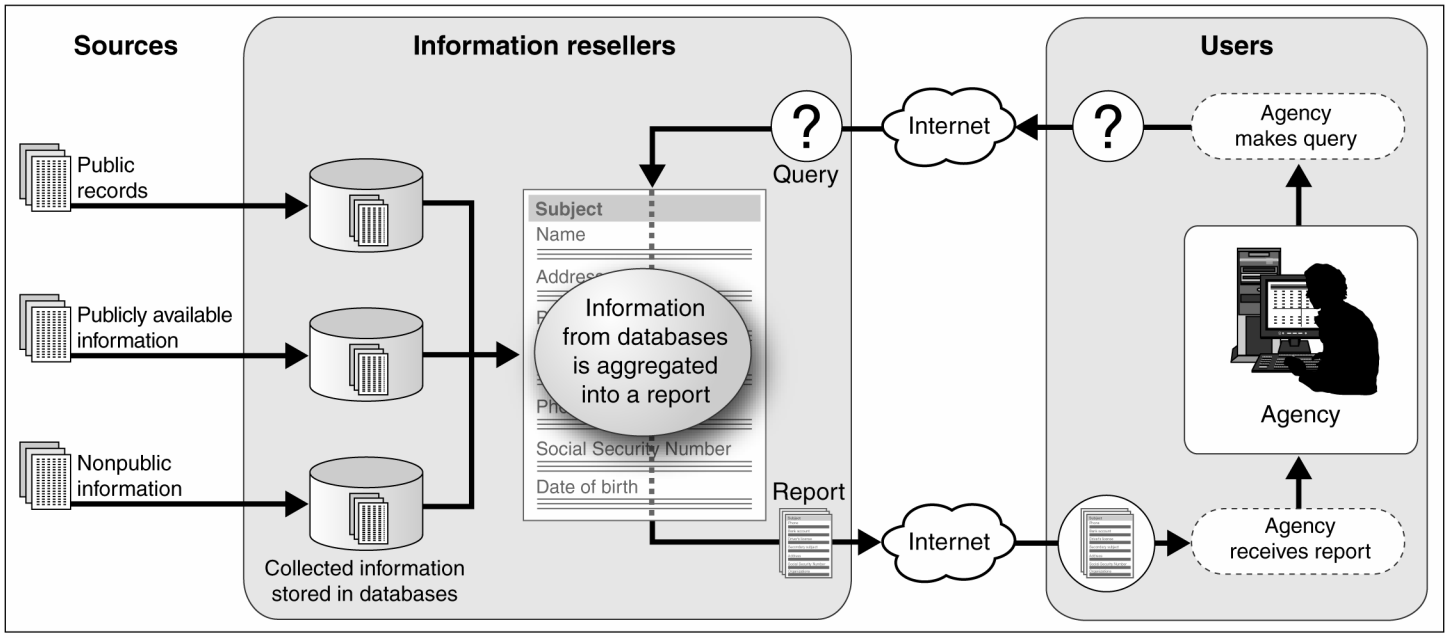
Information resellers have now amassed extensive amounts of personal information about large numbers of Americans. They supply it to customers in both government and the private sector, typically via a centralized online resource. Generally, three types of information are collected:

- *Public records* such as birth and death records, property records, motor vehicle and voter registrations, criminal records, and civil case files.
- *Publicly available information* not found in public records but nevertheless publicly available through other sources, such as telephone directories, business directories, classified ads or magazines, Internet sites, and other sources accessible by the general public.
- *Nonpublic information* derived from proprietary or nonpublic sources, such as credit header data,[8] product warranty registrations, and other application information provided to private businesses directly by consumers.

[8]Credit header data are the nonfinancial identifying information located at the top of a credit report, such as name, current and prior addresses, telephone number, and Social Security number.

Figure 1 illustrates how these types of information are collected and aggregated into reports that are ultimately accessed by customers, including government agencies.

Figure 1: Typical Information Flow through Resellers to Government Customers



Source: GAO analysis of information reseller and agency-provided data.

Federal Laws and Guidance Govern Use of Personal Information in Federal Agencies

No single federal law governs all use or disclosure of personal information. The major requirements for the protection of personal privacy by federal agencies come from the Privacy Act of 1974 and the privacy provisions of the E-Government Act of 2002.

Federal use of personal information is governed primarily by the Privacy Act of 1974,[9] which places limitations on agencies'

[9]The Privacy Act of 1974, Pub. L. No. 93-579, 88 Stat. 1896 (codified as amended at 5 U.S.C. § 552a) provides safeguards against an invasion of privacy through the misuse of records by federal agencies and allows citizens to learn how their personal information is collected, maintained, used, and disseminated by the federal government.

collection, disclosure, and use of personal information maintained in systems of records. The act describes a "record" as any item, collection, or grouping of information about an individual that is maintained by an agency and contains his or her name or another personal identifier. It also defines "system of records" as a group of records under the control of any agency from which information is retrieved by the name of the individual or by an individual identifier. The Privacy Act requires that when agencies establish or make changes to a system of records, they must notify the public by placing a notice in the *Federal Register* identifying, among other things, the type of data collected, the types of individuals about whom the information is collected, the routine uses[10] of the data, and procedures that individuals can use to review and correct their personal information. Additional provisions of the Privacy Act are discussed in the 2006 report.

