

GAO

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

September 2010

PRIVACY

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



GAO

Accountability * Integrity * Reliability



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

PRIVACY

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

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.

Contents

Letter		1
	Background	2
	OPM's Background Investigation Process Involves Extensive Collection and Use of PII	9
	FIS Has Taken Steps to Ensure Privacy Policies and Procedures Meet Statutory Requirements and Align with Fair Information Practices, but Oversight of Implementation is Limited	17
	Conclusions	25
	Recommendations for Executive Action	25
	Agency Comments and Our Evaluation	26
Appendix I	Objectives, Scope, and Methodology	28
Appendix II	GAO Contact and Staff Acknowledgments	30
Table		
	Table 1: Fair Information Practices	6
Figures		
	Figure 1: Key Steps in FIS's Background Investigation Process	9
	Figure 2: Questionnaire Submission Phase Detailed Steps	10
	Figure 3: Scheduling and Initiation Phase Detailed Steps	12
	Figure 4: Investigation Phase Detailed Steps	14
	Figure 5: Review Phase Detailed Steps	15
	Figure 6: Reported Incidents of Lost or Stolen Paper Files Associated with Background Investigations	22

Abbreviations

CIO	Chief Information Officer
DOD	Department of Defense
e-QIP	Electronic Questionnaires for Investigations Processing
FBI	Federal Bureau of Investigation
FIPC	Federal Investigations Processing Center
FIPS	Federal Information Processing Standard
FIS	Federal Investigative Services
MOU	memorandum of understanding
NAC	National Agency Check
NIST	National Institute of Standards and Technology
OECD	Organization for Economic Cooperation and Development
OIG	Office of the Inspector General
OMB	Office of Management and Budget
OPM	Office of Personnel Management
PIA	privacy impact assessment
PII	personally identifiable information
PIPS	Personnel Investigations Processing System
PIPS-R	Personnel Investigations Processing System – Reporting
SORN	System of Records Notice

This is a work of the U.S. government and is not subject to copyright protection in the United States. The published product may be reproduced and distributed in its entirety without further permission from GAO. However, because this work may contain copyrighted images or other material, permission from the copyright holder may be necessary if you wish to reproduce this material separately.



United States Government Accountability Office
Washington, DC 20548

September 7, 2010

The Honorable Daniel K. Akaka
Chairman
The Honorable George V. Voinovich
Ranking Member
Subcommittee on Oversight of Government
Management, the Federal Workforce,
and the District of Columbia
Committee on Homeland Security
and Governmental Affairs
United States Senate

The Federal Investigative Services (FIS) division of the Office of Personnel Management (OPM) is responsible for conducting approximately 90 percent of all federal background investigations. To conduct its work, FIS relies heavily on personally identifiable information (PII) provided by the individuals who are being considered for security clearances. Such information can be extensive and can include financial and medical information, as well as PII on family members and close contacts. 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.

Government agencies have a long-standing obligation under the Privacy Act of 1974 and the E-Government Act of 2002 to protect the privacy of individuals about whom they collect personal information. These laws prescribe specific activities that agencies must perform to protect privacy, such as ensuring that personal information is used only for an authorized purpose and that assessments are conducted of the privacy risks associated with the information technology used to process the personal information.

You asked us to review the implementation of privacy protection provisions for information collected and maintained by FIS as it relates to the background investigation process. Specifically, as agreed with your office, our objectives were to: (1) describe how OPM uses PII in conducting background investigations and (2) determine 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 our first objective, we analyzed agency policies, procedures, and guidance to identify FIS's background investigation process. We interviewed FIS officials at their headquarters in Boyers, Pennsylvania, and at OPM headquarters in Washington, D.C., and conducted site visits of FIS headquarters to identify the current process for conducting background security clearance investigations. We analyzed this information to identify the overall process for conducting investigations and how PII is utilized throughout the process.

To address our second objective, we reviewed pertinent information security and privacy policies, procedures, guidance, and practices in place at OPM. Additionally, we analyzed key privacy laws, standards, and widely accepted privacy practices and compared them with key elements of the FIS investigation processes. We interviewed officials at FIS headquarters and within the OPM Privacy Office to discuss recent efforts to oversee the implementation of privacy policies and procedures.

We conducted this performance audit from October 2009 to September 2010 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives. Our objectives, scope, and methodology are discussed in more detail in appendix I.

Background

OPM is the central human resources agency for the federal government, tasked with ensuring the government has an effective civilian workforce. To carry out this mission, OPM delivers human resources products and services, including personnel background investigations, to agencies on a reimbursable basis. These investigations are the responsibility of OPM's FIS division.

Federal Investigative Services Conducts Background Investigations for the Federal Government

FIS conducts approximately 90 percent of all personnel background investigations for the federal government. FIS provides the results of the investigations to agencies for use in determining individuals' suitability or fitness for federal civilian, military, or federal contract employment as well as eligibility for access to classified national security information. FIS also has responsibility for developing and implementing uniform policies and procedures to ensure the proper completion of investigations. For example, FIS issued internal agency guidance, called the *Investigator's*

Handbook, to direct its federal and contract investigators as they conduct investigations. In fiscal year 2009, FIS conducted over 2 million investigations of varying types.

In addition to background investigations, FIS conducts other types of investigations and checks, including—among others—credit searches of all three major credit bureaus regarding financial responsibility and periodic reinvestigations (generally for moderate or high-risk positions).¹ Many of these may be limited to contacting other federal agencies or private institutions for information and may not require an investigator to conduct traditional investigation activities such as interviewing individuals familiar with the subject. FIS’s investigations staff consists of approximately 2,300 federal employees and 6,000 contractor staff.

To conduct these investigations, FIS officials use information technology systems located at FIS headquarters, known as the Federal Investigations Processing Center (FIPC), to coordinate investigative activities and store all of the information generated by such investigations. At FIPC, officials store and maintain electronic, microfilm, and paper records of OPM-conducted background investigations. Officials at FIPC make security clearance information available to federal personnel offices through a Web portal. FIPC receives requests for investigations from federal agencies, processes the requests through an automated system, and fields questions about its process and ongoing investigations.

Security Clearances and Background Investigations Vary in Breadth and Methods Used to Collect Information

Security clearances are required for access to national security information, which may be classified at one of three levels: confidential, secret, and top secret. The level of classification denotes the degree of protection required for information and the amount of damage that unauthorized disclosure could reasonably be expected to cause to national security. Unauthorized disclosure could reasonably be expected to cause (1) “damage,” in the case of confidential information; (2) “serious damage,” in the case of secret information; and (3) “exceptionally grave damage,” in the case of top secret information.²

¹Moderate and high-risk positions refer to the potential for moderate or exceptionally serious impact to the integrity and efficiency of the service.

²The White House, Exec. Order No. 12958, Classified National Security Information, § 1.3 (Apr. 17, 1995) (as amended), 5 C.F.R. §1312.4 (2008).

Background investigations allow federal agencies to make decisions both about suitability for employment, as well as access to national security information. The scope of information gathered in an investigation depends on the purpose of the investigation, such as whether it is being conducted for an employment suitability determination, an initial clearance, or a clearance renewal. For example, investigators collect information from agencies such as the Federal Bureau of Investigation (FBI) for all initial and renewal clearances. However, for initial top secret clearances investigators need, among other things, to also corroborate the subject's education and interview educational sources, as appropriate.

