



**U.S. Department of Justice
Office of the Inspector General
Evaluation and Inspections Division**

**Review of the Security and
Emergency Planning Staff's
Management of
Background Investigations**

September 2005

Report Number I-2005-010

EXECUTIVE SUMMARY

The Department of Justice's (Department) Security and Emergency Planning Staff (SEPS) is the primary office responsible for developing, implementing, and ensuring compliance with security policy throughout the Department. SEPS has direct responsibility for managing background investigations on 27,000 of the Department's 103,000 employees. SEPS has delegated to personnel security staff in the components the authority to adjudicate background investigations and reinvestigations for their employees and contractors, and the authority to grant waivers so new employees can begin work. In total, 20 components have delegated adjudication authority – 7 have the authority for employees and contractors, and 13 have the authority only for contractors.¹

Overall, SEPS has four responsibilities related to background investigations in the Department: (1) managing background investigations of political appointees, attorneys, and other personnel whose investigations are not delegated to the components; (2) granting clearances for access to Sensitive Compartmented Information (SCI) materials for all Department employees; (3) providing policy guidance and training on background investigations; and (4) providing oversight of the components' background investigation programs.²

The Office of the Inspector General (OIG) conducted this review to examine SEPS's management of its background investigation program. Specifically, we reviewed SEPS's administration of the background investigations and security clearances it manages, SEPS's role in establishing Department policy on background investigations, and SEPS's oversight of the background investigations delegated to components.

¹ The Department components with delegated authority to manage the background investigations of employees and contractors are the Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF); Federal Bureau of Prisons (BOP); Drug Enforcement Agency (DEA); Executive Office for United States Trustees (EOUST); Federal Bureau of Investigation (FBI); National Drug Intelligence Center; and United States Marshals Service (USMS). See Appendix I for additional information on components with delegated authority.

² SCI is a security classification that is more restrictive than Top Secret, often covering information that deals with intelligence sources, methods, or activities.

RESULTS IN BRIEF

In fiscal year (FY) 2004, SEPS met federal regulatory requirements for adjudicating background investigations within 90 days in 85 percent of the cases it processed.³ Further, in response to a SEPS survey, Department components expressed satisfaction with the service SEPS provided on SCI clearances and clearance verifications for Department employees and contractors. SEPS achieved these results despite the fact that, after September 11, 2001, SEPS's workload of background investigation adjudications and SCI clearances more than doubled. Because it received no additional resources to process this workload, SEPS prioritized its background investigation adjudications and redirected its resources to the highest priority cases. In FY 2004, SEPS adjudicated 99 percent of its highest priority cases (those of political appointees and attorneys) within the required 90 days.

However, SEPS did not adjudicate lower priority background investigations within the required time. Further, SEPS did not fully meet other important responsibilities related to policy and oversight. Specifically, the Department's personnel security policy – contained in DOJ Order 2610.2A (August 21, 1990) and more than 40 memorandums issued over the past 15 years – is inconsistent, outdated, and not available in electronic form. In addition, SEPS has not implemented an effective oversight program to ensure that components with delegated authority to adjudicate background investigations comply with regulations and policy.

We also found that SEPS has limited ability to electronically track background investigation files. First, SEPS has no capability to maintain electronic copies of background investigation files. Instead, it relies on an outdated inventory system to track its own paper personnel security files, which are maintained in one location. We believe this is an important vulnerability, as all the files could be lost in a fire or other disaster. Second, there is no Department-wide database to track background investigations. This hinders SEPS's ability to effectively monitor the background investigation process in Department components with delegated authority.

³ Adjudication is defined as the final decision on an individual's suitability to hold a particular position.

Moreover, new standards for background investigations contained in the Intelligence Reform and Terrorism Prevention Act of 2004 (Intelligence Reform Act) will significantly change the standards the Department must meet in completing background investigations. The Intelligence Reform Act requires that, by December 2009, 90 percent of background adjudications must be completed within 20 days and 90 percent of field investigations within 40 days. To meet those standards, SEPS will have to greatly expedite its processing of adjudications from its FY 2004 performance levels. In FY 2004, SEPS completed only 46 percent of adjudications within 20 days. SEPS's oversight workload will also increase because it must ensure that the components with delegated authority comply with the requirements in the Intelligence Reform Act.

In the next sections, we provide more detail regarding these findings.

SEPS's Personnel Security Operations

SEPS's Processing of Background Investigations and SCI Clearances. Federal regulations require that the Department adjudicate background investigations and report the results to the Office of Personnel Management (OPM) within 90 days of the completion of the field investigation. In FY 2004, SEPS processed 85 percent of its initial employee adjudications within the required 90 days.

SEPS accomplished these results even though its workload increased significantly in the last 5 years. From FY 2000 through FY 2004, SEPS's background investigation workload almost doubled, from 7,018 actions (such as initiating investigations of new employees or reinvestigations of current employees) in FY 2000 to 13,509 actions in FY 2004. Overall, SEPS processed 55,197 actions on background investigations during those 5 fiscal years. In addition, SEPS's SCI workload increased by 150 percent from calendar year (CY) 2000 through CY 2004. In CY 2000, SEPS cleared or verified clearances for 2,061 Department staff. In CY 2004, SEPS cleared or verified clearances for 5,166 Department staff.

Because SEPS did not receive additional staffing or resources commensurate with its increased workload, it redirected its existing resources to process adjudications and clearances in priority order. SEPS's four highest personnel security priorities are adjudication of background investigation cases involving political appointees and

attorneys, processing requests for SCI access, certification of clearances to other agencies, and processing waivers.⁴

For political appointees and attorneys, in FY 2004 SEPS completed over 99 percent of the adjudications within the required 90 days. There are no established timeliness standards for SEPS's three other highest work priorities. Therefore, to examine SEPS's performance in these areas, we reviewed correspondence between SEPS and OPM, and a customer satisfaction survey conducted by SEPS. OPM and component officials who commented on these topics in SEPS's survey reported that they were generally satisfied with how quickly SEPS provided SCI clearances and clearance verifications, and processed waiver requests.

Although SEPS almost always adjudicated its highest priority cases within the required 90 days, it did not always adjudicate lower priority background investigation cases within that time. For example, in FY 2004 SEPS adjudicated about 80 percent of the background investigations for non-priority employees and only 54 percent of employee reinvestigations in the required time. We also found that SEPS's performance of its other mission responsibilities – related to providing policy guidance and oversight – was lacking.

SEPS's Policy Guidance. The Department's personnel security guidance is inconsistent and outdated. SEPS has not issued a complete revision of the Department's personnel security policy, known as DOJ Order 2610.2A, since it was issued in 1990. The original order remains in effect, but to reflect changes in security regulations and policy that occurred over the past 15 years, SEPS has issued over 40 memorandums to revise, amend, or supplement the guidance in the original order. Some of the guidance has been amended more than once in separate memorandums, making it difficult for users to readily determine which guidance is current.

Further, SEPS staff informed us that some of the guidance contained in the order and memorandums is outdated because it has not been revised to reflect current security requirements. In December 2004,

⁴ Federal regulations permit agencies to grant waivers from the background investigation requirements of Executive Order 10450 for a limited period of time, allowing new applicants to begin working while their investigations are still in progress. Agencies granting waivers must document which parts of the investigation have been initiated or completed before the individual begins work. See 5 C.F.R. § 732.202(a).

in response to an inquiry related to a prior OIG review, SEPS officials told us that SEPS had begun consolidating and updating the order. But, as of July 2005, the revision was not complete. Among the reasons for delays in completing the revision, SEPS told us that it was waiting for comments from OPM on the draft and for guidance from the Office of Management and Budget (OMB) on new personnel security requirements introduced by Homeland Security Presidential Directive 12 (HSPD-12), which was issued by the President in August 2004 and is scheduled to be initiated in stages starting in October 2005.

Also, SEPS has not effectively used available technology to make security policy and guidance widely and readily accessible. We examined the Personnel Security page of SEPS's intranet site and found that it contained only a list of SEPS's Personnel Security Group's functions. It did not contain any of the Department's personnel security policies – or even a complete list of the current policies. The Security Policies page did not include a personnel security section. It did contain the new Security Programs Operating Manual, but no other personnel security guidance was included.

SEPS's Oversight of Components With Delegated Authority. SEPS has not implemented an effective oversight program to ensure that components with delegated authority to adjudicate background investigations comply with regulations and policy. OPM has delegated to SEPS the responsibility for overseeing all Department background investigations, including any field investigations that are conducted by Department components rather than by OPM, and all adjudications. SEPS has retained direct responsibility for managing background investigations for all political appointees, Department attorneys, employees of the United States Attorneys' Offices (USAO); employees of the Department's Offices, Boards and Divisions; and certain other designated positions. To the FBI, SEPS has delegated authority to conduct the field investigations on all of the Department's political appointees and attorneys as well as on the FBI's own employees and contractors. To the ATF, SEPS has delegated authority to conduct field investigations on its employees who are not political appointees or attorneys and on its contractors. In addition, SEPS has delegated to personnel security staff in the components the authority to adjudicate background investigations and reinvestigations for their employees and contractors, and the authority to grant waivers so new employees can begin work. In total, 20 components have delegated adjudication authority – 7 have the authority for employees and contractors, and 13 have the authority only for contractors (see Appendix I).

The personnel security compliance reviews SEPS conducts of components to which it has delegated authority to manage background investigations are limited in number and scope. Additionally, limited enforcement authority and the lack of a centralized Department-wide database of background investigation files hinder SEPS's ability to ensure that components and personnel comply with policies and regulations related to personnel security.

SEPS's primary method for evaluating the components' personnel security operations is its on-site security compliance review.⁵ However, with only three Security Specialists and an annual travel budget of \$60,000, SEPS reviews about 1 percent of Department offices annually. From 2002 through 2004, SEPS reviewed an average of 39 offices per year. At that rate, it would take SEPS 75 to 90 years to inspect all of the Department's 3,000 to 3,500 offices.

Moreover, the scope of each compliance review includes only a small portion (about 4 hours of the review) dedicated to examining personnel security operations.⁶ The personnel security portion of the review primarily checks that required paperwork was present, that reinvestigations were initiated on time, and that mandatory annual security training was completed. The compliance reviews do not examine the quality of either the components' field investigations or the adjudications of employees' and contractors' clearances because such reviews would mean less time for higher priority physical and information technology security oversight.⁷

Even when compliance reviews identify security violations, SEPS has limited enforcement authority to ensure that components and

⁵ SEPS also receives an annual statistical report from OPM on the Department's performance in meeting the 90-day adjudication standard.

⁶ The on-site security reviews examine several security areas, such as building security and information security, in addition to personnel security.

⁷ SEPS can also ask OPM to conduct an in-depth review of a component's management of its background investigation operations. The last review SEPS requested was of the ATF when it transferred to the Department in 2003.

individuals comply with policies and regulations.⁸ As a consequence, compliance reviews continue to identify violations already reported to the component on past reviews. For example, one recent repeat violation has involved a component's granting security clearances for employees who do not require access to classified material.

Because the Department has no centralized personnel security database, SEPS has limited capability to centrally monitor the background investigation status of all Department employees. Instead, each component keeps its own database, and the systems are not interoperable. SEPS therefore cannot effectively monitor the components' compliance with pre-hiring and reinvestigation regulations, adherence to policy on national security clearances, or the completeness and timeliness of background investigation processing. For example, SEPS cannot effectively identify and track all the Department employees who are overdue for reinvestigation, nor can it perform effective oversight to ensure compliance with personnel security regulations.

SEPS's File Tracking System and Paper Files. SEPS uses an inventory management program called TRAQ to identify the location of each background investigation file. The version of TRAQ used by SEPS is outdated, at full capacity, and does not include needed capabilities. For example, TRAQ lacks quality control features to prevent the entry of erroneous information (such as nonsensical dates), cannot provide SEPS with management reports on the data in the system, and has no capability to maintain electronic copies of scanned security documents.