The E-Government Act of 2002 requires that agencies conduct PIAs. A PIA is an analysis of how personal information is collected, stored, shared, and managed in a federal system. Under the E-Government Act and related OMB guidance, agencies must conduct PIAs (1) before developing or procuring information technology that collects, maintains, or disseminates information that is in a personally identifiable form; (2) before initiating any new data collections involving personal information that will be collected, maintained, or disseminated using information technology if the same questions are asked of 10 or more people; or (3) when a system change creates new privacy risks, for example, by changing the way in which personal information is being used.

OMB is tasked with providing guidance to agencies on how to implement the provisions of the Privacy Act and the E-Government Act and has done so, beginning with guidance on the Privacy Act,

[10]Under the Privacy Act of 1974, the term "routine use" means (with respect to the disclosure of a record) the use of such a record for a purpose that is compatible with the purpose for which it was collected. 5 U.S.C. § 552a (a(7)).

issued in 1975.[11] OMB's guidance on implementing the privacy provisions of the E-Government Act of 2002 identifies circumstances under which agencies must conduct PIAs and explains how to conduct them.

The PIA mandate in the E-Government Act of 2002 provided a mechanism by which agencies can consider privacy in the earliest stages of system development. PIAs can be an important tool to help agencies to address *openness and purpose specification* principles early in the process of developing new information systems. To the extent that PIAs are made publicly available,[12] they provide explanations to the public about such things as the information that will be collected, why it is being collected, how it is to be used, and how the system and data will be maintained and protected.

The Fair Information Practices Are Widely Agreed to Be Key Principles for Privacy Protection

The Privacy Act of 1974 is largely based on a set of internationally recognized principles for protecting the privacy and security of personal information known as the Fair Information Practices. A U.S. government advisory committee first proposed the practices in 1973 to address what it termed a poor level of protection afforded to privacy under contemporary law.[13] The Organization for Economic Cooperation and Development (OECD)[14] developed a revised

[11]OMB, "Privacy Act Implementation: Guidelines and Responsibilities," *Federal Register*, Volume 40, Number 132, Part III, pages 28948-28978 (Washington, D.C.; July 9, 1975). Since the initial Privacy Act guidance of 1975, OMB has periodically published additional guidance. Further information regarding OMB Privacy Act guidance can be found on the OMB Web site at http://www.whitehouse.gov/omb/inforeg/infopoltech.html.

[12]The E-Government Act requires agencies, if practicable, to make PIAs publicly available through agency Web sites, publication in the *Federal Register* or by other means. Pub. L. No. 107-347, § 208 (b)(1)(B)(iii).

[13]U.S. Department of Health, Education, and Welfare, *Records, Computers and the Rights of Citizens*.

[14]OECD, *Guidelines on the Protection of Privacy and Transborder Flow of Personal Data* (Sept. 23, 1980). The OECD plays a prominent role in fostering good governance in the public service and in corporate activity among its 30 member countries. It produces internationally agreed-upon instruments, decisions, and recommendations to promote rules in areas where multilateral agreement is necessary for individual countries to make progress in the global economy.

version of the Fair Information Practices in 1980. This version of the principles was reaffirmed by OECD ministers in a 1998 declaration and further endorsed in a 2006 OECD report.[15] The Fair Information Practices, have, with some variation, formed the basis of privacy laws and related policies in many countries, including the United States, Germany, Sweden, Australia, and New Zealand, as well as the European Union.[16]

In addition, in its 2007 report, *Engaging Privacy and Information Technology in a Digital Age*, the National Research Council[17] found that the principles of fair information practice for the protection of personal information are as relevant today as they were in 1973. Accordingly, the committee recommended that the Fair Information Practices should be extended as far as reasonably feasible to apply to private sector organizations that collect and use personal information. The eight principles of the OECD Fair Information Practices are shown in table 1.

Table 1: The OECD Fair Information Practices

Principle	Description
Collection limitation	The collection of personal information should be limited, should be obtained by lawful and fair means, and, where appropriate, with the knowledge or consent of the individual.
Data quality	Personal information should be relevant to the purpose for which it is collected, and should be accurate, complete, and current as needed for that purpose.
Purpose specification	The purposes for the collection of personal information should be disclosed before collection and upon any change to that purpose, and its use should be limited to those purposes and compatible purposes.
Use limitation	Personal information should not be disclosed or otherwise used for other than a specified purpose without consent of the individual or legal authority.

[15]OECD, *Making Privacy Notices Simple: An OECD Report and Recommendations* (July 24, 2006).