For an investigation for a confidential or secret clearance, investigators gather much of the information electronically. For an investigation for a top secret clearance, investigators gather additional information through more time-consuming efforts such as conducting in-person interviews to corroborate information about a subject's employment and education. In 2009, OPM estimated that approximately 6-10 labor hours were needed for each investigation for a secret or confidential clearance, and 50-60 labor hours were needed for the investigation for an initial top secret clearance.

Key Laws and Privacy Practices Govern the Protection of Personal Information

The primary laws that provide privacy protections for personal information accessed or held by the federal government are the Privacy Act of 1974 and E-Government Act of 2002. These laws describe, among other things, agency responsibilities with regard to protecting PII.³ The Privacy Act places limitations on agencies' collection, disclosure, and use of personal information maintained in systems of records. A system of records is a collection of information about individuals under control of an agency from which information is retrieved by the name of an individual or other identifier. The E-Government Act of 2002 requires agencies to assess the impact of federal information systems on individuals' privacy. Specifically, the E-Government Act strives to enhance the protection of personal information in government information systems and information collections by requiring agencies to conduct privacy impact assessments (PIA).

³For purposes of this report, the terms personal information and personally identifiable information are used interchangeably to refer to any information about an individual maintained by an agency, including (1) any information that can be used to distinguish or trace an individual's identity, such as name, Social Security number, date and place of birth, mother's maiden name, or biometric records, and (2) any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information.

A PIA is an analysis of how personal information is collected, stored, shared, and managed in a federal system. Specifically, according to Office of Management and Budget (OMB) guidance,⁴ the purpose of a PIA is (1) to ensure handling conforms to applicable legal, regulatory, and policy requirements regarding privacy; (2) to determine the risks and effects of collecting, maintaining, and disseminating information in identifiable form in an electronic information system; and (3) to examine and evaluate protections and alternative processes for handling information to mitigate potential privacy risks.

The Privacy Act of 1974 is largely based on a set of internationally recognized principles for protecting the privacy and security of personal information known as the Fair Information Practices. A U.S. government advisory committee first proposed the practices in 1973 to address what it termed a poor level of protection afforded to privacy under contemporary law.⁵ The Organization for Economic Cooperation and Development (OECD)⁶ developed a revised version of the Fair Information Practices in 1980 that has, with some variation, formed the basis of privacy laws and related policies of many countries—including the United States, Australia, and New Zealand—and the European Union.

These practices are now widely accepted as a standard benchmark for evaluating the adequacy of privacy protections. The eight principles of the Fair Information Practices are shown in table 1.

⁴OMB, Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002, Memorandum M-03-22 (Washington, D.C., Sept. 26, 2003).

⁵U.S. Department of Health, Education, and Welfare, *Records, Computers and the Rights of Citizens: Report of the Secretary's Advisory Committee on Automated Personal Data Systems* (Washington, D.C., July 1973).

⁶OECD, *Guidelines on the Protection of Privacy and Transborder Flow of Personal Data* (Sept. 23, 1980). OECD plays a prominent role in fostering good governance in the public service and in corporate activity among its 30 member countries. It produces internationally agreed-upon instruments, decisions, and recommendations to promote rules in areas where multilateral agreement is necessary for individual countries to make progress in the global economy.

Table 1: Fair Information Practices

Principle	Description
1. Collection limitation	The collection of personal information should be limited, should be obtained by lawful and fair means, and, where appropriate, with the knowledge or consent of the individual.
2. Data quality	Personal information should be relevant to the purpose for which it is collected, and should be accurate, complete, and current as needed for that purpose.
3. Purpose specification	The purposes for the collection of personal information should be disclosed before collection and upon any change to that purpose, and its use should be limited to those purposes and compatible purposes.
4. Use limitation	Personal information should not be disclosed or otherwise used for other than a specified purpose without consent of the individual or legal authority.
5. Security safeguards	Personal information should be protected with reasonable security safeguards against risks such as loss or unauthorized access, destruction, use, modification, or disclosure.
6. Openness	The public should be informed about privacy policies and practices, and individuals should have ready means of learning about the use of personal information.
7. Individual participation	Individuals should have the following rights: to know about the collection of personal information, to access that information, to request correction, and to challenge the denial of those rights.
8. Accountability	Individuals controlling the collection or use of personal information should be accountable for taking steps to ensure the implementation of these principles.

Source: OECD.

The Fair Information Practices are not precise legal requirements. Rather, they provide a framework of principles for balancing the need for privacy with other public policy interests, such as national security, law enforcement, and administrative efficiency. Ways to strike that balance vary among countries and according to the type of information under consideration.

OPM and FIS Have Implemented Privacy Protection Structures and Policies

The OPM Privacy Office is tasked with ensuring that the agency is in compliance with privacy laws by providing guidance on how to implement privacy provisions needed to protect personal information. To oversee its implementation of privacy protections, OPM has designated its Chief Information Officer (CIO) as its senior agency official for privacy.⁷ The CIO, in turn, uses the Privacy Program Manager to assist in providing oversight to ensure the agency is complying with privacy policies and guidance. Among other things, the Privacy Program Manager is responsible for developing policies and procedures for the development of PIAs as well as reviewing and recommending their approval.

Within each OPM division, information system owners are responsible for implementing OPM's privacy policies and guidance. To assist division-level officials in assessing potential privacy risks and protecting personal information, OPM's Privacy Office established guidance for conducting PIAs. The guidance includes a template consisting of two parts: (1) an initial screening assessment tool to determine whether system owners are required to complete a PIA and (2) the PIA itself, which requires system owners to answer seven basic questions about the nature of their systems in addition to their intended uses and purposes for collecting personal information. Upon completion of the PIA template, system owners are required to submit PIAs to the Privacy Program Manager for evaluation and recommendation for approval to the CIO. According to OPM guidance, the CIO is responsible for reviewing and signing all OPM PIAs, which signify that a PIA is complete and can be posted to OPM's Web site for public viewing.

Additionally, OPM has developed and issued an agency-wide information security and privacy policy for both its federal and contractor employees to follow in protecting information resources from loss, theft, misuse, and unauthorized access.

To supplement guidance provided by the OPM Privacy Office, FIS also has developed a *Policy on the Protection of Personally Identifiable Information (PII)* to provide employees, including contractors, with a description of their responsibilities in protecting PII and reporting PII breaches. FIS also requires its investigators to adhere to its *Investigator's*

⁷As directed by OMB Memorandum M-05-08, the senior agency official for privacy is responsible for, among other things, ensuring agency compliance with all federal privacy laws and has responsibility for playing a central policy-making role in the development of policy proposals that implicate privacy issues.

Handbook for procedures and policies related to conducting personnel background investigations for the federal government. These two documents guide federal and contract investigators in the protection of PII during the course of their work.⁸ These documents specify procedures that align with the Fair Information Practices. For example, the documents direct investigators to protect PII they possess at their duty stations using a “two-barrier” approach, such as storing it within a locked desk that is located inside of a locked house, which aligns with the *security safeguards* principle.