Because SEPS cannot maintain electronic copies, all SEPS background investigation files are maintained in paper form in one location. Likewise, files related to SCI clearances are also maintained in one location. This represents a significant vulnerability. The loss of the paper records would severely disrupt case processing and clearance verification.

⁸ SEPS has the option to withdraw a component's delegation of authority to adjudicate background investigations and grant security clearances if SEPS determines that the component is not in compliance with security regulations and policies. However, if that occurs, the responsibility for conducting the adjudications would fall to SEPS. Given SEPS's current resource limitations, assuming the additional workload if a delegation were withdrawn would be impractical. SEPS has never withdrawn a component's delegation of authority to adjudicate background investigations.

Changes Directed by the Intelligence Reform Act and HSPD-12

The Intelligence Reform Act imposes progressively tighter timeliness requirements for adjudications and field investigations that may overwhelm SEPS's current limited capabilities. The Intelligence Reform Act requires that, by December 2009, 90 percent of adjudications on background investigations and reinvestigations of individuals requiring national security clearances must be completed within 20 days. Further, 90 percent of the field investigations must be completed within 40 days.

To meet the new timeliness standards, SEPS will have to significantly expedite adjudications. For example, in FY 2004, SEPS adjudicated only 31 percent of employee reinvestigations and only 21 percent of contractor background investigations within 20 days. The Intelligence Reform Act also will require SEPS to ensure that the Department components with authority to conduct field investigations meet timeliness standards for those investigations. SEPS is not well positioned to meet these challenges.

HSPD-12, issued by the President in August 2004 and scheduled to be initiated in stages beginning October 27, 2005, expands SEPS's oversight responsibilities to include reviews of components' hiring practices for contractors who are investigated and hired directly by the field offices where they will be working. Currently, SEPS reviews only the investigations of contractors hired centrally through components' headquarters. The lack of a centralized database prevents SEPS from easily verifying whether each of these contractors received the proper background check or even whether they are still employed. HSPD-12 also requires the recertification of identification cards for all employees and contractors. With its current resources, processes, and authority, SEPS will have difficulty both in meeting the performance requirements of the Intelligence Reform Act and HSPD-12, and in providing oversight of the Department's compliance with those requirements.

RECOMMENDATIONS

In this report, we make six recommendations to help improve SEPS's performance of its personnel security responsibilities and better position the Department to meet the requirements of the Intelligence Reform Act and HSPD-12.

We recommend that the Department:

1. Develop a Department-wide plan for implementing the personnel security requirements of the Intelligence Reform Act and HSPD-12, and identify the resources that will be needed to enable the Department to meet the new requirements.
2. Develop a Department-wide database with imaging capability to enable uniform processing and tracking of employee and contractor personnel security actions, permit central oversight of personnel security operations, and reduce the vulnerability caused by reliance on paper records.

We recommend that SEPS:

3. Once OPM provides the necessary policy decisions, expeditiously issue an updated Department personnel security policy, DOJ Order 2610.2A.
4. Develop a plan for conducting routine oversight of components with delegated authority that provides reasonable coverage and ensures that the background investigations and adjudications meet established standards for quality and timeliness.
5. Institute an annual report to the Deputy Attorney General to describe the performance of the Department and each component in adjudicating background investigations and in complying with Department personnel security regulations and policies.
6. Establish procedures to identify the policies, documents, and other information necessary for personnel security operations, and in coordination with the Department's Office of the Chief Information Officer, make the documents available through the SEPS web site.

TABLE OF CONTENTS

BACKGROUND	1
General Requirements for Background Investigations	1
SEPS’s Organization.....	4
SEPS’s Direct Responsibilities Related to Background Investigations ..	6
SEPS’s Responsibilities for Policy Guidance.....	10
Authorities Delegated by SEPS to the Components	10
SEPS’s Oversight of Components With Delegated Authority	11
Recent Developments and Impending Changes in Background Investigations.....	14
PURPOSE, SCOPE, AND METHODOLOGY OF OIG REVIEW	17
Purpose of the OIG Review	17
Scope.....	17
Methodology.....	17
RESULTS OF THE REVIEW.....	20
Workload and Priorities	20
Adjudication Timeliness	22
Policy Guidance	26
SEPS’s Oversight of Components With Delegated Authority	29
The Department’s Resource Requests for SEPS	37
SEPS’s File Tracking System	37
No Centralized Background Investigation Database	40
Timeliness Requirements of the Intelligence Reform Act.....	43
Requirements of HSPD-12.....	47
CONCLUSIONS AND RECOMMENDATIONS	50
APPENDIX I: Components With Delegated Authority.....	54
APPENDIX II: SEPS’s Organization	56
APPENDIX III: The Justice Management Division’s Response.....	57
APPENDIX IV: The OIG’s Analysis Of JMD’s Response	60

BACKGROUND

The Office of the Inspector General (OIG) conducted this review to examine the Department of Justice's (Department) Security and Emergency Planning Staff's (SEPS) background investigation program. Specifically, we evaluated SEPS's management of four program areas: (1) managing background investigations of political appointees, attorneys, and other personnel whose investigations are not delegated to the components; (2) granting clearances for access to Sensitive Compartmented Information (SCI) materials for all Department employees; (3) providing policy guidance and training on background investigations; and (4) providing oversight of the components' background investigation programs.

General Requirements for Background Investigations

All federal agencies must ensure that only trustworthy individuals are hired to work in national security or public trust positions.⁹ The primary means for determining whether an individual is trustworthy is the background investigation, authorized by Executive Order 10450 and 5 C.F.R. Parts 731, 732, and 736. The background investigation is not an evaluation of the subject's character, but is instead a determination of the likelihood that a particular person will adhere to all Department security requirements in the future.

Each federal agency determines the required security level of each position according to the duties that the employee holding the position will fulfill. Once the security level of a position has been determined, an investigation appropriate to that level is supposed to be conducted. There are several types of background investigations, each varying in scope and complexity. All background investigations begin with a request to the employee to fill out a questionnaire targeted to the

⁹ National security positions either involve the protection of the United States from foreign aggression or espionage, or require regular access to classified material. See 5 C.F.R. § 732.102. Public trust positions involve policy making, major program responsibility, public safety and health, law enforcement duties, fiduciary responsibilities, or other duties demanding a significant degree of public trust, and positions involving access to or operation or control of financial records. See 5 C.F.R. § 731.106(b).

position's responsibilities.¹⁰ This is usually followed by an in-person interview with the applicant and, in most cases, a number of interviews with the applicant's colleagues and personal associates. Currently, there are no federal timeliness requirements for the field investigation portion of the background investigation process.¹¹

The Office of Personnel Management (OPM), through contracts with private companies, conducts the vast majority of field investigations of federal employees and contractors.¹² The Federal Bureau of Investigation (FBI) conducts the field investigations for all of the Department's political appointees and attorneys. SEPS is responsible for managing the background investigations of political appointees, attorneys, and personnel in the Offices, Boards and Divisions (see Appendix I.). Depending on the nature of the position to be filled, either OPM or the FBI conducts the field

OPM Faces Backlog of Field Investigations

There are currently no statutory timeliness requirements for the completion of the field investigation portion of the background investigation process. Instead, OPM sets internal deadlines of 120 days for the initial field investigations and 180 days for the completion of field reinvestigations. In February 2005, OPM reported to the Government Accountability Office that nearly 186,000 field investigations had exceeded these self-imposed timeframes. Furthermore, OPM estimated that approximately 8,000 full-time-equivalent investigators would be needed to clear this backlog and provide timely service for new requests. An OPM official testified at a June 2005 hearing of the Senate Homeland Security and Governmental Affairs Committee that with the hiring of new investigative contractors and the transfer of investigators from the Department of Defense to OPM, OPM now has 8,000 investigators available to work on this issue.

¹⁰ For instance, national security positions require completion of the SF-86 "Questionnaire for National Security Positions," and public trust positions require completing the SF-85P "Questionnaire for Public Trust Positions" or the SF-85 "Questionnaire for Non-Sensitive Positions." Some Department components use their own forms that incorporate required questions contained in the standard forms.

¹¹ The Intelligence Reform and Terrorism Prevention Act of 2004 enacted timeliness requirements for the field investigative portion of the process that must be met beginning in fiscal year (FY) 2007. These changes are discussed in greater detail below.

¹² Components with law enforcement personnel, such as the United States Marshals Service (USMS) and the Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF), may use their investigators to conduct investigations on some of their own contractors. In addition, some contractors' clearances may be transferred from other agencies.

investigations for SEPS. In FY 2004, SEPS submitted more than 3,133 requests to OPM for field investigations.¹³ These investigations ranged in cost from \$425 to \$3,300 each, depending on the type of investigation requested and whether an expedited processing premium was paid.

At one time, OPM estimated that its investigations took 35 days, 75 days, or 120 days, depending on the premium paid for expedited processing. However, OPM has not been able to meet those processing estimates since FY 2001 and, for FY 2004, changed its categories from completion estimates to “priority,” “accelerated,” and “standard,” with priority having the most expedited completion. In FY 2004, OPM’s priority (formerly categorized as 35-day) cases took an average of 100 days, accelerated (formerly 75-day) cases took an average of 227 days, and standard (formerly 120-day) cases took an average of 324 days.¹⁴

A SEPS adjudicator reviews the information collected during the OPM or FBI field investigation and makes the final determination on whether the applicant is suitable. Adjudicators rely on standards established by the Central Intelligence Agency, OPM, the Department, and the Department’s components to evaluate the information provided by the field investigation.¹⁵ These standards encourage adherence to a “whole person” approach to reviewing the issues presented by each individual case. Under that approach, when the investigation identifies derogatory information about the person, the adjudicator should consider factors such as the relevance of the information to position responsibilities, the circumstances surrounding the derogatory information, and the person’s candor in disclosing relevant information. Federal regulations require that the adjudication be completed and the results transmitted to OPM within 90 days after receipt of a completed investigative case file.¹⁶

¹³ In FY 2004, SEPS submitted 495 requests for field investigations to the FBI.

¹⁴ The FBI’s field investigations averaged 197 days in FY 2004.

¹⁵ These standards include Director of Central Intelligence Directive 6/4; the OPM *Suitability Processing Handbook*; Department guidance entitled, “Annex D: Adjudicative Guidelines for Determining Eligibility for Access to Classified Information”; and DOJ Order 2610.2A (August 21, 1990).

¹⁶ See 5 C.F.R. § 732.302(b).

Federal law further requires that employees and contractors holding a security clearance who have been employed in their jobs for certain periods of time be subject to a reinvestigation to verify that they are still suitable for their positions. Reinvestigation is required once every 5 years for individuals possessing a Top Secret clearance, once every 10 years for individuals possessing a Secret clearance, and once every 15 years for individuals possessing a Confidential clearance.¹⁷ Individual federal agencies may impose additional requirements to expand the number of individuals subject to reinvestigation or to require more frequent reinvestigations.

The Department requires all its employees to be reinvestigated once every 5 years.¹⁸ For contractors, the Department only requires reinvestigations for individuals holding national security positions; these reinvestigations are required on the same schedule as those of employees. The Department does not require that contractors in public trust positions be reinvestigated, but some components, including the ATF and USMS, require that these contractors be reinvestigated.

SEPS's Organization

SEPS is the primary office responsible for developing, implementing, and overseeing compliance with security policy throughout the Department.¹⁹ SEPS is a unit of the Justice Management Division (JMD), the administrative component of the Department. The director of SEPS, who is formally known as the Department Security Officer, reports to the Deputy Assistant Attorney General for Human Resources and Administration and to the Assistant Attorney General for Administration.

SEPS has direct adjudicative responsibility for background investigations on certain Department employees. In addition, SEPS has delegated adjudicative responsibility to some components for their employees, but it retains oversight responsibility over the delegated functions. Consequently, SEPS has four responsibilities related to

¹⁷ See 50 U.S.C. § 435b(a)(7).

¹⁸ See DOJ Order 2610.2A, ¶13 (August 21, 1990), and Department Security Officer memorandum FY 2001 Reinvestigation Program (January 16, 2001).

