



HOMELAND SECURITY

DHS Privacy Office Has Made Progress but Faces Continuing Challenges

Highlights of [GAO-07-1024T](#), a testimony before the Subcommittee on Commercial and Administrative Law, Committee on the Judiciary, House of Representatives

Why GAO Did This Study

The Department of Homeland Security (DHS) Privacy Office was established with the appointment of the first Chief Privacy Officer in April 2003, as required by the Homeland Security Act of 2002. The Privacy Office’s major responsibilities include: (1) reviewing and approving privacy impact assessments (PIA)—analyses of how personal information is managed in a federal system, (2) integrating privacy considerations into DHS decision making and ensuring compliance with the Privacy Act of 1974, and (3) preparing and issuing annual reports and reports on key privacy concerns.

GAO was asked to testify on its recent report examining progress made by the DHS Privacy Office in carrying out its statutory responsibilities. GAO compared statutory requirements with Privacy Office processes, documents, and activities.

What GAO Recommends

In its report, GAO recommended that the Secretary of Homeland Security take several actions including appointing privacy officers in key DHS components, implementing a process for reviewing Privacy Act notices, and establishing a schedule for timely issuance of Privacy Office reports.

DHS generally agreed with the report and described actions initiated to address GAO’s recommendations.

www.gao.gov/cgi-bin/getrpt?GAO-07-1024T.

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.

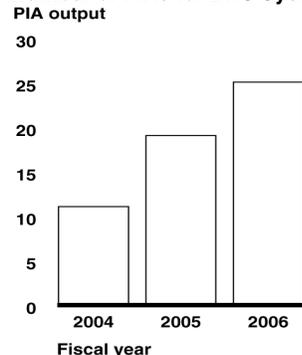
What GAO Found

The DHS Privacy Office has made significant progress in carrying out its statutory responsibilities under the Homeland Security Act and its related role in ensuring compliance with the Privacy Act of 1974 and E-Government Act of 2002, but more work remains to be accomplished. Specifically, the Privacy Office has established a compliance framework for conducting PIAs, which are required by the E-Gov Act. The framework includes formal written guidance, training sessions, and a process for identifying systems requiring such assessments. The framework has contributed to an increase in the quality and number of PIAs issued (see fig.) as well as the identification of many more affected systems. The resultant workload is likely to prove difficult to process in a timely manner. Designating privacy officers in certain DHS components could help speed processing of PIAs, but DHS has not yet taken action to make these designations.

The Privacy Office has also taken actions to integrate privacy considerations into the DHS decision-making process by establishing an advisory committee, holding public workshops, and participating in policy development. However, limited progress has been made in one aspect of ensuring compliance with the Privacy Act—updating public notices for systems of records that were in existence prior to the creation of DHS. These notices should identify, among other things, the type of data collected, the types of individuals about whom information is collected, and the intended uses of the data. Until the notices are brought up-to-date, the department cannot assure the public that the notices reflect current uses and protections of personal information.

Further, the Privacy Office has generally not been timely in issuing public reports. For example, a report on the Multi-state Anti-Terrorism Information Exchange program—a pilot project for law enforcement sharing of public records data—was not issued until long after the program had been terminated. Late issuance of reports has a number of negative consequences, including a potential reduction in the reports’ value and erosion of the office’s credibility.

Number of PIAs for DHS Systems Published by Fiscal Year



Source: GAO analysis of published DHS PIAs.