In addition to its policies and guidance, FIS promotes awareness of privacy protection requirements through PII training and agency newsletters. For example, to support the agency’s initiative to reduce privacy breaches, employees participated in a “no breach” week initiative to help ensure that FIS policies and guidance were being followed.

Previous Inspector
General Review
Recommended
Improvements for the
Protection of PII

In April 2009, the OPM Office of the Inspector General (OIG) completed an audit of the security of PII within the FIS division and made nine recommendations to improve the protection of these data.⁹ The OPM OIG reviewed FIS controls for the storage, security, and transmission of PII. The OIG’s report identified, among other things, that (1) required security awareness and PII training had not been completed by all FIS employees and contractor staff; and (2) FIS did not have adequate controls for ensuring that PII incidents were reported by FIS employees and contractors in a timely manner. In response to the OIG’s recommendations, FIS recently established a security and PII training program and required all employees and contractors to complete PII awareness training. Furthermore, to better ensure PII incidents are properly reported, FIS updated its incident response procedures to require supervisors to ensure that employees and contractors report incidents to the OPM Situation Room—the agency’s central repository for PII incidents—within 30 minutes of identifying a breach or loss.

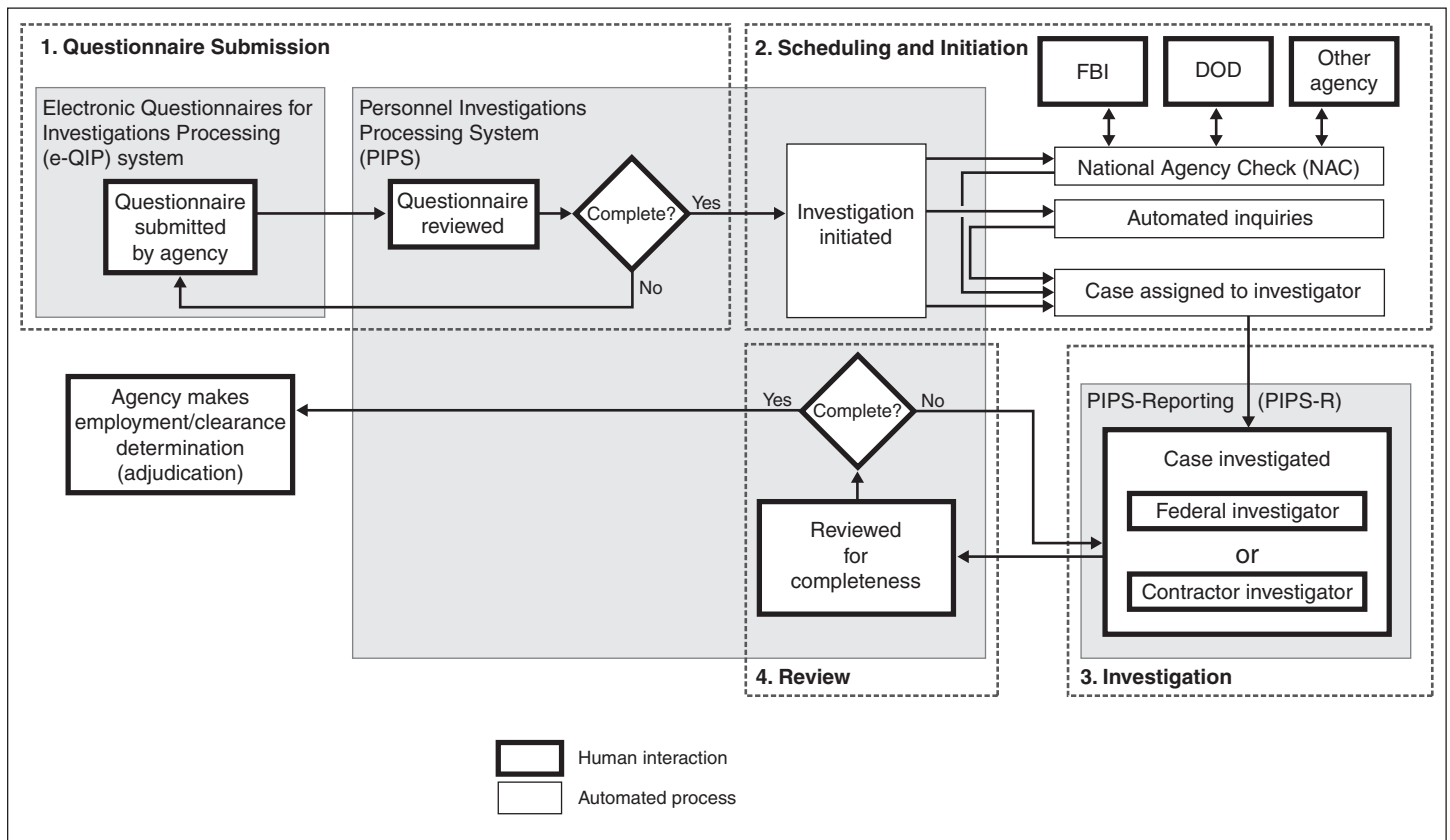
⁸OPM, *Investigator’s Handbook* (July 2007); OPM, *Policy on the Protection of Personally Identifiable Information (PII)* (Nov. 15, 2009).

⁹OPM OIG, *Audit of the Security of Personally Identifiable Information in the Federal Investigative Service Division of the U.S. Office of Personnel Management*, Report No. 4A-IS-00-08-014 (Apr. 21, 2009).

OPM's Background Investigation Process Involves Extensive Collection and Use of PII

FIS conducts background investigations using extensive amounts of PII collected from a variety of sources. FIS uses a combination of automated and manual steps during the course of a background investigation. These steps can be categorized into four distinct phases: (1) Questionnaire Submission, (2) Scheduling and Initiation, (3) Investigation, and (4) Review. Figure 1 provides an overview of the background investigation process delineating these four phases.

Figure 1: Key Steps in FIS's Background Investigation Process



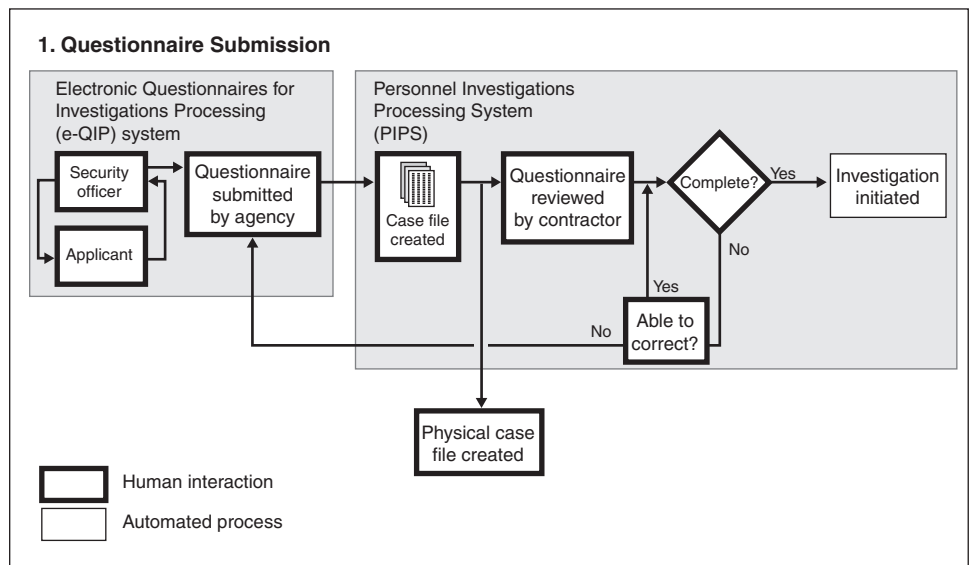
Source: GAO analysis of OPM data.