¹⁹ See DOJ Order 2600.2C (November 28, 2003).

background investigations in the Department: (1) managing background investigations for political appointees, attorneys, and other personnel not delegated to the components; (2) granting clearances for access to SCI materials for all Department employees; (3) providing policy guidance and training on background investigations; and (4) providing oversight of the components' background investigation programs.²⁰

SEPS staff is divided into 4 groups, which are further subdivided into 10 sections. (See Appendix II for a SEPS organizational chart.) In FY 2005, SEPS had 84 employees and 7 contractors, and a budget of \$10 million. SEPS's personnel security and compliance review functions are carried out by four sections in the Personnel Security Group (PERSG) and the Office of Information Safeguards and Security Oversight.

Within PERSG, the Operations Section is responsible for conducting adjudications of completed background investigations and maintaining investigation files on Department employees. The Policy, Training, and Oversight Section is responsible for drafting and distributing official Department policy on all background investigation and reinvestigation matters. In FY 2005, PERSG had 17 employees and 3 contractors.²¹ Five of the employees were adjudicators whose positions were funded by the components for whom they adjudicate reinvestigations.

Within the Office of Information Safeguards and Security Oversight, the Compliance Review Section (CRS) is responsible for conducting compliance reviews of all Department offices to determine their adherence to Department security policy. In FY 2005, CRS had three employees, including the chief. The Technical Security Section is responsible for the security of technology used to store and transmit classified information. Personnel in the Technical Security Section also manage SEPS's background investigation inventory software.

Prior External Reviews Involving SEPS Staffing and Structure. Two external reviews since FY 2001 relating to SEPS's responsibilities have

²⁰ SCI is a classification that is more restrictive than Top Secret, often covering information that deals with intelligence sources, methods, or activities.

²¹ PERSG has lost several staffers through attrition in recent years. While it has been given authorization to fill some of the vacancies, it did not receive any accompanying funding, so overall staffing levels have decreased.

reported that SEPS has inadequate resources and have made recommendations for improving the processing of background investigations. However, we found that these recommendations had not been implemented. First, in March 2002, the Webster Commission report raised concerns about SEPS's inadequate resources and lack of standing within the Department hierarchy.²² In a footnote to the discussion of its recommendation to create an Office of Security within the FBI that reports to the Director, the Webster Commission stated:

[SEPS] is responsible for developing security policy and overseeing its implementation in Department components, such as the FBI. Although we have not examined SEPS in detail, the program seems to suffer from many of the structural weaknesses that led us to recommend creation of an Office of Security in the [FBI], weaknesses such as inadequate resources and insufficient stature within the Department's structure. We recommend that the Department address this issue.²³

On July 15, 2004, a report issued by the National Archives and Records Administration's Information Security Oversight Office expressed concern that the Department had neglected to address the Webster Commission's recommendation. The new report recommended that the Department move SEPS out of JMD and commit sufficient resources to its security programs. In his October 13, 2004, response to the National Archives and Records Administration report, the Assistant Attorney General for Administration agreed on the need for additional resources but declined to move SEPS out of JMD, stating that being a part of JMD did not hinder SEPS from fulfilling its responsibilities.²⁴

SEPS's Direct Responsibilities Related to Background Investigations

SEPS retains direct responsibility for background investigations for all employees of the Department's Offices, Boards and Divisions, all employees of the United States Attorneys' Offices (USAO), all political

²² The Webster Commission was convened to examine the FBI's security programs following the detection of espionage by FBI agent Robert Hanssen.

²³ See *Commission for Review of FBI Security Programs, A Review of FBI Security Programs*, March 31, 2002, p. 93, n. 34.

²⁴ Since this response, however, SEPS has not received additional resources.

appointees, all attorneys, and certain other designated positions.²⁵ SEPS is also responsible for the background investigations of some contractors. At present, therefore, SEPS is responsible for the background investigations of approximately 27,000 of the Department's 103,000 employees, as well as for 7,000 contractors.

As part of its responsibilities, PERSG obtains the required paperwork from political appointees who do not require Senate confirmation and certain other employees and contractors, schedules background investigations with OPM or the FBI, submits requests for FBI name checks, adjudicates the completed files, and processes waivers.^{26, 27} As Figure 1 shows, for certain categories of cases one of the Department's components initiates, receives, and evaluates the field investigation before the personnel file is sent to SEPS for adjudication. For political appointees requiring Senate confirmation, the Office of Legal Policy (OLP) provides SEPS the background investigation file after Senate review. For attorneys, the Office of Attorney Recruitment and Management (OARM) initiates and reviews the FBI field investigation. For its employees who are not attorneys or political appointees, the Executive Office of the United States Attorneys (EOUSA) conducts an internal review of the OPM investigation before forwarding the file to

²⁵ For example, SEPS manages the background investigations of the officials responsible for overseeing personnel background investigations at components.

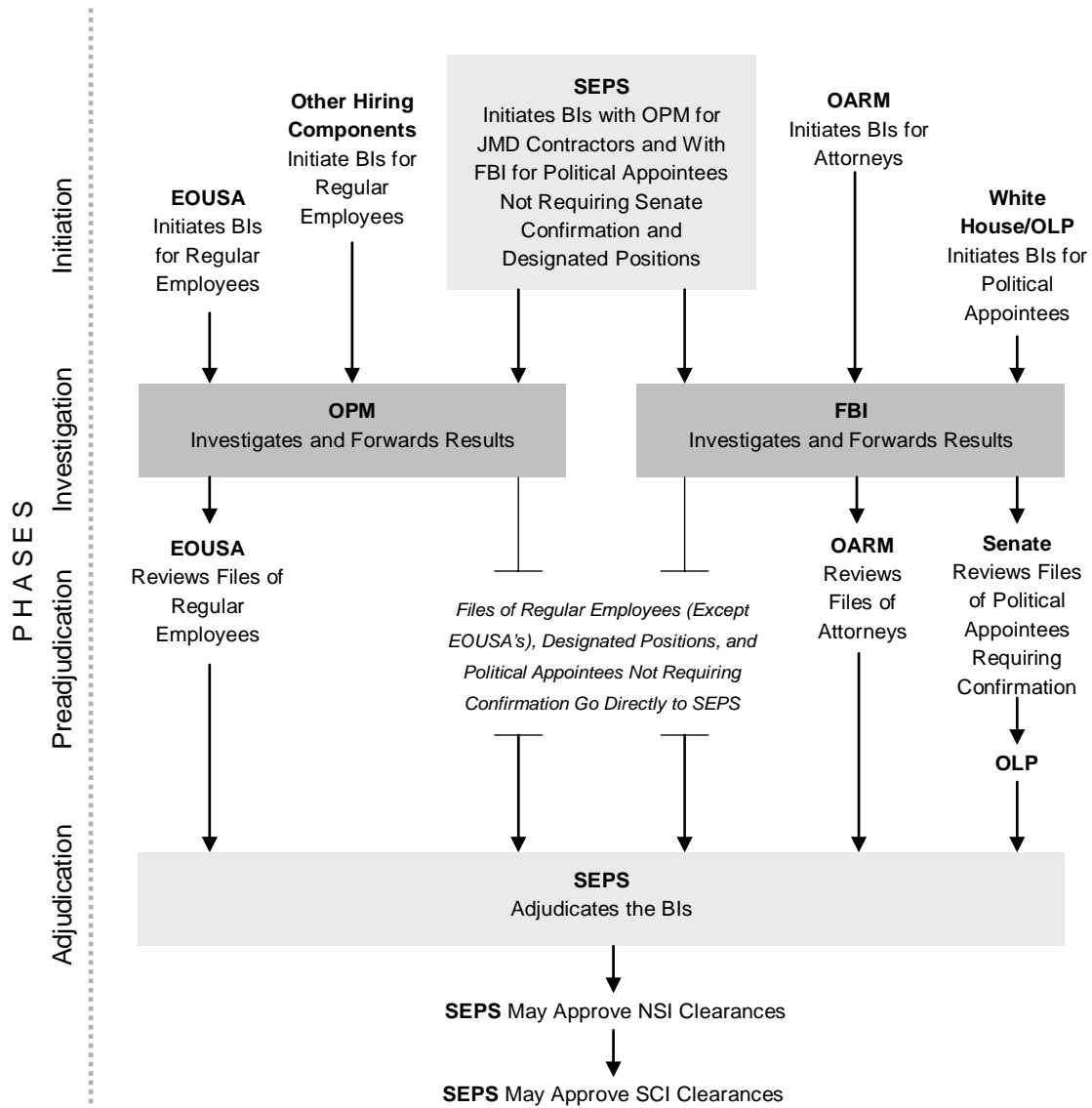
²⁶ The FBI's National Name Check Program (NNCP) disseminates "information from the FBI's Central Records System (CRS) in response to requests by federal agencies, congressional committees, the federal judiciary, friendly foreign police and intelligence agencies, and state and local criminal justice agencies." [Testimony of Robert J. Garrity, Jr., Acting Assistant Director, Record Management Division, FBI, July 10, 2003.] The FBI records maintained in the CRS consist of administrative, applicant, criminal, personnel, and other files compiled for law enforcement purposes. The NNCP electronically searches the requested name checks through the Universal Index (UNI) located within the CRS, where individual names have been indexed to all investigative and administrative cases. The names, including spelling variations, are searched phonetically against the UNI records and matches are retrieved. The primary difference between the National Crime Information Center, which search for state and local arrest information and dispositions, and the NNCP is that the NNCP identifies subjects of any ongoing federal investigations and searches all FBI records and classifications for references to individuals.

²⁷ Federal regulations permit agencies to grant waivers from the background investigation requirements of Executive Order 10450 for a limited period of time, allowing new employees to begin working while their investigations are still in progress. Agencies granting waivers must document which parts of the investigation have been initiated or completed before the individual begins work. See 5 C.F.R. § 732.202(a).

SEPS. Figure 1 shows the typical work flow for these responsibilities. PERSG is responsible for initiating reinvestigations from this caseload of 27,000 employees and 7,000 contractors. Currently, all stages of the background investigation are paper-based and manual, no imaging functions are available to convert paper documents to digital files, and none of the stages for managing background investigations or reinvestigations are automated. PERSG tracks the physical location of its files using an inventory management software application called TRAQ.²⁸ Only SEPS uses the software; none of the components has access to TRAQ.

²⁸ TRAQ is not an acronym; it is the full name of the software application.

Figure 1: Background Investigation (BI) Process



Notes

“Regular Employees” refers to personnel who are not attorneys or political appointees.

“Designated Positions” refers primarily to high-level officials and officials responsible for overseeing personnel background investigations at components.

OARM is the Office of Attorney Recruitment and Management.

OLP is the Office of Legal Policy, which serves as the liaison to the White House on political appointments.

Source: OIG

SEPS's Responsibilities for Policy Guidance

PERSG is responsible for interpreting federal policies and guidance on all issues related to background investigations and reinvestigations. PERSG is also responsible for issuing Department policies for all Department components to follow. DOJ Order 2610.2A, dated August 21, 1990, is currently the official Department policy on background investigation and reinvestigation procedures.²⁹ However, from 1990 through 2005, SEPS has issued over 40 separate update memorandums to supplement or amend the order. PERSG also provides formal training on the guidance and adjudicative standards for background investigations and reinvestigations, and provides informal guidance, primarily over the phone or via e-mail, to component staff.

Authorities Delegated by SEPS to the Components

SEPS has delegated to components' personnel security staff the authority to adjudicate background investigations and reinvestigations for their employees and contractors, and the authority to grant waivers so new employees can begin work before their investigations are complete. In total, 20 components have delegated adjudication authority – 7 have the authority for employees and contractors, and 13 have the authority only for contractors (see Appendix I).

Approximately 76,000 employees, as well as a large number of contractors, work in the components with delegated authority.³⁰ SEPS also has delegated to some components the authority to grant security clearances up to and including the level of Top Secret, upon an individual's successful completion of an investigation. When delegating authority to a component, SEPS issues a memorandum that specifies the authorities being delegated as well as any restrictions imposed. The memorandum specifies that SEPS retains oversight of the delegated areas.