[16]European Union Data Protection Directive ("Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and the Free Movement of Such Data") (1995).

[17]National Research Council of the National Academies, *Engaging Privacy and Information Technology in a Digital Age* (Washington, D.C.; 2007).

Principle	Description
Security safeguards	Personal information should be protected with reasonable security safeguards against risks such as loss or unauthorized access, destruction, use, modification, or disclosure.
Openness	The public should be informed about privacy policies and practices, and individuals should have ready means of learning about the use of personal information.
Individual participation	Individuals should have the following rights: to know about the collection of personal information, to access that information, to request correction, and to challenge the denial of those rights.
Accountability	Individuals controlling the collection or use of personal information should be accountable for taking steps to ensure the implementation of these principles.

Source: OECD.

The Fair Information Practices are not precise legal requirements. Rather, they provide a framework of principles for balancing the need for privacy with other public policy interests, such as national security, law enforcement, and administrative efficiency. Ways to strike that balance vary among countries and according to the type of information under consideration.

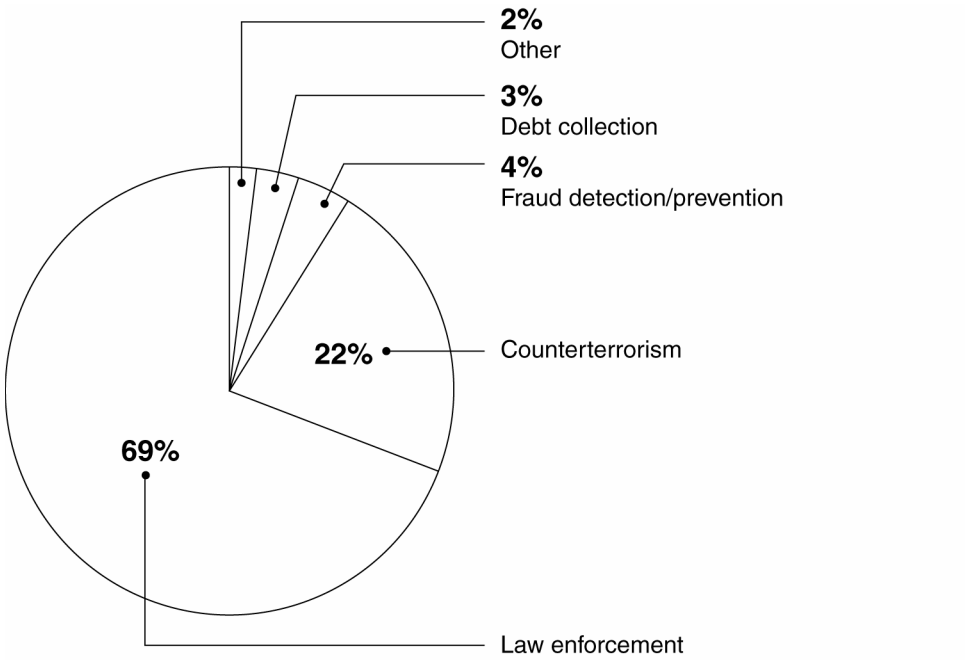
Agencies Used Governmentwide Contracts to Obtain Personal Information from Information Resellers for a Variety of Purposes

DOJ, DHS, State, and SSA reported approximately $30 million through contracts with information resellers in fiscal year 2005.[18] The agencies reported using personal information obtained from resellers for a variety of purposes including law enforcement, counterterrorism, fraud detection/prevention, and debt collection. In all, approximately 91 percent of agency uses of reseller data were in the categories of law enforcement (69 percent) or counterterrorism

[18] This figure comprises contracts and task orders with information resellers that included the acquisition and use of personal information. However, some of these funds may have been for uses that do not involve personal information; we could not omit all such uses because agency officials were not always able to separate the amounts associated with the use of personal information from those for other uses (for example, LexisNexis and West provide news and legal research in addition to public records). In some instances, where the reported use was primarily for legal research, we omitted these funds from the total.

(22 percent). Figure 2 details contract values categorized by their reported use.

Figure 2: Fiscal Year 2005 Contractual Vehicles Enabling the Use of Personal Information from Information Resellers, Categorized by Reported Use



Source: GAO analysis of agency-provided data.

DOJ, which accounted for about 63 percent of the funding, mostly used the data for law enforcement and counterterrorism. DHS also used reseller information primarily for law enforcement and counterterrorism. State and SSA reported acquiring personal information from information resellers for fraud prevention and detection, identity verification, and benefits eligibility determination.