The following sections outline detailed steps and how PII is used within each of the phases of FIS’s background investigation process and the measures taken within each phase to protect PII.

Phase 1: Questionnaire Submission

In order to initiate an investigation, a questionnaire must be submitted with the required information and accepted by FIS. Figure 2 shows detailed steps in the questionnaire submission phase.

Figure 2: Questionnaire Submission Phase Detailed Steps



Source: GAO analysis of OPM data.

1. A security officer at the requesting agency forwards to the subject—the individual who will be investigated—an investigative questionnaire, which seeks information on the subject’s personal history and includes identifying information such as the subject’s first and last name, Social Security number, and place and date of birth. In addition, subjects are asked to provide personal information on family members, friends, and other contacts. The questionnaire can be completed either electronically using OPM’s Electronic Questionnaires for Investigations Processing (e-QIP) system or in paper form. Most questionnaires are currently completed electronically.
2. The completed questionnaire is reviewed by the originating agency’s security office and then sent with supporting documentation, such as fingerprints, to FIS. If a questionnaire is submitted electronically using

e-QIP, it is automatically uploaded into the Personnel Investigations Processing System (PIPS), a FIS system containing over 15 million background investigation records of federal employees, military personnel, and contractors used for the automated entry, scheduling, case control, and closing of background investigations. Should FIS receive a paper questionnaire, the information is manually entered into PIPS.

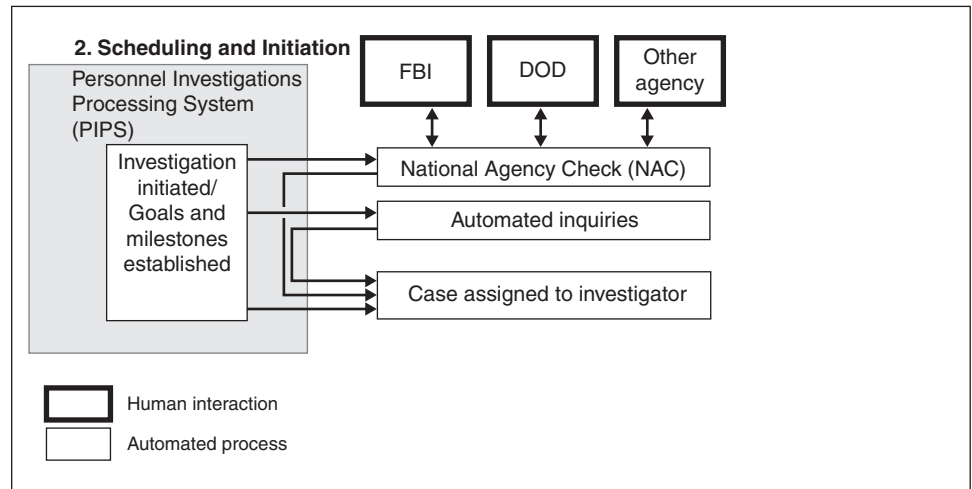
3. Once a questionnaire is received at FIPC, a physical case file is created that contains the questionnaire, a summary sheet,¹⁰ and any documentation provided as a supplement to the questionnaire.
4. Before the investigation is initiated, the questionnaire must pass a review by a FIS contractor for completeness and identification of any obvious errors. If there is missing or erroneous information, or required attachments that are missing, such as fingerprints, FIS contractors first attempt to correct this with the agency. If this is unsuccessful, the investigation request is returned to the agency. If the questionnaire is deemed complete, the contractor completes the on-line screening or data entry process in PIPS to initiate the investigation.

¹⁰The summary sheet allows FIS contractors to quickly see the case number, the name of the subject, and if there are any attachments with the questionnaire.

Phase 2: Scheduling and Initiation

After a questionnaire is accepted by FIS, the associated investigation is scheduled and initiated. Figure 3 represents detailed steps in this phase.

Figure 3: Scheduling and Initiation Phase Detailed Steps



Source: GAO analysis of OPM data.

Once online screening or data entry is completed, PIPS initiates a four-step scheduling process:

1. Goals and milestones are established for the initial security clearance investigation to comply with statutory requirements. Investigation timelines are based on provisions of the Intelligence Reform and Terrorism Prevention Act of 2004, which required adjudicative agencies to develop plans to ensure that, to the extent practical, determinations could be made on at least 90 percent of all applications for a security clearance within 60 days, with no longer than 40 days allotted for the investigation and 20 days allotted for the adjudication.¹¹
2. PIPS requests information through a National Agency Check (NAC): a set of queries sent to national record repositories, such as OPM, the

¹¹Pub. L. No. 108-458, § 3001(g) (2004). Executive Order 13467 defines adjudication as the evaluation of pertinent data in a background investigation, as well as any other available information that is relevant and reliable, to determine whether an individual is (1) suitable for government employment; (2) eligible for logical and physical access; (3) eligible for access to classified information; (4) eligible to hold a sensitive position; or (5) fit to perform work for or on behalf of the government as a contractor employee.

FBI, and Department of Defense (DOD) investigation databases; and a fingerprint-based criminal history check through the FBI.¹² Once the agencies have manually or electronically checked their databases for the information, the results are returned to FIS headquarters and stored in PIPS or in the physical case file after being scanned into PIPS. The results returned to FIS can include FBI fingerprint and investigation records, DOD investigations records, and the subject's credit history.

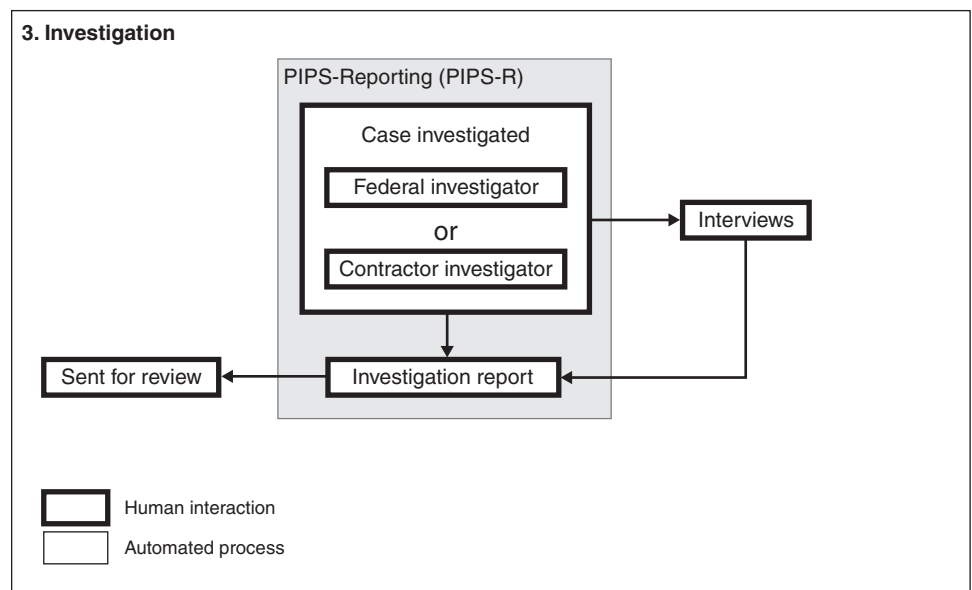
3. PIPS automatically readies inquiries in the form of scannable inquiries that are mailed to a variety of entities—including universities and local law enforcement—and individuals listed as contacts by the subject. The inquiries include questions concerning the subject's character and what association an entity or individual had with the subject. Once a recipient returns the completed scannable inquiries, FIS uses high-speed scanners to upload these data into PIPS.
4. PIPS automatically assigns the investigation to a field office based on the zip code for the activities to be covered. A supervisory agent in charge at the office assigns the items to be completed to a specific investigator. Often, work is assigned to multiple investigators who are responsible for conducting the investigation. Processes exist to reassign a case if there is a better located investigator. The investigators assigned to conduct the field work for the investigation may be contractors or federal employees. When the investigator receives the assignment, he or she is provided the case papers in hard copy or electronic form. The investigator may also receive a summary of the NAC items once they have been completed.

