June 8, 2006

PRIVACY

Preventing and Responding to Improper Disclosures of Personal Information

GAO Accountability·Integrity·Reliability

Highlights

Highlights of GAO-06-833T, a testimony before the Committee on Government Reform, House of Representatives

Why GAO Did This Study

The recent security breach at the Department of Veterans Affairs, in which personal data on millions of veterans were compromised, has highlighted the importance of the federal government's processes for protecting personal information. As the federal government obtains and processes information about individuals in increasingly diverse ways, it remains critically important that it properly protect this information and respect the privacy rights of individuals.

GAO was asked to testify on preventing and responding to improper disclosures of personal information in the federal government, including how agencies should notify individuals and the public when breaches occur. In preparing this testimony, GAO drew on its previous reports and testimonies, as well as on expert opinion provided in congressional testimony and other sources.

What GAO Recommends

GAO has made recommendations previously to agencies and to the Office of Management and Budget (OMB), which provides guidance to agencies on implementing federal privacy and security laws, to ensure that they are adequately addressing security and privacy issues.
In addition, in considering security breach notification legislation, the Congress should consider setting specific reporting requirements for agencies.

www.gao.gov/cgi-bin/getrpt?GAO-06-833T.

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 can take a number of actions to help guard against the possibility that databases of personally identifiable information are inadvertently compromised. Two key steps are as follows:

- Develop a privacy impact assessment—an analysis of how personal information is collected, stored, shared, and managed—whenever information technology is used to process personal information. These assessments, required by the E-Government Act of 2002, are a tool for agencies to fully consider the privacy implications of planned systems and data collections before implementation, when it may be easier to make critical adjustments.
- Ensure that a robust information security program is in place, as required by the Federal Information Security Management Act of 2002 (FISMA). Such a program includes periodic risk assessments; security awareness training; security policies, procedures, and practices, as well as tests of their effectiveness; and procedures for addressing deficiencies and for detecting, reporting, and responding to security incidents.

More specific practical measures aimed at preventing inadvertent data breaches include limiting the collection of personal information, limiting the time that such data are retained, limiting access to personal information and training personnel accordingly, and considering the use of technological controls such as encryption when data need to be stored on mobile devices.

When data breaches do occur, notification to the individuals affected and/or the public has clear benefits, allowing people the opportunity to take steps to protect themselves against the dangers of identity theft. Although existing laws do not require agencies to notify the public when data breaches occur, such notification is consistent with agencies' responsibility to inform individuals about how their information is being accessed and used, and it promotes accountability for privacy protection. That said, care is needed in defining appropriate criteria for incidents that merit notification. Notifying individuals of security incidents that do not pose serious risks could be counterproductive and costly, while giving too much discretion to agencies could result in their avoiding the disclosure of potentially harmful breaches. Care is also needed to ensure that notices are useful and easy to understand, so that they are effective in alerting recipients to actions they may want to take to minimize the risk of identity theft. Among other things, it is important to provide context in the notice—explaining to recipients why they are receiving a notice and what to do about it. It is also important the notices be coordinated with law enforcement to avoid impeding ongoing investigations. Given that individuals may be adversely impacted by a compromise of their personal information, it is critical that they fully understand the nature of the threat and the options they have to address it.