²⁹ On September 15, 1994, the 1990 DOJ Order was amended to change two sections, but the original order was not reissued.

³⁰ SEPS is able to verify the number of Department employees because all employees are paid through the National Finance Center payroll system and are tracked through headquarters personnel and security offices. However, SEPS cannot determine the number of Department contractors because contractors are not tracked centrally through either personnel or security offices.

SEPS's Oversight of Components With Delegated Authority

Although SEPS delegates to components the authority for background investigations, it remains responsible for overseeing the function. As described below, the various elements of SEPS's oversight of the components with delegated authority are carried out by CRS and PERSG.

CRS Oversight Functions. SEPS's primary oversight mechanism is the security compliance review conducted by its Compliance Review Section (CRS). CRS's three Security Specialists are responsible for conducting security compliance reviews of the Department's 3,000 to 3,500 offices and sub-offices worldwide. They travel to components' locations, conduct the security compliance reviews, write reports describing the results of the review, and follow up with components that require corrective action. In selecting offices to review, CRS considers: (1) whether the office handles classified information; (2) whether SEPS has ever reviewed the office or when it last reviewed; (3) whether the office recently moved into a new building; and (4) the size of the office (larger offices are typically reviewed more often). CRS also considers input it receives from Security Programs Managers on potential security risks or problems at offices in their components. CRS issues a list of the offices it plans to review to the components' Security Programs Managers at the beginning of each fiscal year.

Each review typically lasts 2 to 3 days and covers physical, personnel, contractor, information, computer, and communications security as well as safety and health and continuity of operations and occupant emergency plans. The highest priority of the review is ensuring that the physical security of Department offices is adequate and in compliance with applicable regulations.³¹ Only a small portion of most

³¹ SEPS defines physical security as "the application of physical barriers and control procedures as preventive measures or countermeasures against threats to resources and information." *SEPS Security Program Operating Manual*, revised May 2005, p. 89.

compliance reviews (3 to 4 hours) is dedicated to reviewing personnel security issues.³²

Before visiting a site, the CRS staff reviews a sample of background investigation files maintained by the component's headquarters office. The CRS staff estimated that, for large offices, it requests up to one third of the employee files for review and a higher percentage for smaller offices. While on site, Security Specialists use checklists for each of the security disciplines to guide them in conducting interviews with relevant security officials and recording findings and observations. The Personnel Security Checklist covers the following areas: (1) the minimum requirements of a waiver; (2) the background investigation requirements for temporary appointments; (3) the number of national security and public trust positions; (4) resignation and reinstatement procedures; (5) reinvestigation processes; (6) national security information access, training, and security clearances; and (7) SCI access procedures. The CRS staff asks for a roster of locally hired contractors, and checks the files kept on site. CRS will also talk to the General Services Administration about shared contract staff, such as janitors. Security Specialists interview the individual responsible for conducting security clearance briefings, and may also interview one or more employees with security clearances, to ensure that employees who access classified materials have received required training and signed required disclosure forms.

The CRS staff compiles its findings, observations, and recommendations into written reports and sends them to the component's Security Programs Manager for corrective action.³³ CRS has no requirement to issue reports within a particular time frame, but CRS has established an internal goal of issuing its reports approximately 4 to 6 weeks after the completion of the site visit.

³² The physical security portion of the review typically lasts the longest and requires walking around the perimeter of the building and examining exterior and interior doors, windows, locks, alarms, security cameras, guard services, magnetometers, X-ray equipment, and air intake valves; documenting security weaknesses with a digital camera; and often meeting with the building manager to discuss building and office access control procedures.

³³ Findings are direct violations of federal regulations, public laws, or Department security policy that require corrective action, while observations are the CRS staff's suggestions on improving security.

There are no Department regulations or orders that establish requirements for the security compliance reviews or CRS's authority for enforcing its security findings.³⁴ SEPS has not established a formal performance measure for the number of security reviews it conducts each year, but has an informal internal goal of 60 reviews a year. SEPS also established an internal requirement for Security Programs Managers to respond in writing to CRS's findings within 60 days of the report publication date. CRS staff may conduct a follow-up review after components respond to ensure that recommendations were addressed.³⁵

PERSG Oversight Functions. In addition to the CRS compliance reviews, PERSG also conducts some oversight of the components with delegated authority. PERSG receives yearly reports from OPM on the percentage of adjudications each component is completing within 90 days, as regulations require. PERSG can also request that OPM perform an appraisal, or substantive audit, of a component's ability to perform suitability adjudications. For example, PERSG requested an appraisal of the ATF's performance following its transfer to the Department. OPM certified that the ATF was performing these duties well. The results of this appraisal led to PERSG's decision to delegate to the ATF the authority to perform investigations and adjudications, and to grant security clearances up to and including the level of Top Secret.

Oversight Enforcement Mechanisms. If any of the oversight mechanisms described above indicates that a component is not adhering to Department security policy, SEPS may recommend that the Department Security Officer modify or revoke the component's delegation of authority. The revocation option, used rarely, is the only sanction available to SEPS to ensure that components with delegated authority follow policy. It was last used in 2000 to transfer the responsibility for conducting field investigations from the Drug Enforcement Administration (DEA) to OPM. This decision was made after an OPM review of the DEA's program revealed that many of the investigations the

³⁴ DOJ Order 2600.2C, issued November 28, 2003, establishes the Department's security programs and the associated responsibilities. However, the Order does not mention CRS.

³⁵ CRS officials told us that they try to schedule follow-up reviews concurrently with regular security compliance reviews. During follow-up reviews, CRS focuses on the areas that it previously found deficient, as well as any new issues or security vulnerabilities that have surfaced since the original review.

DEA conducted did not meet government standards for sufficiency or due process.

Recent Developments and Impending Changes in Background Investigations

Three recent developments have the potential to significantly affect background investigations and clearances. These developments are the passage of the Intelligence Reform and Terrorism Prevention Act of 2004 (the Intelligence Reform Act, Pub. L. 108-458), the issuance of Homeland Security Presidential Directive 12 (HSPD-12), and OPM's e-Clearance initiative.

The Intelligence Reform Act. On July 22, 2004, the National Commission on Terrorist Attacks Upon the United States (the 9/11 Commission) released a report documenting numerous intelligence and security failures throughout the federal government and made over 40 recommendations for reforming the intelligence community and the intelligence-related activities of the United States government. Included among them was a recommendation that “[a] single federal agency should be responsible for providing and maintaining security clearances, ensuring uniform standards – including uniform security questionnaires and financial report requirements, and maintaining a single database.”³⁶

Several of the 9/11 Commission's recommendations were incorporated into the Intelligence Reform Act. These provisions have two major goals – to consolidate background investigations and the issuance of security clearances under a single government agency and to significantly reduce the time it takes to complete investigations. The Act first requires the President to name a single agency to be responsible for government-wide oversight of the security clearance process. This agency will also be responsible for standardizing and streamlining the process across agencies and ensuring reciprocal recognition of security clearances across agencies. In June 2005, the President assigned this role to the Office of Management and Budget (OMB). The Act also prohibits individual agencies from imposing any investigative or adjudicative requirements beyond those outlined in any Executive Orders establishing security requirements for access to classified information.

³⁶ National Commission on Terrorist Attacks Upon the United States, *The 9/11 Commission Report*, W.W. Norton & Co., 2004, p. 422.

In addition to designating an oversight agency, the Act requires the President to designate a single federal agency to be responsible for conducting background investigations on all federal employees and issuing all security clearances.³⁷ These investigations are to be conducted in accordance with the standards to be developed by OMB. The investigating agency is also expected to create a single, government-wide database to store information on the background investigations and clearance status of all federal employees.

In addition, the Act sets strict deadlines for the completion of various phases of the investigation. The Act mandates that, by the end of 2006, 80 percent of investigations must be completed within an average of 90 days and adjudications within an average of 30 days, for an overall average of 120 days for a case to be completed. By the end of 2009, 90 percent of investigations must be completed in an average of 40 days and adjudications in an average of 20 days, for an overall average of 60 days for a case to be completed.

HSPD-12. On August 27, 2004, President Bush signed HSPD-12, which requires a standardized form of official identification for both government employees and contractors. Implementation, in stages, will begin on October 27, 2005. The Office of the Chief Information Officer was designated to coordinate implementation for the Department, with SEPS providing input on personnel security issues. The directive states that official identification cards necessary to access government offices should be issued only to those employees with certain pre-employment background checks completed and that the validity of these checks must be updated or verified every 5 years. OMB is responsible for issuing government-wide implementation guidance on the directive.

Originally, the minimum requirement for issuing an identification card was that all National Agency Checks be completed, with additional paper inquiries completed after employment.³⁸ This type of background investigation is called the NACI (National Agency Checks with Inquiries).

³⁷ As of the date of publication, the President had not designated an agency to fill this role.

³⁸ The minimum National Agency Checks required are the Security/Suitability Investigations Index, Defense Clearance Investigation Index, FBI Name Check, and the FBI National Criminal History Fingerprint check. The minimum Inquiries required are of employment, education, residence, references, and checks of law enforcement databases where the applicant has lived.

As of FY 2004, OPM reported that the NACI process was taking an average of 89 days to complete. In August 2005, OMB reduced the pre-employment requirement. Currently, although the NACI must be initiated before a new employee enters on duty and the fingerprint check completed, an agency can issue an identification card if it has not received the remaining elements of the NACI within 5 days.

e-Clearance Initiative. OPM has proposed a transition to electronic recordkeeping to minimize the burden of background investigations. It is focusing on three specific improvements to the paper-based recordkeeping process. The first element of this program, called e-QIP, would provide automated online versions of the different background investigation questionnaires. Under OPM's current system, an individual must fill out the security questionnaire from scratch each time an investigation is required, and OPM must manually enter the data into its system. Once fully implemented, e-QIP would allow for electronic transmission of the forms to appropriate agencies and for maintenance of historical data. OPM has further proposed the creation of an electronic version of the form used to update the original application, a change that it envisions would save both time and money when reinvestigations are required.

The second element calls for a government-wide database that would allow personnel security staff to verify the clearances of individuals in most government agencies.³⁹ The ultimate goal is for the system to display clearance information in real time. The third element of the initiative calls for the imaging of all documentation related to background investigations. Imaging would allow for electronic transmittal of records to the appropriate offices, eliminating mailing delays. It would also allow OPM to maintain historical information. Providing quick access to previous investigations would minimize requests for duplicate investigations, thereby saving time and money. OPM has asked all government agencies that conduct background investigations to image the files of completed background investigations.

³⁹ OPM currently uses a program called the Clearance Verification System. As described by SEPS, agencies provide updated information to OPM on their employees' clearance levels approximately once every 6 months.

PURPOSE, SCOPE, AND METHODOLOGY OF OIG REVIEW

Purpose of the OIG Review

The OIG conducted this review to examine SEPS's background investigation program. Specifically, we evaluated SEPS's management of four program areas: (1) managing background investigations of political appointees, attorneys, and other personnel whose investigations are not delegated to the components; (2) granting clearances for access to SCI materials for all Department employees; (3) providing policy guidance and training on background investigations; and (4) providing oversight of the components' background investigation programs.

Scope

This review focused on the operations of SEPS's Personnel Security Group and the Compliance Review Section. We examined functions that are currently SEPS's responsibility and also analyzed several areas that will become SEPS's responsibility once enacted legislation takes effect. Our scope did not include reviewing individual files to evaluate the quality of the field investigations and adjudications, nor did we evaluate SEPS's performance in its other areas of responsibility, such as physical security, communications security, and technical security.

Methodology

Interviews. We interviewed Security Programs Managers from 12 components, as well as staff from SEPS, the FBI, the ATF, the OIG, JMD, and the Office of the Deputy Attorney General.

Interviews With Security Programs Managers. We conducted telephone interviews with Security Programs Managers from the following components: the FBI, ATF, BOP, USMS, DEA, EOUSA, Executive Office of the United States Trustees (EOUST), Executive Office for Immigration Review (EOIR), OIG, Criminal Division, and Civil Division.