DOJ and DHS Used Information Resellers Primarily for Law Enforcement and Counterterrorism

In fiscal year 2005, DOJ and its components reported approximately $19 million through contracts with a wide variety of information resellers, primarily for purposes related to law enforcement (75 percent) and counterterrorism (18 percent). The Federal Bureau of

Investigation (FBI), which is DOJ's largest user of information resellers, used reseller information to, among other things, analyze intelligence and detect terrorist activities in support of ongoing investigations by law enforcement agencies and the intelligence community. In this capacity, resellers provided the FBI's Foreign Terrorist Tracking Task Force with names, addresses, telephone numbers, and other biographical and demographical information as well as legal briefs, vehicle and boat registrations, and business ownership records.[19]

The Drug Enforcement Administration (DEA), the second largest DOJ user of information resellers in fiscal year 2005, obtained reseller data primarily to detect fraud in prescription drug transactions.[20] Agents used reseller data to detect irregular prescription patterns for specific drugs and trace this information to the pharmacy and prescribing doctor.[21]

DHS and its components reported that they used information reseller data in fiscal year 2005 primarily for law enforcement purposes, such as developing leads on subjects in criminal investigations and detecting fraud in immigration benefit applications (part of enforcing immigration laws). DHS's largest investigative component, the U.S. Immigration and Customs Enforcement, is also its largest user of personal information from resellers. It collected data such as address and vehicle information for criminal investigations and background security checks. Another DHS component, U.S. Customs and Border Protection, conducts queries on people, businesses, property. The Federal Emergency Management Agency, an additional component, used an information reseller to detect fraud in disaster assistance applications.

[19]GAO, *Data Mining: Agencies Have Taken Key Steps to Protect Privacy in Selected Efforts, but Significant Compliance Issues Remain*, GAO-05-866 (Washington, D.C.: Aug. 15, 2005).

[20]DEA's mission includes enforcing laws pertaining to the manufacture, distribution, and dispensing of legally produced controlled substances.

[21]The personal information contained in this information reseller database is limited to the prescribing doctor and does not contain personal patient information.

DHS also reported using information resellers in its counterterrorism efforts. For example, the Transportation Security Administration (TSA), a DHS component, used data obtained from information resellers as part of a test associated with the development of its domestic passenger prescreening program, called Secure Flight.[22] TSA planned for Secure Flight to compare domestic flight reservation information submitted to TSA by aircraft operators with federal watch lists of individuals known or suspected of activities related to terrorism.[23]

SSA and State Used Information Resellers Primarily for Fraud Prevention and Detection

In an effort to ensure the accuracy of Social Security benefit payments, the SSA and its components reported approximately $1.3 million in contracts with information resellers in fiscal year 2005 for purposes relating to fraud prevention (such as skiptracing),[24] confirming suspected fraud related to workers' compensation payments, obtaining information on criminal suspects for follow-up investigations, and collecting debts. For example, the Office of the Inspector General (OIG), the largest user of information reseller data at SSA, used several information resellers to assist investigative agents in detecting benefits abuse by Social Security claimants and to assist agents in locating claimants. Regional office agents may also use reseller data in investigating persons suspected of claiming disability fraudulently.

State and its components reported approximately $569,000 in contracts with information resellers for fiscal year 2005, mainly to support investigations of passport-related activities. For example, several components accessed personal information to validate familial relationships, birth and identity data, and other information

[22]For an assessment of privacy issues associated with the Secure Flight commercial data test, see GAO, *Aviation Security: Transportation Security Administration Did Not Fully Disclose Uses of Personal Information during Secure Flight Program Testing in Initial Privacy Notices, but Has Recently Taken Steps to More Fully Inform the Public*, GAO-05-864R (Washington, D.C.: July 22, 2005).

[23]TSA's current plans for Secure Flight do not include the use of reseller information.

[24]Skiptracing is the process of locating people who have fled in order to avoid paying debts.

submitted on immigrant and nonimmigrant visa petitions. State also used reseller data to investigate passport and visa fraud cases.

Agencies Lacked Policies on Use of Reseller Data, and Practices Do Not Consistently Reflect the Fair Information Practices

Agencies generally lacked policies that specifically addressed their use of personal information from commercial sources (although DHS Privacy Office officials reported in 2006 that they were drafting such a policy[25]), and agency practices for handling personal information acquired from information resellers did not always fully reflect the Fair Information Practices. Specifically, agency practices generally reflected four of the eight Fair Information Practices.

As table 2 shows, the *collection limitation*, *data quality*, *use limitation*, and *security safeguards* principles were generally reflected in agency practices. For example, several agency components (specifically, law enforcement agencies such as the FBI and the U.S. Secret Service) reported that in practice, they generally corroborate information obtained from resellers when it is used as part of an investigation. This practice is consistent with the principle of *data quality*.

Agency policies and practices with regard to the other four principles were uneven. Specifically, agencies did not always have policies or practices in place to address the *purpose specification*, *openness*, and *individual participation* principles with respect to reseller data. The inconsistencies in applying these principles as well as the lack of specific agency policies can be attributed in part to ambiguities in OMB guidance regarding the applicability of the Privacy Act to information obtained from resellers. Further, privacy impact assessments, a valuable tool that could address important aspects of the Fair Information Practices, were often not conducted. Finally, components within each of the four agencies did not

[25]Subsequent to the 2006 report, the DHS Privacy Office took steps to develop guidance on the use of personal information from information resellers in its PIA guidance.

consistently hold staff accountable by monitoring usage of personal information from information resellers and ensuring that it was appropriate; thus, their application of the fourth principle, *accountability*, was uneven.