¹²Other sources can include military personnel records, official personnel folders and information obtained from Citizenship and Immigration Services, investigative agencies, federal agency security offices, and the Central Intelligence Agency.

Phase 3: Investigation

Once assigned to the case, an investigator receives the case information and conducts the investigation of the subject. The detailed steps for the Investigation phase are displayed in Figure 4.

Figure 4: Investigation Phase Detailed Steps



Source: GAO analysis of OPM data.

1. When an investigator has been assigned a case in PIPS, he or she can access the case information maintained in the system. The investigator can input the results of the interviews and record checks into templates in PIPS-Reporting (PIPS-R)—a computer application housed on the investigator's laptop computer, which is used to electronically document the investigation and transmit the investigation report electronically to FIPC. PIPS-R temporarily stores the report of investigation, while the physical case file is maintained at FIPC.
2. Investigators gather information on the subject including data about the subject received during interviews with the contacts listed in the questionnaire. Investigators share limited personal information on a subject with identified contacts during an interview. Information obtained from these interviews includes character descriptions and details of any criminal activities. The information is used to determine the accuracy of subject-provided information and generate further leads to complete an investigation. This part of the process may take

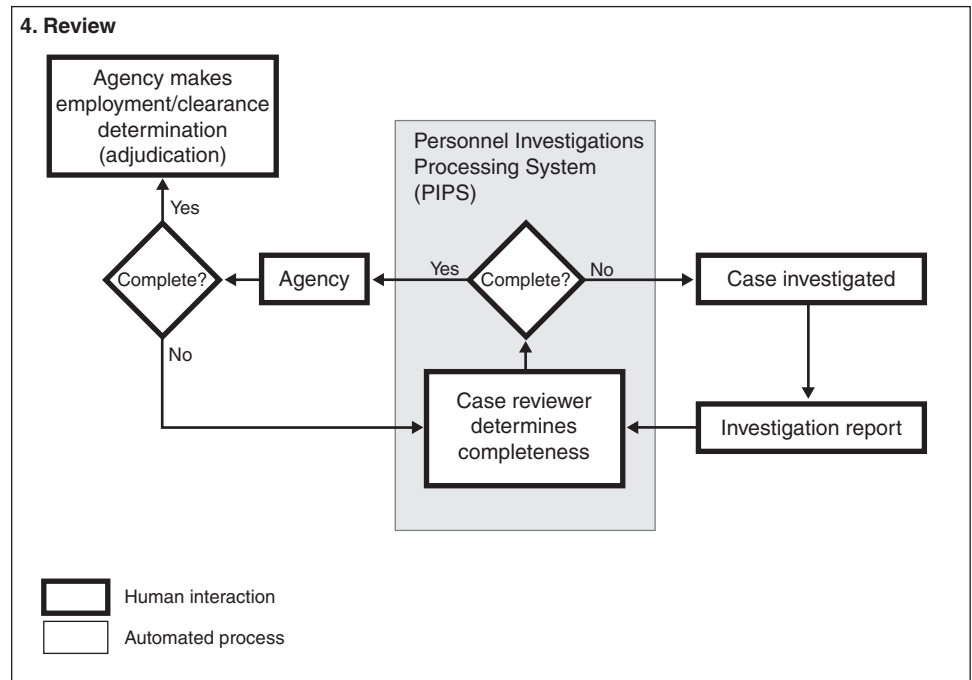
several weeks, as investigators attempt to contact and interview multiple contacts. PIPS-R requires the investigators to enter information into templates that allow PIPS-R to compile the information into a report.

3. Upon completion of the investigation, the investigator closes the case in PIPS-R and electronically transfers the data into PIPS. The investigator then delivers the case notes to an assigned regional investigations office, where the notes are shredded 30 days after the case is closed. The report in PIPS-R is manually deleted by the investigator 30 days after the case is closed.

Phase 4: Review

Upon the completion of the field work by the investigators, a case review is initiated to ensure the investigative report is complete. Figure 5 outlines detailed steps in the Review phase.

Figure 5: Review Phase Detailed Steps



Source: GAO analysis of OPM data.

-
1. A case reviewer at FIPC determines the completeness of the investigation and identifies any inconsistencies, errors, and omissions in the investigator's report. For example, if the investigator did not corroborate the subject's education, the investigator may need to interview educational sources.
 2. Should the reviewer identify any discrepancies or omissions, the case is returned to the investigator for correction, sometimes through additional field work.
 3. If the reviewer determines that the case is completed, FIS closes the case and provides a summary report to the agency that requested the investigation for adjudication. Currently this is done by mailing a hard copy of the report to the agency or using electronic delivery with agencies that have signed up for electronic dissemination.
 4. The agency may return an investigation to FIS for further work if it does not provide the information necessary to make an adjudication decision.
 5. The investigation information is kept by FIS for varying time periods. The main case file within FIPC is scanned and saved as an electronic image within 30 days of a case closing. After 30 days, the physical case file, along with the investigator's notes, and PIPS-R records are destroyed. The scanned file is maintained either electronically or on microfilm, according to OPM's retention guidelines, for 16 or 25 years if potentially actionable issues exist or unless the record becomes part of a new investigation.

FIS Has Taken Steps to Ensure Privacy Policies and Procedures Meet Statutory Requirements and Align with Fair Information Practices, but Oversight of Implementation is Limited

FIS has taken steps to incorporate key privacy principles into policies and procedures that guide and direct agency officials in performing background investigations. Specifically, FIS has complied with requirements of the Privacy Act and E-Government Act by publishing information on its use of PII and by conducting privacy impact assessments of its major information systems. However, it has not assessed the risks associated with the use of PII, an important element of conducting a privacy impact assessment. In addition, while FIS policies and practices for conducting investigations generally align with the Fair Information Practices, the agency has exercised only limited oversight of the use of PII by its field investigators and customer agencies.

