September 2010

PRIVACY

OPM Should Better Monitor Implementation of Privacy-Related Policies and Procedures for Background Investigations

GAO Accountability • Integrity • Reliability

Highlights

Highlights of GAO-10-849, a report to 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

Approximately 90 percent of all federal background investigations are provided by the Office of Personnel Management's (OPM) Federal Investigative Services (FIS) division. In fiscal year 2009, FIS conducted over 2 million investigations of varying types, making the organization a major steward of personal information on U.S. citizens. GAO was asked to (1) describe how OPM uses personally identifiable information (PII) in conducting background investigations and (2) assess the extent to which OPM's privacy policies and procedures for protecting PII related to investigations meet statutory requirements and align with widely accepted privacy practices. To address these objectives, GAO compared OPM and FIS policies and procedures with key privacy laws and widely accepted practices.

What GAO Recommends

GAO is recommending that the Director of OPM (1) develop guidance for analyzing and mitigating privacy risks in privacy impact assessments, and (2) develop and implement oversight mechanisms for ensuring that investigators properly protect PII and that customer agencies adhere to agreed-upon privacy protection measures. OPM agreed with our recommendations.

View GAO-10-849 or key components.
For more information, contact Gregory C. Wilshusen at (202) 512-6244 or wilshuseng@gao.gov

What GAO Found

FIS, a component of OPM, conducts background investigations using extensive amounts of PII. Specifically, FIS collects PII from the individual being investigated, government agencies holding relevant data on the subject, and contacts familiar with the subject of the investigation. It uses this information during the four phases of the investigation process: (1) Questionnaire Submission, when requesting agencies submit a questionnaire completed by the individual who will be investigated; (2) Scheduling and Initiation, during which goals and milestones are set, automated information requests occur, and an investigator is assigned; (3) Investigation, during which an investigator gathers information from the automated requests and from interviews and prepares a report; and (4) Review, during which a reviewer determines if a report is complete before allowing it to be sent to the requesting agency.

FIS has taken steps to incorporate key privacy laws and widely accepted privacy practices into policies and procedures for conducting background investigations. For example, field investigators are directed to limit collection of PII to only information relevant to an investigation, and several procedures are in place to ensure that such information is recorded as accurately as possible in OPM's systems. However, the agency has conducted limited oversight of FIS's development of privacy impact assessments (PIA), investigators' implementation of privacy protection guidance, and customer agencies' adherence to privacy agreements. A PIA is an analysis of how personal information is collected, stored, shared, and managed in a federal system. It is required by the E-Government Act of 2002. Related Office of Management and Budget guidance emphasizes the need to identify and assess privacy risks in concert with developing a PIA. However, OPM's guidance for PIAs does not require that privacy risks be analyzed or mitigation strategies be identified for those risks. Consequently, OPM cannot be sure that potential risks associated with the use of PII in its information systems have been adequately assessed and mitigated. Additionally, widely accepted privacy practices call for accountability to ensure privacy-protection policies are implemented to safeguard personal information from potential risks. Such accountability includes monitoring to ensure proper implementation of privacy protection measures. However, although FIS tracks PII that is provided to and received from field investigators, it had not monitored investigators' adherence to its policies and procedures for protecting PII while investigations are underway. Further, while FIS has developed agreements with customer agencies related to the protection of PII contained in investigation case files, it does not monitor customer agencies' implementation of these policies, even though its agreements state it is responsible for doing so. Without oversight processes for monitoring investigators' and customer agencies' adherence to its PII protection policies, OPM lacks assurance that its privacy protection measures are being properly implemented.