Table 2: Application of Fair Information Practices to the Reported Handling of Personal Information from Data Resellers at Four Agencies

Principle	Agency application of principle	Agency practices
Collection limitation. The collection of personal information should be limited, should be obtained by lawful and fair means, and, where appropriate, with the knowledge or consent of the individual.	General	Agencies limited personal data collection to individuals under investigation or their associates.
Data quality. Personal information should be relevant to the purpose for which it is collected, and should be accurate, complete, and current as needed for that purpose.	General	Agencies corroborated information from resellers and did not take actions based exclusively on such information.
Purpose specification. The purpose for the collection of personal information should be disclosed before collection and upon any change to that purpose, and its use should be limited to that purpose and compatible purposes.	Uneven	Agency system-of-records notices did not generally reveal that agency systems could incorporate information from data resellers. Agencies also generally did not conduct privacy impact assessments for their systems or programs that involve use of reseller data.
Use limitation. Personal information should not be disclosed or otherwise used for other than a specified purpose without consent of the individual or legal authority.	General	Agencies generally limited their use of personal information to specific investigations (including law enforcement, counterterrorism, fraud detection, and debt collection).
Security safeguards. Personal information should be protected with reasonable security safeguards against risks such as loss or unauthorized access, destruction, use, modification, or disclosure.	General	Agencies had security safeguards such as requiring passwords to access databases, basing access rights on need to know, and logging search activities (including "cloaked logging," which prevents the vendor from monitoring search content).
Openness. The public should be informed about privacy policies and practices, and individuals should have ready means of learning about the use of personal information.	Uneven	See *Purpose specification* above. Agencies did not have established policies specifically addressing the use of personal information obtained from resellers.
Individual participation. Individuals should have the following rights: to know about the collection of personal information, to access that information, to request correction, and to challenge the denial of those rights.	Uneven	See *Purpose specification* above. Because agencies generally did not disclose their collections of personal information from resellers, individuals were often unable to exercise these rights.
Accountability. Individuals controlling the collection or use of personal information should be accountable for taking steps to ensure the implementation of these principles.	Uneven	Agencies did not generally monitor usage of personal information from information resellers to hold users accountable for appropriate use; instead, they relied on users to be responsible for their behavior. For example, agencies may instruct users in their responsibilities to use personal information appropriately, have them sign statements of responsibility, and have them indicate what permissible purpose a given search fulfills.

Source: GAO analysis of agency-supplied data.

Legend:

General = policies or procedures to address all major aspects of a particular principle.

Uneven = policies or procedures addressed some, but not all, aspects of a particular principle or some but not all agencies and components had policies or practices in place addressing the principle.

Note: We did not independently assess the effectiveness of agency information security programs. Our assessment of overall agency application of the Fair Information Practices was based on the policies and management practices described by the Department of State and SSA as a whole and by major components of DOJ and DHS. We did not obtain information on smaller components of DOJ and DHS.

Agency procedures generally reflected the *collection limitation*, *data quality*, *use limitation*, and *security safeguards* principles. Regarding collection limitation, for most law-enforcement and counterterrorism purposes (which accounted for 90 percent of usage in fiscal year 2005), agencies generally limited their personal data collection in that they reported obtaining information only on specific individuals under investigation or associates of those individuals. Regarding *data quality*, agencies reported taking steps to mitigate the risk of inaccurate information reseller data by corroborating information obtained from resellers. Agency officials described the practice of corroborating information as a standard element of conducting investigations. Likewise, for non-law-enforcement use, such as debt collection and fraud detection and prevention, agency components reported that they mitigated potential problems with the accuracy of data provided by resellers by obtaining additional information from other sources when necessary. As for *use limitation*, agency officials said their use of reseller information was limited to distinct purposes that were generally related to law enforcement or counterterrorism. Finally, while we did not assess the effectiveness of information security at any of these agencies, we found that all four had measures in place intended to safeguard the security of personal information obtained from resellers.[26]

[26]Although we did not assess the effectiveness of information security at any agency as part of this review, we have previously reported on weaknesses in almost all areas of information security controls at 24 major agencies, including DOJ, DHS, State, and SSA. For additional information see GAO, *Information Security: Weaknesses Persist at Federal Agencies Despite Progress Made in Implementing Related Statutory Requirements*, GAO-05-552 (Washington, D.C.: July 15, 2005) and *Information Security: Department of Homeland Security Needs to Fully Implement Its Security Program*, GAO-05-700 (Washington, D.C.: June 17, 2005).