OPM Privacy Policies Meet Statutory Requirements, but the Agency does not Assess Privacy Risks of Handling PII

The major requirements for the protection of personal privacy by federal agencies come from two laws, the Privacy Act of 1974 and the privacy provisions of the E-Government Act of 2002. Under the Privacy Act, federal agencies must issue public notices, known as System of Records Notices (SORN), in the *Federal Register* identifying, among other things, the type of data collected, the types of individuals about whom information is collected, and procedures that individuals can use to review and correct personal information. To address Privacy Act requirements, OPM published two SORNs that apply to FIS's information systems, known as the *Central 9* and *Internal 16* notices. These notices include—among other things—a description of FIS's purpose for collecting and using personal information and how individuals can access and correct information maintained about them. For example, both SORNs state that individuals can request access to records by writing to FIPC.

In addition to notice requirements established by the Privacy Act, federal agencies are tasked by the E-Government Act to conduct privacy impact assessments (PIA) to ensure the protection of PII. As described earlier, a PIA is an analysis of how personal information is collected, stored, shared, and managed in a federal system. In response to these requirements, OMB has developed guidance for agencies on conducting PIAs.

Assessing privacy risks is an important element of a PIA intended to help program managers and system owners determine appropriate privacy

protection policies and techniques to implement those policies. A privacy risk analysis should be performed to determine the nature of privacy risks and the resulting impact if corrective actions are not in place to mitigate those risks. For example, in ensuring that personal information is used only for specified purposes—the *use limitation* principle—system owners should identify potential ways in which unauthorized use could occur and implement privacy controls to prevent disclosure of personal data for such uses.

OPM has developed assessments for a number of systems throughout the agency. For example, assessments for key FIS systems such as PIPS and e-QIP have been developed and approved by OPM’s Chief Privacy Officer. These assessments were last revised in August 2007.

Although OPM developed PIAs for each of the key FIS background investigation systems, it did not assess the risks associated with the handling of PII within the systems or identify mitigating controls to address risks. For example, the assessment prepared for PIPS provided general descriptions of system functions—such as that sources of information will be “directly from the person to whom the information pertains, from other people, other sources, such as databases, Web sites, etc.”—but did not include analysis of privacy risks associated with this broad collection of personal information. Without analyzing privacy risks, agency officials may be forgoing opportunities to identify measures that could be taken to mitigate them and enhance privacy protections.

Current OPM guidance on PIAs does not instruct divisions to conduct privacy risk analysis. Instead it directs officials to answer general questions for each system to aid OPM’s Privacy Office in assessing potential privacy risks. While OPM guidance emphasizes the need for system owners to provide detailed information in response to questions, the guidance does not instruct system owners to assess privacy risks. Until the current guidance is revised to require risk analysis and new and existing PIAs are updated to include risk analyses, OPM will continue to have limited assurance that PII contained in its systems is being properly protected from potential privacy threats.

FIS Has Taken Steps to Institute Protections that Align with the Fair Information Practices

FIS has taken steps to include privacy protections in its procedures for conducting background investigations. Privacy protections can be categorized in relation to the Fair Information Practices, which, as discussed earlier, form the basis for privacy laws such as the Privacy Act. In a number of cases, the protections instituted by FIS can be aligned with the Fair Information Practices. For example, the agency’s publication of

privacy notices addresses the *openness* and *individual participation* principles. The principles can be applied in varying degrees to all FIS activities that involve PII. The following are selected FIS procedures that illustrate specific ways in which the Fair Information Practices have been addressed.

- *Collection limitation.* FIS investigators are directed to limit the PII they collect and include in their investigation reports to information directly relevant to the assigned investigation. Investigators do not report PII in the investigation reports unless they develop information that varies from the subject-provided information. If an investigator collects information that is not vital, he or she is to destroy the information at the end of the investigation. This information is included with the investigator's notes and returned to the supervisor's office when the investigator has completed his or her portion of the case. The information is then destroyed 30 days after the case is closed. This aligns with the principle that the collection of PII should be limited.
- *Data quality.* When FIS receives a hard copy questionnaire, two personnel input the same PII data into PIPS. The system then confirms that both inputs match exactly before uploading the questionnaire data into PIPS, thus helping to ensure that the information provided in the hard copy questionnaire is correctly transferred to the electronic system. Additionally, FIS officials review the final investigation report prior to its delivery to the customer agency in order to ensure that the investigator took all of the steps necessary to conduct the investigation and that there are no errors or omissions in the report. Finally, in an effort to ensure completeness of an investigation, a customer agency can request additional investigative work be conducted by FIS if it identifies inaccuracies in the final investigation report or areas that require additional information prior to making an adjudication decision. This aligns with the principle that the collected information should be accurate and complete.
- *Purpose specification.* Questionnaire forms used by FIS—such as the Standard Form 86—include disclaimer language that informs the subject that the information he or she provides will only be used for the purpose of the specific background investigation and lists the reasons the information may be disclosed. Further, automated inquiry forms sent out during the Scheduling and Initiation phase contain disclaimer language that specifies that information provided on the forms will be used solely for the related investigation. This aligns with the principle that the

purposes of an information collection should be disclosed before collection.

- *Use limitation.* FIS agreements with customer agencies limit how background investigation reports may be used by stating that information provided by FIS should be used only for the purpose of adjudication. Additionally, all attempts to access case files within PIPS (e.g., viewing or editing) are recorded in an automated log file. These logs are reviewed daily by FIS personnel to identify unauthorized access attempts that violate agency restrictions on use. This aligns with the principle that the information should not be disclosed or used for anything other than the specified purpose.
- *Security safeguards.* FIS uses a collection of security safeguards to protect and control access to PII located physically at FIPC. Physical security controls and processes include (1) screening individuals with metal detectors and x-ray machines prior to entry to the facility; (2) using electronically coded cards and badges to grant access to the room containing hard copies of active case files; (3) checking manifests of case files mailed to other facilities to ensure that the contents of the files have not changed; and (4) ensuring the proper destruction of investigative materials with locked disposal bins and supervised shredding by a FIS official. FIS officials also reported that a number of information security measures are used to protect personal information maintained in FIS systems.¹³ For example, FIS policy requires that access to PIPS is to be limited to officials who are authorized by their respective agencies' security offices and have appropriate background investigations.¹⁴ The system is also to restrict agency user access to information from cases they have been specifically authorized to review. Furthermore, officials stated that annual security assessments are conducted on all FIS systems to ensure that they are compliant with governmentwide information security control standards, including National Institute of Standards and Technology (NIST) Special Publication 800-53¹⁵ and Federal Information

¹³Due to the scope of our review, we did not test the effectiveness of physical and information security controls.

¹⁴An approved user located at FIPC can directly access the system using his or her assigned unique username and password. If accessing the system remotely, users are required to log into a FIS Web portal prior to logging onto PIPS.

¹⁵National Institute of Standards and Technology, *Information Security: Recommended Security Controls for Federal Information Systems*, NIST Special Publication 800-53 (Gaithersburg, Md., August 2009).

Processing Standard (FIPS) 140-2.¹⁶ This aligns with the principle that information should be protected with security safeguards against risks such as unauthorized access, use, or modification.