Interviews With SEPS staff. We interviewed the Director and Executive Officer of SEPS. From the Personnel Security Group, we interviewed the Assistant Director. We also interviewed the Chiefs of the Operations and the Policy, Training, and Oversight sections. From the

Office of Information Safeguards and Security Oversight, we interviewed the Assistant Director. From the Compliance Review Section, we interviewed all three Security Specialists, including the CRS Chief. We also spoke with two former Security Specialists. From the Technical Security Section, we interviewed the managers of the software application used to track background investigations.

Interviews With FBI staff. We interviewed the Unit Chief and staff from the National Name Check Section of the Records Management Division at FBI Headquarters.

Interviews With ATF staff. We interviewed the Chief of the ATF's Personnel Security Branch and two individuals from the Software Management Branch, Information Services Division.

Interviews With OIG staff. We interviewed the OIG's Personnel Security Specialist and Security Programs Manager, who is one of the former Compliance Review Section staff members.

Interviews With JMD staff. We interviewed the Chief Information Officer, the Deputy Chief Information Officer, a contractor working in conjunction with the Office of the Chief Information Officer, and an employee from JMD's Management and Planning Staff.

Interview With the Office of the Deputy Attorney General staff. We interviewed an Associate Deputy Attorney General.

Site visits. In early March 2005, the OIG review team accompanied the CRS Chief on a security compliance review of the ATF and USMS in Louisville, Kentucky. The compliance review included two ATF offices – the Louisville field division and a sub-office located in Lexington, Kentucky – and the USMS's office in the federal courthouse in Louisville. We also attended a May 2005 Security Programs Managers training conference.

Documentation review. We reviewed numerous documents, including internal SEPS documents, Department security policies, security updates and notices to Security Programs Managers from SEPS, budget requests, customer satisfaction surveys, position descriptions, external reports on security and SEPS, congressional testimony, pending legislative changes to personnel security, OPM's timeliness and workload

requirements for the Department, and online information regarding SEPS.

Data analysis. After requesting data from SEPS's background investigation inventory software, we analyzed the data using SPSS software and Microsoft Excel and Access. Our data analysis included timeliness, background investigation processing, reinvestigation compliance, and projections for current and anticipated SEPS workload. We provided the analyzed data and our interpretation to SEPS for concurrence prior to issuance of the draft report.

RESULTS OF THE REVIEW

In FY 2004, SEPS met federal regulatory requirements for adjudicating background investigations within 90 days in 99 percent of its highest priority cases (political appointees and attorneys) and in 85 percent of cases overall. SEPS also generally met Department needs for processing SCI clearances and providing clearance verifications. However, SEPS did not fully meet other important responsibilities related to policy and oversight. The Department's personnel security policy, amended by more than 40 memorandums issued over the past 15 years, is inconsistent, outdated, and not widely and readily accessible. In addition, SEPS's program of security compliance reviews and its enforcement authority are too limited to ensure that components with delegated authority comply with regulations and policy. Also, because SEPS relies on outdated technology to manage its own files and there is no Department-wide database of background investigation information, SEPS has limited ability to manage and oversee the background investigation process across the Department.

Workload and Priorities

From FY 2000 to FY 2004, portions of SEPS's background investigation workload more than doubled, particularly in the areas of granting clearances and the initiation and adjudication of contractor background investigations (see Table 1). In response to the increasing background investigation caseload, PERSG designated four of its responsibilities as being its highest priorities: (1) adjudication of the background investigations and reinvestigations of political appointees and attorneys; (2) adjudication of requests for access to SCI material; (3) certification of clearances to other agencies; and (4) processing requests for waivers. As lesser priorities, SEPS adjudicates background investigations for other new employees, adjudicates reinvestigations for

employees, adjudicates all contractor cases, and develops policy guidance.⁴⁰

Table 1: SEPS's Background Investigation (BI) and Reinvestigation (RI) Workload FY 2000-2004						
	FY 2000	FY 2001	FY 2002	FY 2003	FY 2004	Percentage Change 2000-2004
Employees						
BI Initiations	1,286	1,675	2,382	2,004	1,784	38.7
Waivers	558	876	1,081	1,224	1,142	104.7
BI Adjudications	1,188	1,795	1,407	1,698	2,237	88.3
Clearance Actions Taken	382	536	892	1,140	1,609	321.2
RI Initiations	1,321	3,000	2,454	3,051	2,422	83.4
RI Adjudications	1,508	1,421	1,743	2,266	1,983	31.5
Contractors						
BI Initiations	291	326	821	984	1,263	334.0
BI Adjudications	446	421	579	784	1,033	131.6
RI Initiations	21	8	25	24	12	-42.9
RI Adjudications	17	14	14	25	24	41.2
TOTAL ACTIONS	7,018	10,072	11,398	13,200	13,509	92.5

Source: PERSG TRAQ

SEPS's SCI clearance workload also increased dramatically from 2000 to 2004. PERSG retains the sole authority within the Department to grant SCI clearances and to confirm these clearances for personnel who require SCI access to other components or other federal agencies. Table 2 shows SEPS's SCI clearance workload from calendar years 2000 through 2004.

Table 2: SEPS's SCI Clearance Workload for Calendar Years (CY) 2000-2004						
	CY 2000	CY 2001	CY 2002	CY 2003	CY 2004	Percentage Change 2000-2004
SCI Clearances Processed	1,251	2,196	2,457	3,129	3,113	148.8
SCI Clearances Verified	810	1,261	1,667	2,005	2,053	153.5
TOTAL ACTIONS	2,061	3,457	4,124	5,134	5,166	150.7

Source: SEPS CRS

⁴⁰ PERSG places less emphasis on the adjudication of these routine investigations because waivers are granted for more than half of the new employees the Department hires to fill positions other than law enforcement officer positions. The waivers allow the employees to begin work before their background investigations are complete.

Adjudication Timeliness

We found that SEPS's adjudication of background investigations was generally timely. We examined SEPS's processing of 55,197 actions on background investigations for which it retained authority during the 5 fiscal years from FY 2000 through FY 2004 (see Table 1). The percentage of adjudications of initial background investigations for employees and contractors processed by SEPS within 90 days for each of the fiscal years is shown in Table 3. In FY 2004, SEPS adjudicated 85 percent of all employee background investigations within 90 days.

Table 3: SEPS Background Investigation Adjudications Completed Within 90 Days FY 2000-2004					
Percentage completed in 90 days					
	FY 2000	FY 2001	FY 2002	FY 2003	FY 2004
Employees	94	90	73	75	85
Contractors	83	81	60	73	96

Source: PERSG TRAQ

In discussions with SEPS staff responsible for adjudications, we asked why some cases were not processed within 90 days. SEPS staff explained that some cases were delayed because SEPS lacked the staffing needed to perform all adjudications within the required time and that, in other cases, decisions were delayed pending the receipt of documentation or until issues related to the applicant's suitability were resolved. For example, when a background investigation identified credit issues, a final decision on the adjudication might be delayed until the employee documented 3 months of on-time payments.

Staffing and Resources Not Increased Commensurate With Workload. As described in the background section, two previous external reports from the Webster Commission and the National Archives and Records Administration found significant shortfalls in SEPS staffing. SEPS requested additional staffing both before and after those reviews. Between FY 2000 and FY 2005, SEPS's annual budget requests included additional staff and provided extensive performance and workload measures to justify the requests. For example, SEPS provided studies comparing its staffing levels to those of three other Department

components with comparable adjudications responsibilities and to other components or agencies with comparable security responsibilities. As Table 4 shows, in 2001 SEPS had the smallest ratio of adjudications staff to background investigation caseload.⁴¹ Despite the recommendations from these reports, SEPS did not receive the requested additional resources, except for one additional position in the CRS.

Table 4: PERSG's 2001 Comparison of Its Staffing Levels to Three Department Components			
	Caseload (Employees and Contractors)	Adjudicators	Average Cases Per Adjudicator
SEPS	33,000	9	3,667
BOP	51,143	17	3,008
DEA	22,700	26	873
INS*	41,000	47	872

Source: PERSG

* On March 1, 2003, the Immigration and Naturalization Service (INS) was transferred to the Department of Homeland Security.

SEPS's Workload Management. Despite its low staffing levels, SEPS has taken several steps to manage its increasing case workload more effectively. These steps include redirecting personnel assigned to other duties to adjudications, and identifying and focusing its available resources on its highest priority cases. Specifically, PERSG staff stated that they relied on a combination of staff redirected from other duties, overtime from adjudicators, and assistance from employees in other sections of SEPS with prior adjudicative experience. For example, because they had experience as adjudicators, the PERSG Chief for Policy, Training, and Oversight and a Security Specialist from this section were assigned, as needed, to process requests for SCI clearances and other adjudication cases. Also, the Operations Section scheduled one day a week when all PERSG staff devoted the entire day to adjudicating backlogged cases. The size of the adjudications backlog has diminished since October 2003 (see Table 5).

⁴¹ SEPS must also process the SCI clearances of all Department components. In CY 2004, there were 5,166 cases, as shown in Table 2.

Table 5: PERSG FY 2004 Adjudication Pending Caseload

Months	Employee Cases		Contractor Cases		Total
	Not Yet Screened by SEPS*	Pending Adjudication	Not Yet Screened by SEPS*	Pending Adjudication	
Oct. 2003	1,072	698	98	286	2,440
Nov. 2003	1,039	682	72	287	2,367
Dec. 2003	1,143	677	35	272	2,399
Jan. 2004	970	679	63	200	2,112
Feb. 2004	1,073	675	-	-	1,748
Mar. 2004	846	694	50	76	1,742
Apr. 2004	853	683	-	-	1,536
May 2004	933	703	58	169	2,032
June 2004	1,059	562	101	165	2,052
July 2004	1,112	570	95	98	1,973
Aug. 2004	968	547	89	91	1,786
Sept. 2004	1,005	545	98	98	1,881
PERCENTAGE CHANGE	-6.3	-21.9	0.0	-65.7	-22.9

Source: SEPS

*These cases refer to those that PERSG had not yet reviewed.

SEPS does not operate on a fee-for-service basis (i.e., the components do not directly reimburse SEPS for the cost of the services it provides). However, since 1992, Department components have contributed funding to enable SEPS to hire staff dedicated to managing reinvestigations. Of the nine adjudicator positions, five are assigned to reinvestigations and are paid for proportionally by the components. The components also contribute to a fund from which SEPS pays staff overtime for conducting adjudications. In FY 2004, the components agreed to contribute \$22,000 to the overtime fund.⁴²

Also, as described previously on pages 20 and 21, SEPS established priorities for the processing of cases. The priorities were (in order) political appointees, attorneys, other FBI investigations (i.e., not political or attorney positions), OPM national security information (NSI)

⁴² SEPS is compensated directly only for its costs incurred; money that is not used is returned to the components. Actual costs were not available for FY 2004. Total overtime costs have never exceeded the initial overtime fund contributions. SEPS does not track adjudication overtime separately from other overtime.

investigations, other OPM investigations, employee reinvestigations, and contractors. Our review of the processing times for cases involving these categories of employees found that SEPS is processing the highest priority cases first (see Table 6).⁴³ For example, based on records contained in TRAQ, we determined that SEPS processed over 99 percent of its highest priority cases (political appointees and attorneys) within 90 days.

Table 6: SEPS Adjudication Processing by Priority Level					
Adjudication Priorities (Highest to Lowest)	Percentage Completed in 90 days				
	FY 2000	FY 2001	FY 2002	FY 2003	FY 2004
Political appointees	100	100	100	100	—
Attorneys	99	99	99	99	100
FBI NSI investigations	100	88	94	92	96
OPM NSI investigations	92	91	85	74	79
Other OPM investigations	91	85	48	62	81
Employee reinvestigations	84	83	59	48	54
Contractors	83	81	60	73	96

Source: PERSG TRAQ

To determine whether SEPS met OPM timeliness expectations, we reviewed FY 2004 correspondence between PERSG and the OPM Investigations Program Specialist assigned to the Department’s oversight. The OPM Specialist noted that SEPS’s performance (85 percent of adjudications completed in less than 90 days) and that of the Department as a whole (87 percent completed in less than 90 days) “exceed[ed] compliance expectations” and was “meeting” an “important goal.” We also reviewed a recent PERSG customer service survey and conducted an additional survey of 12 Security Programs Managers. All 12 indicated that they were generally satisfied with the service SEPS provided in processing background investigations and security clearances. Separately, in SEPS’s own customer service survey of

⁴³ Contractor cases were sometimes processed faster than other higher priority cases because, although cases are generally processed according to priority, SEPS also reviews field investigations as they are received to identify cases for which there are no potentially derogatory issues and adjudicates those cases as quickly as possible. Because over 90 percent of contractors are hired for lower risk positions with limited background checks that result in no derogatory information, those cases can be quickly adjudicated.