Limitations in the Applicability of the Privacy Act and Ambiguities in OMB Guidance Contributed to an Uneven Adherence to the *Purpose Specification*, *Openness*, and *Individual Participation* Principles

The *purpose specification*, *openness*, and *individual participation* principles stipulate that individuals should be made aware of the purpose and intended uses of the personal information being collected about them, and, if necessary, have the ability to access and correct their information. These principles are reflected in the Privacy Act requirement for agencies to publish in the *Federal Register*, "upon establishment or revision, a notice of the existence and character of a system of records." This notice is to include, among other things, the categories of records in the system as well as the categories of sources of records.[27]

In a number of cases, agencies using reseller information did not adhere to the *purpose specification* or *openness* principles in that they did not notify the public that they were using such information and did not specify the purpose for their data collections. Agency officials said that they generally did not prepare system-of-records notices that would address these principles because they were not required to do so by the Privacy Act. The act's vehicle for public notification—the system-of-records notice—is required of an agency only when the agency collects, maintains, and retrieves personal data in the way defined by the act or when a contractor does the same thing explicitly on behalf of the government. Agencies generally did not issue system-of-records notices specifically for their use of information resellers largely because information reseller databases were not considered "systems of records operated by or on behalf of a government agency" and thus were not considered subject to the provisions of the Privacy Act.[28] OMB guidance on implementing the Privacy Act does not specifically

[27]5 U.S.C. § 552a(e)(4)(C) & (I). The Privacy Act allows agencies to claim an exemption from identifying the categories of sources of records for records compiled for criminal law enforcement purposes, as well as for a broader category of uses, including investigative records compiled for criminal or civil law enforcement purposes.

[28]The act provides for its requirements to apply to government contractors when agencies contract for the operation by or on behalf of the agency, a system of records to accomplish an agency function. 5 U.S.C. § 552a(m).

refer to the use of reseller data or how it should be treated. According to OMB and other agency officials, information resellers operate their databases for multiple customers, and federal agency use of these databases does not amount to the operation of a system of records on behalf of the government. Further, agency officials stated that merely querying information reseller databases did not amount to agency "maintenance" of the personal information being queried and thus also did not trigger the provisions of the Privacy Act. In many cases, agency officials considered their use of resellers to be of this type—essentially "ad hoc" querying or "pinging" of reseller databases for personal information about specific individuals, which they believed they were not doing in connection with a formal system of records.

In other cases, however, agencies maintained information reseller data in systems for which system-of-records notices had been previously published. For example, law enforcement agency officials stated that, to the extent they retain the results of reseller data queries, this collection and use is covered by the system-of-records notices for their case file systems. However, in preparing such notices, agencies generally did not specify that they were obtaining information from resellers. Among system-of-records notices that were identified by agency officials as applying to the use of reseller data, only one—TSA's system-of-records notice for the test phase of its Secure Flight program—specifically identified the use of information reseller data.[29]

In several of these cases, agency sources for personal information were described only in vague terms, such as "private organizations," "other public sources," or "public source material," when information was being obtained from information resellers.

The inconsistency with which agencies specify resellers as a source of information in system-of-records notices is due in part to

[29]As we have previously reported, this notice did not fully disclose the scope of the use of reseller data during the test phase. See GAO, *Aviation Security: Transportation Security Administration Did Not Fully Disclose Uses of Personal Information during Secure Flight Program Testing in Initial Privacy Notices, but Has Recently Taken Steps to More Fully Inform the Public*, GAO-05-864R (Washington, D.C.: July 22, 2005).

ambiguity in OMB guidance, which states that "for systems of records which contain information obtained from sources other than the individual to whom the records pertain, the notice should list the types of sources used."[30] Although the guidance is unclear as to what would constitute adequate disclosure of "types of sources," OMB and DHS Privacy Office officials agreed that to the extent that reseller data is subject to the Privacy Act, agencies should specifically identify information resellers as a source and that merely citing public records information does not sufficiently describe the source.

Aside from certain law enforcement exemptions[31] to the Privacy Act, adherence to the *purpose specification* and *openness* principles is critical to preserving a measure of individual control over the use of personal information. Without clear guidance from OMB or specific policies in place, agencies have not consistently reflected these principles in their collection and use of reseller information. As a result, without being notified of the existence of an agency's information collection activities, individuals have no ability to know that their personal information could be obtained from commercial sources and potentially used as a basis, or partial basis, for taking action that could have consequences for their welfare.

Privacy Impact Assessments Could Address Openness and Purpose Specification Principles but Often Were Not Conducted

PIAs can be an important tool to help agencies to address *openness and purpose specification* principles early in the process of developing new information systems. To the extent that PIAs are

[30]OMB, "Privacy Act Implementation: Guidelines and Responsibilities," *Federal Register*, Volume 40, Number 132, Part III, p. 28964 (Washington, D.C.: July 9, 1975).

