May 17, 2006

PRIVACY

Key Challenges Facing Federal Agencies

GAO Accountability·Integrity·Reliability

Highlights

Highlights of GAO-06-777T, a testimony before the Subcommittee on Commercial and Administrative Law, Committee on the Judiciary, House of Representatives

Why GAO Did This Study

Advances in information technology make it easier than ever for the federal government to obtain and process personal information about citizens and residents in many ways and for many purposes. To ensure that the privacy rights of individuals are respected, this information must be properly protected in accordance with current law, particularly the Privacy Act and the E-Government Act of 2002. These laws prescribe specific activities that agencies must perform to protect privacy, and the Office of Management and Budget (OMB) has developed guidance on how and in what circumstances agencies are to carry out these activities.

Many agencies designate officials as focal points for privacy-related matters, and increasingly, many have created senior positions, such as chief privacy officer, to assume primary responsibility for privacy policy, as well as dedicated privacy offices.

GAO was asked to testify on key challenges facing agency privacy officers. To address this issue, GAO identified and summarized issues raised in its previous reports on privacy.

What GAO Recommends

Because GAO has already made privacy-related recommendations in the earlier reports described here, it is making no further recommendations at this time.

www.gao.gov/cgi-bin/getrpt?GAO-06-777T.

To view the full product, including the scope and methodology, click on the link above. For more information, contact Linda Koontz at (202) 512-6240 or koontzl@gao.gov.

What GAO Found

Agencies and their privacy officers face growing demands in addressing privacy challenges. For example, as GAO reported in 2003, agency compliance with Privacy Act requirements was uneven, owing to ambiguities in guidance, lack of awareness, and lack of priority. While agencies generally did well with certain aspects of the Privacy Act's requirements—such as issuing notices concerning certain systems containing collections of personal information—they did less well at others, such as ensuring that information is complete, accurate, relevant, and timely before it is disclosed to a nonfederal organization. In addition, the E-Gov Act requires that agencies perform privacy impact assessments (PIA) on such information collections. Such assessments are important to ensure, among other things, that information is handled in a way that conforms to privacy requirements. However, in work on commercial data resellers, GAO determined in 2006 that many agencies did not perform PIAs on systems that used reseller information, believing that these were not required. In addition, in public notices on these systems, agencies did not always reveal that information resellers were among the sources to be used. To address such challenges, chief privacy officers can work with officials from OMB and other agencies to identify ambiguities and provide clarifications about the applicability of privacy provisions, such as in situations involving the use of reseller information. In addition, as senior officials, they can increase agency awareness and raise the priority of privacy issues.

Agencies and privacy officers will also face the challenge of ensuring that privacy protections are not compromised by advances in technology. For example, federal agency use of data mining—the analysis of large amounts of data to uncover hidden patterns and relationships—was initially aimed at detecting financial fraud and abuse. Increasingly, however, the use of this tool has expanded to include purposes such as detecting terrorist threats. GAO found in 2005 that agencies employing data mining took many steps needed to protect privacy (such as issuing public notices), but none followed all key procedures (such as including in these notices the intended uses of personal information). Another new technology development presenting privacy challenges is radio frequency identification (RFID), which uses wireless communication to transmit data and thus electronically identify, track, and store information on tags attached to or embedded in objects. GAO reported in 2005 that federal agencies use or propose to use the technology for physical access controls and tracking assets, documents, or materials. For example, the Department of Defense was using RFID to track shipments. Although such applications are not likely to generate privacy concerns, others could, such as the use of RFIDs by the federal government to track the movement of individuals traveling within the United States. Agency privacy offices can serve as a key mechanism for ensuring that privacy is fully addressed in agency approaches to new technologies such as data mining and RFID.