March 21, 2007

HOMELAND SECURITY

Continuing Attention to Privacy Concerns Is Needed as Programs Are Developed

GAO Accountability · Integrity · Reliability

Highlights

Highlights of GAO-07-630T, a testimony before the Subcommittee on Homeland Security, Committee on Appropriations, House of Representatives

Why GAO Did This Study

Advances in information technology make it easier than ever for the Department of Homeland Security (DHS) and other agencies to obtain and process information about citizens and residents in many ways and for many purposes. The demands of the war on terror also drive agencies to extract as much value as possible from the information available to them, adding to the potential for compromising privacy. Recognizing that securing the homeland and protecting the privacy rights of individuals are both important goals, the Congress has asked GAO to perform several reviews of DHS programs and their privacy implications over the past several years.

For this hearing, GAO was asked to testify on key privacy challenges facing DHS. To address this issue, GAO identified and summarized issues raised in its previous reports on privacy and assessed recent governmentwide privacy guidance.

What GAO Recommends

Because GAO has already made privacy-related recommendations in its earlier reports, it is making no further recommendations at this time. Officials have taken action or have said they are in the process of taking action to address the recommendations. Implementation is critical to ensuring that privacy protections are in place throughout key DHS programs and activities.

www.gao.gov/cgi-bin/getrpt?GAO-07-630T.

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

As it develops and participates in important homeland security activities, DHS faces challenges in ensuring that privacy concerns are addressed early, are reassessed when key programmatic changes are made, and are thoroughly reflected in guidance on emerging technologies and uses of personal data. GAO's reviews of DHS programs have identified cases where these challenges were not fully met. For example, increased use by federal agencies of data mining—the analysis of large amounts of data to uncover hidden patterns and relationships—has been accompanied by uncertainty regarding privacy requirements and oversight of such systems. As described in a recent GAO report, DHS did not assess privacy risks in developing a data mining tool known as ADVISE (Analysis, Dissemination, Visualization, Insight, and Semantic Enhancement), as required by the E-Government Act of 2002. ADVISE is a data mining tool under development intended to help the department analyze large amounts of information. Because privacy had not been assessed and mitigating controls had not been implemented, DHS faced the risk that uses of ADVISE in systems containing personal information could require costly and potentially duplicative retrofitting at a later date to add the needed controls.

GAO has also reported on privacy challenges experienced by DHS in reassessing privacy risks when key programmatic changes were made during development of a prescreening program for airline passengers. The Transportation Security Administration (TSA) has been working to develop a computer-assisted passenger prescreening system, known as Secure Flight, to be used to evaluate passengers before they board an aircraft on domestic flights. GAO reported that TSA had not fully disclosed uses of personal information during testing of Secure Flight, as required by the Privacy Act of 1974. To prevent such problems from recurring, TSA officials recently said that they have added privacy experts to Secure Flight's development teams to address privacy considerations on a continuous basis as they arise.

Another challenge DHS faces is ensuring that privacy considerations are addressed in the emerging information sharing environment. The Intelligence Reform and Terrorism Prevention Act of 2004 requires the establishment of an environment to facilitate the sharing of terrorism information, as well as the issuance of privacy guidelines for operation in this environment. Recently issued privacy guidelines developed by the Office of the Director of National Intelligence provide only a high-level framework for privacy protection. While DHS is only one participant, it has the responsibility to ensure that the information under its control is shared with other organizations in ways that adequately protect privacy. Accordingly, it will be important for the department to clearly establish departmental guidelines so that privacy protections are implemented properly and consistently.