[31]The Privacy Act allows agencies to claim exemptions if the records are used for certain purposes. 5 U.S.C. § 552a (j) and (k). For example, records compiled for criminal law enforcement purposes can be exempt from the access and correction provisions. In general, the exemptions for law enforcement purposes are intended to prevent the disclosure of information collected as part of an ongoing investigation that could impair the investigation or allow those under investigation to change their behavior or take other actions to escape prosecution. In most cases where officials identified system-of-record notices associated with reseller data collection for law enforcement purposes, agencies claimed this exemption.

made publicly available,[32] they provide explanations to the public about things such as the information that will be collected, why it is being collected, how it is to be used, and how the system and data will be maintained and protected.

However, few agency components reported developing PIAs for their systems or programs that make use of information reseller data. As with system-of-records notices, agencies often did not conduct PIAs because officials did not believe they were required. Current OMB guidance on conducting PIAs is not always clear about when they should be conducted. According to guidance from OMB, a PIA is required by the E-Government Act when agencies "systematically incorporate into existing information systems databases of information in identifiable form purchased or obtained from commercial or public sources."[33] However, the same guidance also instructs agencies that "merely querying a database on an ad hoc basis does not trigger the PIA requirement." Reported uses of reseller data were generally not described as a "systematic" incorporation of data into existing information systems; rather, most involved querying a database and, in some cases, retaining the results of these queries. OMB officials stated that agencies would need to make their own judgments on whether retaining the results of searches of information reseller databases constituted a "systematic incorporation" of information.

Until PIAs are conducted more thoroughly and consistently, the public is likely to remain incompletely informed about agency purposes and uses for obtaining reseller information.

[32]The E-Government Act requires agencies, if practicable, to make privacy impact assessments publicly available through agency Web sites, publication in the *Federal Register*, or by other means. Pub. L. No. 107-347, § 208 (b)(1)(B)(iii).

[33]OMB, *Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002*, Memorandum M-03-22 (Washington, D.C.: Sept. 26, 2003).

Agencies Often Did Not Have Practices in Place to Ensure Accountability for Proper Handling of Information Reseller Data

According to the *accountability* principle, individuals controlling the collection or use of personal information should be accountable for ensuring the implementation of the Fair Information Practices. This means that agencies should take steps to ensure that they use personal information from information resellers appropriately.

Agencies described using activities to oversee their use of reseller information that were largely based on trust in the individual user to use the information appropriately, rather than on management oversight of usage details. For example, in describing controls placed on the use of commercial data, officials from component agencies identified measures such as instructing users that reseller data are for official use only and requiring users to sign statements attesting 1) to their need to access information reseller databases and 2) that their use will be limited to official business. Additionally, agency officials reported that their users are required to select from a list of vendor-defined "permissible purposes" (for example, law enforcement, transactions authorized by the consumer) before conducting a search on reseller databases.

While these practices appear consistent with the accountability principle, they are focused on individual user responsibility instead of monitoring and oversight. Agencies did not have practices in place to obtain reports from resellers that would allow them to monitor usage of reseller databases at a detailed level. Although agencies generally receive usage reports from the information resellers, these reports are designed primarily for monitoring costs. Further, these reports generally contained only high-level statistics on the number of searches and databases accessed, not the contents of what was actually searched, thus limiting their utility in monitoring usage.

To the extent that federal agencies do not implement methods such as user monitoring or auditing of usage records, they provide limited accountability for their usage of information reseller data and have limited assurance that the information is being used appropriately.

Not All Agencies Have Taken Steps to Address our Recommendations

In our report, we recommended that the agencies develop specific policies for the collection, maintenance, and use of personal information obtained from resellers. We also recommended that OMB revise its privacy guidance to clarify the applicability of requirements for public notices and privacy impact assessments to agency use of personal information from resellers and direct agencies to review their uses of such information to ensure it is explicitly referenced in privacy notices and assessments. The agencies generally agreed with our findings and described actions initiated to address our recommendations.

Since the issuance of our 2006 report, two of the four agencies have taken action to address our recommendation. For example, the DHS Privacy Office incorporated specific questions in its May 2007 PIA guidance concerning use of commercial data. The guidance requires programs that use commercial or publicly available data to explain why and how such data are used. Further, the guidance for systems that use or rely on commercial data requires an explanation of how data accuracy and integrity are preserved and the reliability of the data assessed with regard to its value to the purpose of the system. According to DHS Privacy Office officials, after identifying use of commercial data through the PIA process, the Privacy Office works with the relevant DHS component to review uses of commercial data to ensure appropriate controls are in place and that the planned uses are appropriately disclosed in privacy notices. In addition, officials at DOJ informed us that the Privacy and Civil Liberties Office has in place a verbal agreement with agency components that there are to be no bulk acquisitions of commercial data and that when the agency takes in data from commercial sources, there should be a valid system-of-records notice that specifically identifies commercial data as a source. Further, DOJ has updated several of its system-of-records notices to reflect their use of data from information resellers. SSA and State have not yet addressed our recommendation.

