July 31, 2012

PRIVACY

Federal Law Should Be Updated to Address Changing Technology Landscape

GAO Accountability * Integrity * Reliability

Highlights

Highlights of GAO-12-961T, a testimony before the Subcommittee on Oversight of Government Management, the Federal Workforce, and the District of Columbia, Committee on Homeland Security and Governmental Affairs, U.S. Senate

Why GAO Did This Study

The federal government collects and uses personal information on individuals in increasingly sophisticated ways, and its reliance on information technology (IT) to collect, store, and transmit this information has also grown. While this enables federal agencies to carry out many of the government's critical functions, concerns have been raised that the existing laws for protecting individuals' personal information may no longer be sufficient given current practices. Moreover, vulnerabilities arising from agencies' increased dependence on IT can result in the compromise of sensitive personal information, such as inappropriate use, modification, or disclosure.

GAO was asked to provide a statement describing (1) the impact of recent technology developments on existing laws for privacy protection in the federal government and (2) actions agencies can take to protect against and respond to breaches involving personal information. In preparing this statement, GAO relied on previous work in these areas as well as a review of more recent reports on security vulnerabilities.

What GAO Recommends

GAO previously suggested that Congress consider amending applicable privacy laws to address identified issues. GAO has also made numerous recommendations to agencies over the last several years to address weaknesses in policies and procedures related to privacy and to strengthen their information security programs.

View GAO-12-961T. For more information, contact Gregory C. Wilshusen (202) 512-6244 or wilshuseng@gao.gov.

What GAO Found

Technological developments since the Privacy Act became law in 1974 have changed the way information is organized and shared among organizations and individuals. Such advances have rendered some of the provisions of the Privacy Act and the E-Government Act of 2002 inadequate to fully protect all personally identifiable information collected, used, and maintained by the federal government. For example, GAO has reported on challenges in protecting the privacy of personal information relative to agencies' use of Web 2.0 and data-mining technologies.

While laws and guidance set minimum requirements for agencies, they may not protect personal information in all circumstances in which it is collected and used throughout the government and may not fully adhere to key privacy principles. GAO has identified issues in three major areas:

- **Applying privacy protections consistently to all federal collection and use of personal information.** The Privacy Act's protections only apply to personal information when it is considered part of a "system of records" as defined by the act. However, agencies routinely access such information in ways that may not fall under this definition.
- **Ensuring that use of personally identifiable information is limited to a stated purpose.** Current law and guidance impose only modest requirements for describing the purposes for collecting personal information and how it will be used. This could allow for unnecessarily broad ranges of uses of the information.
- **Establishing effective mechanisms for informing the public about privacy protections.** Agencies are required to provide notices in the *Federal Register* of information collected, categories of individuals about whom information is collected, and the intended use of the information, among other things. However, concerns have been raised whether this is an effective mechanism for informing the public.

The potential for data breaches at federal agencies also pose a serious risk to the privacy of individuals' personal information. OMB has specified actions agencies should take to prevent and respond to such breaches. In addition, GAO has previously reported that agencies can take steps that include

- assessing the privacy implications of a planned information system or data collection prior to implementation;
- ensuring the implementation of a robust information security program; and
- limiting the collection of personal information, the time it is retained, and who has access to it, as well as implementing encryption.

However, GAO and inspectors general have continued to report on vulnerabilities in security controls over agency systems and weaknesses in their information security programs, potentially resulting in the compromise of personal information. These risks are illustrated by recent security incidents involving individuals' personal information. Federal agencies reported 13,017 such incidents in 2010 and 15,560 in 2011, an increase of 19 percent.