Security Programs Managers, PERSG's responsiveness in obtaining SCI access and certifying national security clearances to other components and agencies were the two highest rated elements.⁴⁴

Overall, we believe that SEPS has taken reasonable steps to use the resources available to manage its case processing workload, and OPM and the components have been generally satisfied with SEPS's performance. SEPS met regulatory timeliness requirements 85 percent of the time in FY 2004 for the background investigations for which it is directly responsible and is meeting Department needs by processing SCI clearances and clearance verifications as quickly as possible. In only 15 percent of the employee cases and 4 percent of the contractor cases did SEPS not meet OPM's timeliness requirements. However, as we discuss in greater detail below, the Intelligence Reform Act and HSPD-12 directed changes that will, when implemented, require faster processing times and increase the number of case processing stages that SEPS must accomplish to complete background investigations.

Policy Guidance

The Department's personnel security policy, amended by more than 40 memorandums issued over the past 15 years, is inconsistent, outdated, and not widely and readily accessible. SEPS, which is responsible for issuing policy and providing guidance for the Department, issued the last complete revision of the Department's security policy, known as DOJ Order 2610.2A, in 1990. Although the basic order has not been updated, from 1990 through 2005 SEPS issued more than 40 memorandums that revised or supplemented the order. Because the changes have been issued in a piecemeal fashion, there is no single, consolidated document that contains all current guidance for component security officials and other Department employees to consult.

Despite the many revisions and supplements, the guidance has not been updated to reflect recent changes in the security environment, according to PERSG staff. For example, the guidance does not require the reinvestigation of all contractors, which SEPS has long considered

⁴⁴ There are no regulatory timeliness requirements for these processes, but they are often time-sensitive. SEPS reported that it currently has two employees who manage clearance certifications as a collateral duty, one for 65 percent of duties, and one for 25 percent.

necessary to ensure the Department's security.⁴⁵ In customer service surveys conducted by the OIG and SEPS, Security Programs Managers and adjudicators expressed frustration with having to work with outdated and confusing materials. In responses to our survey, for example, Security Programs Managers pointed out that SEPS's memorandums often modify or correct prior memorandums, making it difficult to determine whether the order or one of the various memorandums is the correct guidance. In PERSG's 2004 customer service survey, Security Programs Managers rated PERSG lowest in the area of policy guidance.

According to SEPS employees, SEPS has not consolidated the updates it has issued into a revised policy because its staff in the Policy, Training, and Oversight Section were dedicated to processing SEPS's background investigation caseload. In December 2004, in response to an inquiry related to another OIG review, SEPS officials told us that they had begun consolidating and updating the existing guidance on employees. However, as of July 2005, the revised DOJ Order 2610.2A was still undergoing review. Moreover, SEPS had not worked on new requirements for contractors – and for visitors – since March 2005. Further, SEPS staff told us that the order cannot be finalized until OPM approves SEPS's proposed minimum level of background investigation for hiring public trust employees. SEPS was also waiting for OMB guidance on implementation of HSPD-12 since this guidance may supersede SEPS's proposed changes to both DOJ Order 2610.2A and contractor policy.

Limited Use of Technology. SEPS has not effectively used available technology to disseminate policy and guidance. We examined SEPS's presence on the Department's intranet and found that the Personnel Security page consisted solely of a list of tasks that PERSG handles. Although adjudicative guidelines were available on the SEPS site as an appendix to the Security Program Operating Manual and several relevant regulations and executive orders were listed on the Security Policies page, the Personnel Security page did not contain a link or cross-reference to this information. Further, that page did not provide

⁴⁵ SEPS has taken initial steps to draft a reinvestigation policy for all Department contractors, but inadequate staffing and potential changes in federal standards under HSPD-12 have delayed the drafting. SEPS had already identified a need for a review of contractor reinvestigation guidance when we interviewed SEPS officials in March 2004.

Department personnel security policies, did not identify the names or dates of Department policies currently in effect, and did not provide answers to commonly asked questions. Because this information was not readily available on the intranet, PERSG and CRS staff provided guidance by answering case-specific questions from components or faxed copies of memorandums upon request.

We also examined the CRS section of the SEPS intranet and found that with the exception of the Security Program Operating Manual issued in May 2005, it contained only limited and outdated information. When we interviewed CRS staff in February 2005, they noted that they had requested that copies of the checklists used to conduct compliance reviews, the package of information sent to Security Programs Managers when a compliance review is announced, and training materials be posted on the web site.

PERSG's 2004 customer service survey also identified shortcomings in online guidance. In particular, several components commented on SEPS's failure to use the intranet effectively. For example, one component stated that "PERSG is behind the times when it comes to posting information to the DOJ intranet. It would be helpful if personnel security information was made available."

Our interviews with SEPS staff identified three reasons for the delays in posting information. First, SEPS gave no priority to the posting of information on its web site. Second, SEPS did not clearly define internal responsibilities and approval processes for posting information. Third, SEPS officials did not follow up to ensure that approved information was posted to the web site.

In June 2005, we contacted an official from the Department's Office of the Chief Information Officer (OCIO) to determine what the procedures for posting information on the web site were.⁴⁶ An OCIO

⁴⁶ A 2005 Departmental restructuring transferred the e-Gov staff from the Department's library to the OCIO. The e-Gov staff is responsible for posting information from the Offices, Boards, and Divisions on the intranet. Individual offices are responsible for approving content prior to submitting documents to be posted; the e-Gov staff converts that content to a format appropriate for posting, and ensures that information is also accessible to disabled users. Many of the larger components or offices have the ability to post information directly, without contacting the e-Gov staff for assistance.

official stated that approved information submitted in the required format would be posted within a few days of receipt. In July 2005, we revisited the web site to determine whether SEPS had begun posting information. We found that the May 2005 *Security Program Operating Manual* had been posted. However, other information that CRS staff told us in February 2005 had been submitted for internal SEPS approval was still not on the web site.

SEPS's Oversight of Components With Delegated Authority

SEPS has not implemented an effective oversight program to ensure that components with delegated authority to adjudicate background investigations comply with regulations and policy regarding personnel security. SEPS has delegated to 20 components the authority to perform adjudications and grant security clearances for employees or contractors, but SEPS remains responsible for conducting oversight to ensure that the components are carrying out their delegated authority in accordance with Department regulations. SEPS receives an annual statistical report from OPM on the Department's performance in meeting the 90-day adjudication standard. However, SEPS's primary method of overseeing components' operations is the security compliance reviews conducted by CRS. The CRS reviews are limited both in number and in scope of the examination related to personnel security. Further, both SEPS and the components' Security Programs Managers have limited authority to ensure that corrective actions are taken.

SEPS Conducts Few Security Compliance Reviews. Overall, SEPS inspects less than 1 percent of Department offices each year. According to the CRS Chief, SEPS's internal goal is to conduct 60 security compliance reviews each year. However, with a staff of only three Security Specialists and an annual travel budget of \$60,000, CRS has been unable to meet this goal. In the past 3 years, CRS has achieved its goal of conducting 60 reviews only once, completing an average of 39

compliance reviews each year (Table 7).⁴⁷ At that rate, it would take SEPS approximately 75 to 90 years to inspect all of the Department's estimated 3,000 to 3,500 offices.

Table 7: CRS Reviews Conducted in Calendar Years 2002-2004			
Year	Component Offices Reviewed (Number of Reviews Conducted)	Total Reviews	Percentage of Department Offices
2002	Civil Division (1), Office of Community Oriented Policing Services (1), Criminal Division (2), Civil Rights Division (1), DEA (19), Environmental and Natural Resources Division (1), EOUST (4), FBI (14), INS (6), Office of Justice Programs (1), OIG (1), Tax Division (1), USAO (4), USMS (5)	61	2.0
2003	ATF (1), Executive Office for Immigration Review (1), EOUST (1), FBI (3), JMD (1), USAO (8), USMS (4)	19	0.6
2004	ATF (4), BOP (1), Criminal Division (1), Community Relations Service (1), DEA (3), Executive Office for Immigration Review (3), EOUST (5), FBI (5), USAO (8), USMS (6)	37	1.2

Source: CRS

Similar to the adjudication staffing studies discussed earlier, in 2002 a CRS Security Specialist conducted a study that compared the number of SEPS Security Specialists with the number of Security Specialists in other security compliance review offices within and outside the Department. According to the CRS comparison, in 2002 CRS had two Security Specialists to conduct reviews of the Department's approximately 3,000 offices. In contrast, CRS's data indicated that the FBI had 37 security staff to conduct reviews of its 500 offices and the DEA had 6 security staff to conduct reviews of its 100 offices. Those staffing levels provide a staff-to-workload ratio of 1,500 offices per Security Specialist for SEPS, as compared with 13.5 for the FBI and 16.7 for the DEA. CRS has gained one additional Security Specialist since 2002 and currently has three Security Specialists. However, this still

⁴⁷ During 2002, SEPS staff conducted inspections of overseas offices. Because most overseas offices are housed within an embassy in which the Department of State retains responsibility for physical security and security conditions are identical for Department components in the embassy, SEPS was able to conduct multiple component reviews at most locations and expedite each review. The number of reviews was lower in 2003 because SEPS was tasked by Congress to conduct physical security surveys of Department offices in buildings operated by the General Services Administration nationwide in order to assess the buildings' physical security vulnerabilities. In response to the congressional mandate, CRS conducted 137 physical security building inspections.

leaves SEPS's staff-to-workload ratio at 1,000 offices per Security Specialist.

SEPS also receives annual reports from OPM on component compliance with the regulatory requirement that adjudications be completed within 90 days. In response to the OPM reports, the CRS site visits, or other information, SEPS may request that OPM conduct an in-depth review of components' management of background investigations. This occurs infrequently. According to SEPS, the most recent OPM review it requested was of the ATF when that component transferred from the Department of the Treasury to the Department of Justice.⁴⁸ PERSG has the option of requesting OPM appraisals of the component programs more frequently, but told us that they recognized from the difficulty they experienced in obtaining a review of the ATF process that OPM has to balance these requests with its own heavy workload of investigations.

Personnel Security Issues Receive Minimal Attention. In addition to conducting few security compliance reviews, CRS also devotes little time to personnel security issues during each review. During the 2-day security review we participated in, CRS staff spent about 4 hours on personnel security issues. CRS staff confirmed that 3 to 4 hours per review was typical. That includes both time spent reviewing background investigation files before the site visit and time spent reviewing personnel security issues on site at the office under review.

Because components' background investigation files are maintained centrally, prior to each site visit Security Specialists spend 2 to 3 hours reviewing background investigation files of select employees from the office that will be reviewed. We accompanied a Security Specialist on a file review to observe the procedure. The Security Specialist selected 30 personnel files (26 employees and 4 contractors) out of the approximately 150 employees assigned to the office under review. CRS reviews the files to determine whether investigations have been initiated and adjudicated within the timeframes required by regulations, waivers have been appropriately requested and approved, required reinvestigations have been initiated, required paperwork (such as nondisclosure agreements and security clearance justifications) have

⁴⁸ OPM found the ATF capable of conducting its own field investigations and adjudications for its staff and contractors.

been placed in the file, and the requested clearance level is appropriate for the level of classified information accessed by the employee.