However, OMB has not addressed our recommendations. In an August 2006 letter to congressional committees in response to the recommendations contained in our April 2006 report, OMB noted

that work on the protection of personal information through the Identity Theft Task Force was ongoing and that following the completion of this work, they would consider issuing appropriate clarifying guidance concerning reseller data. Since then, OMB's efforts on the Identity Theft Task Force have been completed and on May 22, 2007 OMB issued M-07-16, "Safeguarding Against the Breach of Personally Identifiable Information." To date, OMB has not issued additional clarifying guidance concerning reseller data.

Privacy Provisions of the Proposed Federal Agency Data Protection Act are Consistent with Our Recommendations

The Federal Agency Data Protection Act was introduced on December 18, 2007. Among other things, the legislation contains privacy provisions that would require agencies to conduct PIAs when "purchasing or subscribing for a fee to information in identifiable form from a data broker." We believe that such a requirement is consistent with the recommendations contained in our report, particularly given the debate concerning whether or not agencies "systematically incorporate" information or are "merely pinging or querying the information." Our report found that PIAs could serve to address certain Fair Information Practice principles such as *purpose specification* and *openness*, but often were not conducted. Such a requirement could more readily ensure agencies perform these assessments. Further, since OMB has not clarified its guidance on this issue, a requirement in law could provide needed direction to agencies.

The proposed Federal Agency Data Protection Act would also require each agency to prescribe regulations that specify, among other things, the personnel permitted to access, analyze, or otherwise use commercial reseller databases. This legislation is consistent with our recommendation that agencies develop policies concerning their use of personal information from information resellers.

In summary, services provided by information resellers are important to federal agency functions such as law enforcement and fraud protection and identification. While agencies have taken steps

to adhere to some Fair Information Practices such as the *collection limitation*, *data quality*, *use limitation*, and *security safeguards* principles, they have not taken all the steps they could to reflect others—or to use the specific processes of the Privacy Act and E-Government Act requirements—in their handling of reseller data. Because OMB privacy guidance does not clearly address information reseller data, agencies are left largely on their own to determine how to satisfy legal requirements and protect privacy when acquiring and using reseller data. Since we issued our report in 2006, two of the four agencies have taken steps to address our recommendations. However, OMB has not modified its guidance. Without current and specific guidance, the government risks continued uneven adherence to important, well-established privacy principles and lacks assurance that the privacy rights of individuals are being adequately protected. Absent action from OMB to revise guidance, privacy provisions contained in the proposed Federal Agency Data Protection Act could clarify the need to conduct privacy impact assessments wherever reseller data are involved and promote the development of agency policies and procedures concerning the use of such data. We believe these provisions are consistent with the results and recommendations contained in our 2006 report.

Mr. Chairman, this concludes my testimony today. I would be happy to answer any questions you or other members of the subcommittee may have.

Contacts and Acknowledgements

If you have any questions concerning this testimony, please contact Linda Koontz, Director, Information Management, at (202) 512-6240, or koontzl@gao.gov. Other individuals who made key contributions to this testimony were Susan Czachor, John de Ferrari, Nancy Glover, Rebecca LaPaze, David Plocher, and Jamie Pressman.

GAO's Mission

The Government Accountability Office, the audit, evaluation, and investigative arm of Congress, exists to support Congress in meeting its constitutional responsibilities and to help improve the performance and accountability of the federal government for the American people. GAO examines the use of public funds; evaluates federal programs and policies; and provides analyses, recommendations, and other assistance to help Congress make informed oversight, policy, and funding decisions. GAO's commitment to good government is reflected in its core values of accountability, integrity, and reliability.

Obtaining Copies of GAO Reports and Testimony

The fastest and easiest way to obtain copies of GAO documents at no cost is through GAO's Web site (www.gao.gov). Each weekday, GAO posts newly released reports, testimony, and correspondence on its Web site. To have GAO e-mail you a list of newly posted products every afternoon, go to www.gao.gov and select "E-mail Updates."

Order by Mail or Phone

The first copy of each printed report is free. Additional copies are $2 each. A check or money order should be made out to the Superintendent of Documents. GAO also accepts VISA and Mastercard. Orders for 100 or more copies mailed to a single address are discounted 25 percent. Orders should be sent to:

U.S. Government Accountability Office
441 G Street NW, Room LM
Washington, DC 20548

To order by Phone: Voice: (202) 512-6000
TDD: (202) 512-2537
Fax: (202) 512-6061

To Report Fraud, Waste, and Abuse in Federal Programs

Contact:

Web site: www.gao.gov/fraudnet/fraudnet.htm
E-mail: fraudnet@gao.gov
Automated answering system: (800) 424-5454 or (202) 512-7470

Congressional Relations

Ralph Dawn, Managing Director, dawnr@gao.gov, (202) 512-4400
U.S. Government Accountability Office, 441 G Street NW, Room 7125
Washington, DC 20548

Public Affairs

Chuck Young, Managing Director, youngc1@gao.gov, (202) 512-4800
U.S. Government Accountability Office, 441 G Street NW, Room 7149
Washington, DC 20548