FIS Oversight of the Implementation of Privacy Protections is Limited

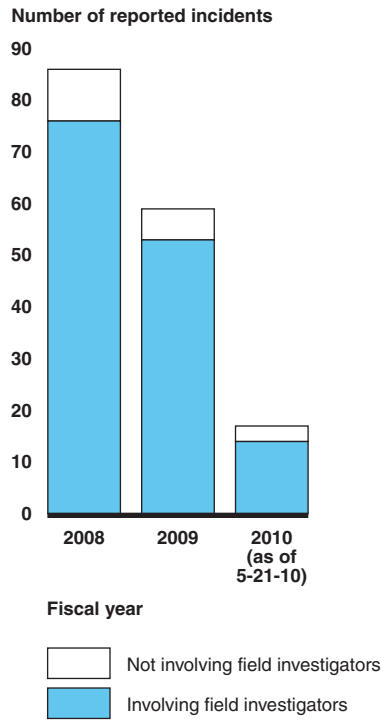
Although FIS has established a number of privacy protection measures for its investigations program that reflect the Fair Information Practices, it has taken limited steps to oversee its field investigators and customer agencies to ensure they are implementing the measures appropriately. Such oversight would align with the *accountability* principle, which states that individuals controlling the collection or use of PII should be accountable for ensuring the implementation of the Fair Information Practices. Without such oversight, it is unclear whether the agency's protection measures are being properly implemented.

FIS Has Not Ensured that Investigators are Following PII Protection Policies and Procedures

In recent years, field investigators have been involved in over 80 percent of reported incidents of lost or stolen paper files in the FIS division (see figure 6). As previously discussed, the more than 7,000 field investigators who conduct background investigations for OPM collect and are responsible for safeguarding extensive amounts of PII. As a result, these field investigators are key to ensuring that PII is properly protected, especially when it is in paper form.

¹⁶National Institute of Standards and Technology, *Security Requirements for Cryptographic Modules*, FIPS PUB 140-2 (Gaithersburg, Md., May 25, 2001).

Figure 6: Reported Incidents of Lost or Stolen Paper Files Associated with Background Investigations



Sources: Federal Investigative Services division, OPM.

Recently, FIS has taken steps to promote better accountability for the protection of personal information provided to and received from investigators. This includes providing training to all employees and holding a “No PII Loss Week,” during which all staff were encouraged to focus on proper handling and storing of PII in their possession.

Oversight of these investigators and FIS employees can ensure that appropriate protections are being implemented for the PII contained in investigative files. Recent recommendations by the OPM OIG highlight the importance of such oversight.¹⁷ In response to recommendations by the OIG to conduct oversight, FIS officials began conducting periodic checks

¹⁷OPM OIG, *Audit of the Security of Personally Identifiable Information in the Federal Investigative Service Division of the U.S. Office of Personnel Management*, Report No. 4A-IS-00-08-014 (Apr. 21, 2009).

of documents received from investigators once an investigation is closed to encourage a full and proper accounting of PII.

However, FIS officials had not monitored whether investigators are following agency policies described in the *Investigator's Handbook* and the *Policy On The Protection Of Personally Identifiable Information (PII)* for handling PII while investigative activity is underway. Officials from the agency's oversight groups responsible for federal and contract investigators said they used other methods for determining investigators' adherence to PII protection requirements. For example, officials stated the investigators are required to report to their supervisors daily on the case information or other PII they have with them during the course of their work. This is to account for the information they have on hand if there is a loss or the investigator becomes incapacitated due to an accident or medical emergency. The tallies provided by the investigators are intended to allow their supervisors to account for all such information. In addition, officials from FIS oversight units recently began conducting physical audits of regional field offices to determine compliance with PII requirements.

Although these recent efforts may increase assurance that investigators are adequately accounting for the investigative files in their possession, no process currently exists to monitor investigators' compliance with FIS privacy protection policies as they perform their field work. For example, FIS does not have procedures for examining how investigators protect information while traveling to conduct interviews or how they ensure that only appropriate information is being gathered. Without an oversight mechanism to ensure investigators' adherence to PII protection policies during investigations—such as through periodic, structured evaluations by supervisors—the agency lacks assurance that sensitive information is being handled appropriately during this critical phase of the background investigation process.

FIS Has Not Monitored Customer Agencies' Implementation of Privacy Protections

We previously reported on the federal legal framework for privacy protection, including issues and challenges associated with ensuring compliance with privacy protections when PII is transferred among agencies.¹⁸ We highlighted the need for an effective oversight structure to monitor how PII is protected. For example, requiring agencies to establish

¹⁸GAO, *Privacy: Alternatives Exist for Enhancing Protection of Personally Identifiable Information*, GAO-08-536 (Washington, D.C.: May 19, 2008).

agreements with external government entities before sharing PII is a practical method that enables an agency's privacy controls to be forwarded to its recipients, thus offering assurance that personal information is adequately protected from privacy risks following the data transfer. Designating entities within those agreements who are responsible for ensuring the proper implementation of privacy requirements is also consistent with the Fair Information Practice of *accountability*, which calls for those who control the collection or use of personal information to be held accountable for taking steps to ensure it is protected.

FIS relies on memoranda of understanding (MOU) with its customer agencies to establish procedures and policies for protecting PII related to background investigation case files, and these agreements specifically designate OPM as being responsible for ensuring that customer agencies comply with the requirements of the Privacy Act when handling PII received from OPM. Within these agreements, FIS outlines, among other things, system security controls, appropriate uses of investigative information, and other provisions for adherence to the Privacy Act. For example, the agency's e-Delivery system—an information system used to electronically assemble and deliver closed case files from FIS to requesting agencies—includes a description of security and privacy expectations and responsibilities necessary for agencies to utilize the system.

However, OPM has not taken any steps to carry out its responsibility for ensuring that personal information is protected at customer agencies. Specifically, it does not monitor customer agencies' adherence to the requirements agreed upon through the MOUs. FIS officials stated that they visit customer agencies on a recurring basis to review other aspects of the agreements but that reviews of customer agencies' privacy protection measures take place only if a potential compromise of PII has been identified. Although these frequent visits to customer agencies provide opportunities for OPM to ensure that customer agencies are protecting PII properly, without focusing on privacy protections outlined within the MOUs as a key element of its established process, OPM may not be meeting its responsibility to ensure that agencies comply with the requirements of the MOU. As a result, OPM may not have reasonable assurance that the personal information contained within background investigation files is being appropriately used and adequately protected by customer agencies.

Conclusions

OPM and FIS have incorporated key privacy principles into their processes and documentation that guide agency officials in the performance of background investigations. Key agency activities include measures addressing the Fair Information Practices, and steps have been taken to meet requirements of the Privacy Act and the E-Government Act.

However, limited oversight of the implementation of key processes reduces assurances that PII is properly protected. Current OPM guidance does not require assessments of the privacy impact of FIS systems to be accompanied by privacy risk analyses. Until the guidance requires privacy risk analyses with PIAs and existing PIAs are revised to include privacy risk analyses, OPM will continue to have limited assurance that PII contained in its systems is being properly protected.

While FIS has policies and procedures to protect PII used by its field investigators, there is no process to assess the level of protection of PII provided by these investigators while investigative activity is underway. Without an oversight mechanism that directly assesses investigators' adherence to OPM PII protection policies, the agency lacks assurance that PII is being properly protected.