Component security officials in field offices have limited involvement in background investigations. Therefore, SEPS Security Specialists typically spend only about an hour on personnel security issues while on site. During that time they question security staff and other employees to determine how employees and their supervisors are notified of pending reinvestigations, whether training is provided on handling classified material, what information security staff and managers have on personnel clearance levels, and how background investigations of locally hired contractors and interns are conducted.

The security compliance review reports that we examined identified a limited number of problems related to administrative personnel security. The 20 reports issued in FY 2003 contained a total of 4 findings (direct violations of federal regulations) and no observations (vulnerabilities not directly covered by federal regulations) related to personnel security.⁴⁹ The findings were: (1) required reinvestigations had not been initiated for some employees; (2) an employee was in a sensitive position without a completed and favorably adjudicated background investigation on file; (3) employees who did not need access to national security information had been given national security clearances; and (4) memorandums requesting security clearances lacked accurate need-to-know justifications. CRS staff stated that the deficiencies cited in the FY 2003 reports are typical of what they found in more recent site visits.

Security Specialists do *not* review the quality of the adjudication or investigation of employees' and contractors' background investigations or reinvestigations, nor do any other personnel in SEPS. CRS staff explained that they do not examine files for substantive issues or to determine whether there are investigations or disciplinary actions pending, as such in-depth reviews would mean less time for higher priority physical and information technology security oversight. Instead, Security Specialists ensure only that the required paperwork (e.g., signed

⁴⁹ In contrast, the 20 reports issued in FY 2003 contained a total of 2 findings and 78 observations related to physical security. CRS staff stated that because there are few federal or Department standards on physical security, important security issues are often addressed in observations.

disclosure forms for cleared employees) is included in employees' files and that reinvestigations are timely.⁵⁰

When asked whether they were concerned that no personnel at SEPS perform any qualitative reviews of components' adjudications, SEPS officials confirmed that they were. They stated that it is not currently possible for SEPS to ensure that components effectively identify national security concerns during adjudications. However, SEPS officials noted that other case processing and security oversight issues remained a higher priority.

CRS Has Limited Authority to Correct Problems. CRS has no formal authority to compel a component to correct a security violation.⁵¹ The six current and former CRS Security Specialists we interviewed all commented that because of this limitation, CRS must carefully decide which compliance issues it pursues aggressively. For example, CRS found that the ATF obtains national security clearances for all its Special Agents, including those who work in offices that do not handle classified information. Nor does the ATF periodically review whether these security clearances are necessary.⁵² CRS informed us that this practice is not consistent with security regulations and therefore must be reported as a finding.⁵³ CRS told us that it had reported this deficiency during prior reviews of ATF field offices, and on the site visit we observed, we noted that the Security Specialist again raised the issue. However, neither CRS nor the ATF Security Programs Manager had the authority to compel the

⁵⁰ Reinvestigations are considered timely if the initiation paperwork is submitted by the end of the fiscal year in which the reinvestigation is due.

⁵¹ For example, although CRS requests that components either implement changes required by their findings or report why the changes could not be implemented, of the 20 reports issued in FY 2003, 11 components responded within the requested 60 days, 4 components responded after 60 days (ranging from 2 to 7 months after the due date), and 4 components did not respond to CRS at all.

⁵² A waiver of the periodic review may be granted if the component can show a continuing need for all employees to be cleared. For example, SEPS granted the FBI a waiver because it demonstrated such a need.

⁵³ Under 28 C.F.R. § 17.12(d), each component head must "continuously review the requirements for personnel access to classified information as a part of the continuous need-to-know evaluation, and initiate action to administratively withdraw or reduce the level of access authorized, as appropriate." SEPS interprets this regulation to require at least an annual review of employee security clearances to verify that the employee still requires access.

ATF to either limit the number of clearances or obtain a waiver of the requirement that clearances be given only to those who must handle classified information. CRS staff stated that they will continue to report this issue, but that CRS's priority is resolving more immediate physical security risks.

While component Security Programs Managers provide assistance to CRS, both in identifying security weaknesses and addressing CRS's site visit findings and observations, their authority is also limited. DOJ Order 2600.2C assigns Security Programs Managers 11 separate areas of responsibility for ensuring the security of their respective components, but it provides no specific instructions on the measures Security Programs Managers can take to enforce security requirements. In our survey of Security Programs Managers, several explained that they were unable to implement a CRS finding because there was a component policy that the Security Programs Manager could not change (such as some components' policies of obtaining national security clearances for all law enforcement officers).

PERSG Has Limited Authority to Correct Problems. Just as CRS has no formal authority to require components to comply with personnel security regulations, PERSG has no formal authority to require individuals to comply with personnel security regulations. Because SEPS cannot effectively identify and track all the Department employees who are overdue for reinvestigation, it cannot perform effective oversight to ensure compliance with that requirement.

In its management of component background investigations, PERSG is responsible for ensuring that personnel submit the paperwork to initiate their background reinvestigations in a timely manner. To facilitate compliance for the 27,000 employees and 7,000 contractors for whom SEPS has retained authority, SEPS provides each component's Security Programs Manager with a list of personnel whose reinvestigations must be initiated by the end of the fiscal year. SEPS maintains records of personnel who have not submitted the necessary reinvestigation paperwork in a timely manner (PERSG refers to these cases as the "backlog"), and forwards the backlog lists to the Security Programs Managers to follow up with the individuals. SEPS also

provides a list to the OIG of personnel for whom it has not received the necessary reinvestigation paperwork.⁵⁴

We asked SEPS staff and the Security Programs Managers about how backlogged cases are handled and, more specifically, how noncompliance is addressed for personnel with security clearances and for personnel in public trust positions. For personnel with security clearances, SEPS staff stated that personnel generally comply with SEPS's requests for reinvestigation paperwork because SEPS can administratively withdraw clearances for failure to submit the paperwork.⁵⁵ Security Programs Managers in our survey confirm that they do obtain paperwork from personnel who require access to classified information. In contrast, for personnel in public trust positions, which do not require a security clearance, SEPS staff stated that they have no sanctions comparable to the administrative withdrawal of a clearance. To obtain compliance, they send a memorandum to the OIG reporting personnel overdue for reinvestigation, and may also involve the Security Programs Managers. Security Programs Managers can initiate disciplinary procedures for noncompliance, but stated that it is a lengthy process. Both SEPS and the Security Programs Managers stated that they do eventually obtain compliance.

Incorrect SEPS Data on EOUSA Reinvestigations. To confirm that overdue individuals are eventually submitting their paperwork, we reviewed TRAQ data to identify personnel more than 1 year overdue for reinvestigation as of March 2005. According to the TRAQ data, there were 399 Department personnel who were more than 1 year overdue for reinvestigation, of whom 357 were EOUSA employees. SEPS explained that this data was erroneous because EOUSA initiates its own reinvestigations and does not report the initiations to SEPS. Consequently, the individuals continue to be shown in TRAQ as overdue for reinvestigation.

⁵⁴ SEPS also monitors and reports to Security Programs Managers and the OIG cases in which it believes an employee has entered on duty without the necessary waiver and initiation of a background investigation. SEPS informed us that some of these cases are due to a component's slow reporting, but in other cases background investigations have not been initiated. For FY 2003 through FY 2005, these cases generally numbered fewer than 20 per year.

⁵⁵ Administrative withdrawals of national security clearances can occur for a variety of reasons, including a component's determination that an employee no longer needs access to classified information.

Because SEPS did not have complete and accurate data in TRAQ on the specific number of individuals in the Department that were more than 1 year overdue for reinvestigation, in May 2005 we requested information on a sample of 28 overdue cases to determine how many were actually overdue and how many were erroneous entries in which reinvestigations were not reported by the component. Of the 28 sample cases, 14 were erroneous entries that either had a reinvestigation initiated or in which the employee did not require reinvestigation for other reasons (such as that they were no longer employed by the component). Of the 14 cases in which the employee was actually overdue for reinvestigation, we found that half – including all the individuals holding NSI clearances – were less than 2 years overdue, but some public trust employees had been overdue for longer periods, including one individual who was more than 10 years overdue for reinvestigation. Overall, our analysis indicated that processing delays accounted for approximately half of the backlogged EOUSA cases. Nonetheless, even accounting for the erroneous EOUSA entries, most of the backlogged cases involved EOUSA employees.⁵⁶

Because SEPS cannot independently identify when EOUSA initiates reinvestigations, it provides an annual status report to EOUSA showing the individuals overdue for reinvestigation and requests that EOUSA initiate appropriate action. The status reports we reviewed did not specifically request that EOUSA provide a response, and the PERSG Chief of Operations told us that EOUSA often does not respond directly to the status reports. Consequently, SEPS often only learns that a reinvestigation has been initiated when EOUSA forwards the results of the OPM field investigation.

The Department does not have a centralized database containing information on the status of background investigations and reinvestigations that can be accessed and updated by SEPS staff, the components for which it retains authority (such as EOUSA), or components with delegated authority. As we will discuss in greater detail beginning on page 40, SEPS's inability to monitor and manage overdue reinvestigations is one example of the limitations of the Department's current technological resources.

⁵⁶ EOUSA employees represent 89 percent of the backlog (357 of 399 cases in FY 2004), and only 54 percent of the employees for whom SEPS has retained authority (14,535 employees of 26,906). If half of the apparent backlog represents a delay in reporting, 81 percent (179 of 221) of the backlog would be EOUSA employees.

The Department's Resource Requests for SEPS

Despite efforts to increase SEPS's staff and secure funding for technology improvements, the Department has not received increased appropriations for SEPS. In its FY 2005 budget submission, SEPS requested three additional PERSG positions, six additional compliance review security specialists, \$2,000,000 to replace the TRAQ database, and \$105,000 in additional travel money for CRS site visits. SEPS's budget submission tied the need for additional funding directly to the Department's counter-intelligence priority and the importance of ensuring that the Department hire and retain only trustworthy personnel. The request noted that PERSG staff had worked more than 500 hours of overtime since October 1, 2002, but that PERSG was still backlogged. The request explained that the existing PERSG file tracking system, TRAQ, was at the end of its life cycle and at full capacity, and that a new Department-wide system was needed to enable SEPS to adequately monitor the Department's personnel security program. The budget submission noted the Department's growing presence overseas and the need to ensure that the Department's most vulnerable facilities be reviewed at least every 5 years.

The Department supported the budget request, and the Office of Management and Budget approved the personnel requests and \$1,500,000 for the new database. Funding for these items was included in the appropriations bill approved by the House, but it was not included in the final version of the appropriations bill passed by Congress for FY 2005. PERSG has reduced its backlog since the budget submission, but as previously noted, it is not able to meet regulatory timeliness requirements at its current staffing level. Moreover, as discussed below, with the implementation of HSPD-12 and the Intelligence Reform Act, SEPS will face an increased workload, more stringent timeliness requirements, and an expanded oversight role.

SEPS's File Tracking System

The file tracking system SEPS uses is outdated, at full capacity, and does not include needed capabilities. PERSG staff told us that they selected the system, an inventory management program called TRAQ, because it had a barcode-scanning capability that allowed PERSG to track the physical location of each personnel security file. Currently, PERSG's TRAQ system contains information on approximately 27,000 Department employees and 7,000 contractors. This represents

approximately one-fourth of the Department's employees and an unknown percentage of its contractors. TRAQ contains no information on the approximately 76,000 employees who work in the components with delegated adjudicative authority.

