January 2008

INFORMATION SECURITY

Protecting Personally Identifiable Information

GAO Accountability • Integrity • Reliability

Highlights

Highlights of GAO-08-343, a report to congressional requesters

Why GAO Did This Study

The loss of personally identifiable information can result in substantial harm, embarrassment, and inconvenience to individuals and may lead to identity theft or other fraudulent use of the information. As shown in prior GAO reports, compromises to such information and long-standing weaknesses in federal information security raise important questions about what steps federal agencies should take to prevent them. As the federal government obtains and processes information about individuals in increasingly diverse ways, properly protecting this information and respecting the privacy rights of individuals will remain critically important.

GAO was requested to (1) identify the federal laws and guidance issued to protect personally identifiable information from unauthorized use or disclosure and (2) describe agencies' progress in developing policies and documented procedures that respond to recent guidance from the Office of Management and Budget (OMB) to protect personally identifiable information that is either accessed remotely or physically transported outside an agency's secured physical perimeter. To do so, GAO reviewed relevant laws and guidance, surveyed officials at 24 major federal agencies, and examined and analyzed agency documents, including policies, procedures, and plans. In commenting on a draft of this report, OMB stated that it generally agreed with the report's contents.

To view the full product, including the scope and methodology, click on GAO-08-343.
For more information, contact Gregory Wilshusen at (202) 512-6244 or wilshuseng@gao.gov.

What GAO Found

Two primary laws (the Privacy Act of 1974 and the E-Government Act of 2002) give federal agencies responsibilities for protecting personal information, including ensuring its security. Additionally, the Federal Information Security Management Act of 2002 (FISMA) requires agencies to develop, document, and implement agencywide programs to provide security for their information and information systems (which include personally identifiable information and the systems on which it resides). The act also requires the National Institute of Standards and Technology (NIST) to develop technical guidance in specific areas, including minimum information security requirements for information and information systems. In the wake of recent incidents of security breaches involving personal data, OMB issued guidance in 2006 and 2007 reiterating agency responsibilities under these laws and technical guidance, drawing particular attention to the requirements associated with personally identifiable information. In this guidance, OMB directed, among other things, that agencies encrypt data on mobile computers or devices and follow NIST security guidelines regarding personally identifiable information that is accessed outside an agency's physical perimeter.

Not all agencies had developed the range of policies and procedures reflecting OMB guidance on protection of personally identifiable information that is either accessed remotely or physically transported outside an agency's secured physical perimeter. Of 24 major agencies, 22 had developed policies requiring personally identifiable information to be encrypted on mobile computers and devices. Fifteen of the 24 agencies had policies to use a "time-out" function for remote access and mobile devices requiring user reauthentication after 30 minutes of inactivity. Fewer agencies (11) had established policies to log computer-readable data extracts from databases holding sensitive information and erase the data within 90 days after extraction. Several agencies indicated that they were researching technical solutions to address these issues. Gaps in their policies and procedures reduced agencies' ability to protect personally identifiable information from improper disclosure.

At the conclusion of GAO's review, OMB announced in November 2007 that agencies that did not complete certain privacy and security requirements, including those just described, received a downgrade in their scores for progress in electronic government initiatives. According to OMB, it will continue working with agencies to help them strengthen their information security and privacy programs, especially as they relate to the protection of personally identifiable information. In view of OMB's recent actions in this area and GAO's previous recommendations on improving agency information security and implementation of FISMA requirements, GAO is making no further recommendations at this time.