Finally, OPM does not actively monitor customer agency adherence to requirements for protecting PII as established in MOUs it has with its customers. As a result, FIS may not have reasonable assurance that the personal information contained within background investigation files is being appropriately used and adequately protected by customer agencies.

Recommendations for Executive Action

To ensure that appropriate privacy protections are in place during all stages of a background investigation, we recommend that the Director of the OPM take the following four actions:

- develop guidance for privacy impact assessments that directs agency officials to perform an analysis of privacy risks and identify mitigating techniques for all FIS systems that access, use, or maintain PII;
- ensure that all existing PIAs are revised to adhere to this guidance;
- perform periodic, structured evaluations to ensure that field investigators handle and protect PII according to agency policies and procedures while conducting their investigations; and

-
- develop and implement procedures for monitoring customer agencies' adherence to the privacy provisions agreed to within memoranda of understanding.

Agency Comments and Our Evaluation

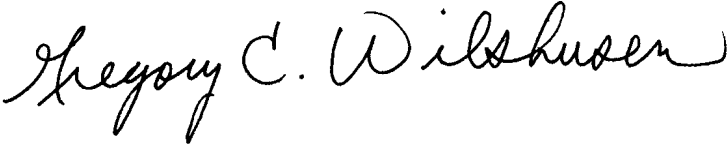
In written comments on a draft of this report transmitted via e-mail by the GAO audit liaison, OPM agreed with our recommendations. However, OPM disagreed with the report's finding regarding protection of PII by field investigators, stating that it was written in a way that suggested that there is no oversight or monitoring. OPM noted that it recently implemented procedures for checking compliance by both federal and contract investigators to agency PII protection requirements. OPM requested that language in the report be modified to recognize these recent efforts.

We adjusted language within our report to clarify the nature of OPM's oversight activities at the time of our review. In addition, the draft report highlighted such recent efforts by FIS to monitor investigator compliance, including daily checks by supervisors of investigator inventories of case information and the division's recently developed program for conducting physical audits of regional field offices to determine compliance with PII requirements. Nevertheless, these recent efforts by FIS have yet to demonstrate that investigators are monitored for compliance while conducting investigations. For example, FIS had yet to develop procedures for examining how investigators protect information while traveling to conduct interviews or how they ensure that only appropriate information is being gathered.

In addition, OPM provided technical comments that were addressed as appropriate.

As agreed with your office, unless you publicly announce the contents of this report earlier, we plan no further distribution until 30 days from the report date. We will then send copies of this report to interested congressional committees and the Director of the Office of Personnel Management. The report also is available at no charge on the GAO Web site at <http://www.gao.gov>.

If you or your staff have any questions regarding this report, please contact me at (202) 512-6244 or at wilshuseng@gao.gov. Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this report. Key contributors to this report are listed in appendix II.

A handwritten signature in black ink that reads "Gregory C. Wilshusen". The signature is written in a cursive style with a large, prominent 'G' and 'W'.

Gregory C. Wilshusen
Director, Information Security Issues

Appendix I: Objectives, Scope, and Methodology

Our objectives were to determine:

- how the Office of Personnel Management (OPM) uses personally identifiable information (PII)¹ in conducting background investigations, and
- 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 our first objective, we identified key steps in the agency's background investigation process by analyzing OPM and Federal Investigative Services (FIS) division policies, procedures, and guidance; conducting site visits of FIS headquarters at the Federal Investigations Processing Center (FIPC) in Boyers, Pennsylvania; and interviewing FIS officials involved in overseeing and conducting key steps in the process located at FIPC and at OPM headquarters. We compiled a four-phase description of the investigation process and confirmed the accuracy of its contents with FIS officials in an iterative fashion.

To address our second objective, we reviewed OPM and FIS privacy policies and procedures and analyzed agency actions to (1) comply with the Privacy Act of 1974 and the E-Government Act of 2002 and (2) align with the Fair Information Practices, a set of widely accepted privacy principles. We interviewed OPM's Chief Information Officer in order to obtain information on OPM policies and procedures on the protection of PII and how OPM monitors compliance with its privacy policies and procedures. We also interviewed key FIS officials, including those from the agency's Field Management Oversight Group, Contract Development and Oversight Group, and the Memorandum of Understanding/Liaisons Group, to discuss their practices and procedures for protecting personal information when performing their oversight responsibilities. Additionally, we reviewed previous GAO and OPM Office of the Inspector General reports pertinent to engagement objectives.

¹For purposes of this report, the terms personal information and personally identifiable information are used interchangeably to refer to any information about an individual maintained by an agency, including (1) any information that can be used to distinguish or trace an individual's identity, such as name, Social Security number, date and place of birth, mother's maiden name, or biometric records, and (2) any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information.

We conducted this performance audit from October 2009 to September 2010 in the Washington, D.C., and Boyers, Pennsylvania, areas, in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Appendix II: GAO Contact and Staff Acknowledgments

GAO Contact

Gregory C. Wilshusen, (202) 512-6244 or wilshuseng@gao.gov

Staff Acknowledgments

In addition to the contact above, John de Ferrari, Assistant Director; Sher`rie Bacon; Neil Doherty; Matthew Grote; Nicholas Marinos; Lee McCracken; David Plocher; and Jeffrey Woodward made key contributions to this report.

GAO's Mission

The Government Accountability Office, the audit, evaluation, and investigative arm of Congress, exists to support Congress in meeting its constitutional responsibilities and to help improve the performance and accountability of the federal government for the American people. GAO examines the use of public funds; evaluates federal programs and policies; and provides analyses, recommendations, and other assistance to help Congress make informed oversight, policy, and funding decisions. GAO's commitment to good government is reflected in its core values of accountability, integrity, and reliability.

Obtaining Copies of GAO Reports and Testimony

The fastest and easiest way to obtain copies of GAO documents at no cost is through GAO's Web site (www.gao.gov). Each weekday afternoon, GAO posts on its Web site newly released reports, testimony, and correspondence. To have GAO e-mail you a list of newly posted products, go to www.gao.gov and select "E-mail Updates."

Order by Phone

The price of each GAO publication reflects GAO's actual cost of production and distribution and depends on the number of pages in the publication and whether the publication is printed in color or black and white. Pricing and ordering information is posted on GAO's Web site, <http://www.gao.gov/ordering.htm>.

Place orders by calling (202) 512-6000, toll free (866) 801-7077, or TDD (202) 512-2537.

Orders may be paid for using American Express, Discover Card, MasterCard, Visa, check, or money order. Call for additional information.

To Report Fraud, Waste, and Abuse in Federal Programs

Contact:

Web site: www.gao.gov/fraudnet/fraudnet.htm

E-mail: fraudnet@gao.gov

Automated answering system: (800) 424-5454 or (202) 512-7470

Congressional Relations

Ralph Dawn, Managing Director, dawnr@gao.gov, (202) 512-4400
U.S. Government Accountability Office, 441 G Street NW, Room 7125
Washington, DC 20548

Public Affairs

Chuck Young, Managing Director, youngc1@gao.gov, (202) 512-4800
U.S. Government Accountability Office, 441 G Street NW, Room 7149
Washington, DC 20548