Because TRAQ was designed to be an inventory management system, SEPS has modified the TRAQ software extensively to accomplish its internal case monitoring tasks. SEPS regularly obtains management reports from TRAQ to set adjudication priorities, identify personnel due for reinvestigation, evaluate security clearance levels, and monitor its adjudicative backlog. However, according to SEPS's technical staff, TRAQ does not provide needed capabilities and cannot be modified further. In a briefing prepared for the budget director on SEPS's justification for its FY 2006 budget request, SEPS staff stated that the TRAQ vendor told SEPS it has pushed the system well beyond its limits and capacity and is at risk of losing data due to system crashes. SEPS staff further stated, "The application will eventually fail due [to] the amount of records the system is trying to manipulate." TRAQ's specific limitations include:

- TRAQ cannot be modified to support continuity of operations. SEPS staff stated that because the system does not support scanned images, the paper files must be retrieved for each step in the background investigation process. We determined that in FY 2004, there were 13,509 transactions recorded in TRAQ for which paper files were needed. SEPS informed us that there were an additional 5,166 transactions on SCI clearances and clearance certifications, which are kept in separate paper files and not recorded in TRAQ.⁵⁷ Four file room clerks are needed to manage the paper copies of the files. (See Tables 1 and 2 for workload statistics.) Further, all of SEPS's paper files are maintained in one location. Because electronic copies have not been made, the loss of the paper records would severely disrupt case processing and clearance verification. For example, if a bioterrorist attack precluded access to the building housing the records, SEPS would lose access to a significant portion of the documents supporting

⁵⁷ The 5,166 SCI clearance and clearance verifications took place in calendar year 2004.

the adjudication of employees' background investigations and other suitability issues.⁵⁸

- TRAQ crashes and file corruptions occur frequently. Because the system is outdated and operating over its intended capacity, system crashes and file corruption are a common occurrence. SEPS did not keep a log of the frequency or duration of system malfunctions, but the SEPS technical staff we interviewed stated that, at times, system crashes occurred several times a day. Because SEPS has modified the system beyond its intended capabilities, it is no longer fully supported by the vendor. As a result, SEPS technical staff must troubleshoot TRAQ and maintain electronic and hard copy backups.
- TRAQ has no internal quality control features. TRAQ lacks the quality control capabilities typically built into databases to ensure data accuracy. For example, TRAQ does not recognize when processing dates for cases are not sequential. Because the software lacks internal quality controls, SEPS pays a contractor to review the data entry for accuracy.
- TRAQ is accessible only to SEPS personnel. Personnel security staff from the components cannot directly access TRAQ. As a consequence, they cannot obtain case processing status or verify clearances without faxing requests or telephoning SEPS adjudicators for updates. In their responses to the PERSG customer service survey and our survey of Security Programs Managers, a number of components stated that they want to access status information on particular cases without having to call PERSG.
- TRAQ's report-generating capabilities are limited. PERSG staff told us that TRAQ cannot easily generate ad hoc reports or reports that can be shared with components or other external agencies. Advanced programming skills are necessary to create new reports from TRAQ, and the layout cannot be modified to improve clarity. SEPS staff must export data from TRAQ into Microsoft Access to generate reports it routinely shares with the components, such as

⁵⁸ SEPS could reconstruct the adjudicative decisions and personnel security files from backup copies of TRAQ and copies of material obtained from the investigating agencies, personnel and internal affairs offices and other sources, but the process would be time-consuming.

reports on cases pending adjudication or requiring reinvestigation, and individuals who have been hired on waivers.

No Centralized Background Investigation Database

The Department has no centralized personnel security database that SEPS can use to monitor the background investigation status of all Department employees. Instead, components maintain information on the background investigations of their personnel in separate systems that are not interoperable or accessible to SEPS. Some components keep their records in Oracle databases, while others maintain their records in Microsoft Access databases or Excel spreadsheets. Further, these systems do not track the same information regarding the background investigation process steps to enable comparison across components.

Based on our review of SEPS's budget requests and our discussions with SEPS staff regarding their oversight program, we identified a number of areas in which the lack of a centralized database impedes SEPS's ability to conduct oversight of the components' background investigation processes:

- SEPS cannot systematically monitor compliance with prehiring requirements. Components must initiate a background investigation and complete a waiver before personnel can enter on duty. SEPS monitors compliance with this requirement for its own workload by downloading biweekly National Finance Center data and comparing it to background investigations. While SEPS has this tool available for monitoring compliance in the components for which it has retained authority, it is not able to conduct comparable tests to monitor compliance in the components with delegated authority.
- SEPS cannot systematically monitor compliance with reinvestigation requirements. Because EOUSA initiates its own reinvestigations, SEPS cannot determine which reinvestigations EOUSA has initiated until it receives the paperwork, often more than a year later. SEPS therefore cannot identify EOUSA personnel who have not completed reinvestigation requirements. SEPS also cannot systematically monitor compliance with reinvestigation requirements in the components with delegated authority, such as timely initiation of reinvestigations and timely adjudication of completed reinvestigations, because those components initiate and adjudicate their own reinvestigations.

-
- SEPS cannot conduct random reviews of the completeness of component field investigations. CRS staff must notify components in advance to obtain rosters and paper copies of the files, and does not review the substance of the adjudicator's decision.
 - SEPS cannot verify that components are conducting required training on the handling of classified information. All components are required to ensure that personnel with security clearances are given initial training and refresher briefings. Security Programs Managers we surveyed reported they use a variety of tracking mechanisms, from databases to paper files, to ensure that components' employees receive initial and refresher briefings as required. However, not all Security Programs Managers from components with field offices conducted direct oversight of field office practices.
 - SEPS cannot determine electronically whether components annually certify the need for access to classified information. SEPS uses a paper questionnaire to verify that personnel in the components that SEPS manages have justified the need to retain security clearances, and oversight of component compliance with this requirement is limited to the sites CRS visits.

As described previously, TRAQ was not designed as a case management database and cannot be further expanded to provide SEPS with additional capabilities it needs to effectively oversee the components' background investigation processes. SEPS's compliance reviews cover only a small fraction of Department personnel each year. A Department-wide database with imaging capability could reduce the risks inherent in a paper-based system and enable SEPS to better oversee components' background investigations programs.

Because this review focused on SEPS, we did not examine whether the components' tracking systems are similarly limited in their capabilities to provide oversight of their internal processes. In our discussions with component Security Programs Managers and SEPS staff, however, we were informed that the DEA is the only component that currently maintains electronic copies of its background investigation files. Therefore, a Department-wide database with imaging capability could provide a security benefit to components with delegated authority, as well as to SEPS.

SEPS has identified the need for a Department-wide database and has requested resources to develop one. The Department concurred with SEPS's request, and in FY 2005, requested at least \$2 million to replace TRAQ with a Department-wide system. However, the funding was not included in the FY 2005 Appropriations Act passed by Congress.

In its FY 2006 budget request, SEPS has again sought requested funding for a Department-wide database, stating that a new Department-wide personnel security database would: (1) allow the Department to re-engineer its background investigation process to comply with the e-Gov initiative; (2) improve timeliness by electronically initiating, receiving, monitoring, and storing background investigations, reinvestigations, and security clearances; (3) improve communication and information sharing within the Department; (4) eliminate duplicate investigations, thereby saving time and money for Department components; (5) enable better enforcement of personnel security standards, and (6) support better oversight at the Department level.

New standards for background investigations contained in the Intelligence Reform Act and HSPD-12 will significantly increase SEPS' requirements for processing and oversight of background investigations. Meeting the new timeliness standards in the Intelligence Reform Act will require SEPS to significantly expedite background investigation adjudications. In addition, HSPD-12 established additional processing requirements for contractors that will increase SEPS's workload. SEPS will also be required to provide additional oversight of components with delegated authority to ensure that they comply with the standards.

Timeliness Requirements of the Intelligence Reform Act

The Intelligence Reform Act imposes progressively tighter timeliness requirements for adjudications and field investigations that will overwhelm SEPS's limited capabilities. To meet the new timeliness standards, SEPS will have to expedite adjudications significantly. SEPS also must increase its oversight of the timeliness of field investigations conducted by the FBI and the ATF to ensure that they meet the new standards. At present, we believe that SEPS is not well positioned to meet these challenges.

Adjudications. Currently, the only formal timeliness requirement is that adjudications of background investigations and reinvestigations are to be completed within 90 days.⁵⁹ The Intelligence Reform Act shortened these timeliness requirements. By the end of 2006, 80 percent of adjudications must be completed within an average of 30 days, and by the end of 2009, 90 percent of adjudications must be completed within an average of 20 days.

To meet the new timeliness standards, SEPS will have to greatly reduce the time it takes to complete adjudications. For example, according to data in TRAQ, in FY 2004 SEPS completed 59 percent of its adjudications of employees' NSI background investigations within 30 days, and completed 46 percent of its adjudications within 20 days (see Table 8). Thus, to meet the December 2006 timeliness standard of 80 percent in 30 days, SEPS will have to greatly increase the number of

⁵⁹ See 5 C.F.R. § 732.302(b).

adjudications it completes within that time. Meeting the standard for adjudications of employee reinvestigations and contractor background investigations will require even greater increases. In FY 2004, SEPS adjudicated only 31 percent of employee reinvestigations and only 21 percent of contractor background investigations within 20 days.

Table 8: How SEPS FY 2004 Adjudication Performance Compares to Intelligence Reform Act Timeliness Requirements*			
	Percentage of SEPS Adjudications Completed		
	within 90 Days	within 30 Days	within 20 Days
Standards			
Current 2005	100	—	—
December 2006	—	80	—
December 2009	—	—	90
SEPS Adjudications in FY 2004			
Employee NSI Background Investigations	87	59	46
Employer NSI Reinvestigations	60	39	31
Contractor NSI Background Investigations	93	43	21

Source: SEPS TRAQ

* For personnel with Secret or Top Secret clearances

Field Investigations. As of July 2005, there were no regulatory requirements regarding the timeliness of field investigations on background investigations. The Intelligence Reform Act requires that, by December 2006, 80 percent of field investigations be completed within 90 days. By December 2009, 90 percent of field investigations must be completed within 40 days. As with adjudications, meeting the new standards will require that field investigations be significantly accelerated from current performance levels.

The FBI and OPM conduct the field investigations on those cases for which SEPS retains adjudication authority. In FY 2004, the FBI took an average of 197 days to complete a field investigation for SEPS. The FBI completed approximately 25 percent of its NSI investigations within 90 days and less than 10 percent within 40 days in FY 2004 (see Table 9). Although OPM's actions are not within the control of the Department of Justice, we noted that the time it takes OPM to conduct field investigations for SEPS will also have to be significantly reduced to meet the new standards. In FY 2004, OPM's highest priority cases took

an average of 100 days, and its routine cases took an average of 324 days.⁶⁰

Table 9: How FBI FY 2004 Field Investigation Performance Compares to Intelligence Reform Act Timeliness Requirements*		
	Percentage of NSI Field Investigations Completed by FBI	
	within 90 Days	within 40 Days
Standards		
December 2006	80	—
December 2009	—	90
FBI Performance in FY 2004		
Employee NSI Background Investigations	24	8

Source: SEPS TRAQ

* For personnel with Secret or Top Secret clearances

Oversight Implications of Timeliness Standards. Given its currently available methods of oversight, SEPS is not well positioned to meet the standards of the Intelligence Reform Act. The Act will require SEPS to ensure that the FBI and the ATF (the two Department components with authority to conduct field investigations) meet timeliness standards for those investigations. SEPS does not currently review the timeliness of these field investigations, since there were no regulatory timeliness requirements before the Act. The new timeliness standards will also apply to the adjudications conducted by Department components with the delegated authority to carry out those actions.

Our review of SEPS's oversight of components with delegated authority found that its primary oversight of components' timeliness in adjudications is accomplished through OPM, which provides SEPS with an annual report on the Department's overall compliance with the 90-day adjudication standard, broken down by component. SEPS may then address any concerns OPM raised about timeliness with the component

⁶⁰ The FBI's field investigations for SEPS averaged 197 days in FY 2004.

directly.⁶¹ In addition, CRS examines the timeliness of the case processing in the particular files they select for review prior to field visits. However, as CRS has been conducting an average of less than 40 site visits each year, the information gained by those reviews was limited and anecdotal.

To conduct effective oversight of the components' compliance with the new requirements, SEPS will require additional data, beyond the annual compliance numbers provided by OPM, that will enable it to track cases as they progress to completion. As described above, the Department does not presently have the databases and other technological infrastructure to allow SEPS to effectively monitor and analyze the components' performance at processing background investigations.

Other Background Investigation Processing. Our review of the required timeframes established by the Intelligence Reform Act found that, as the law is written, no additional time is allowed for aspects of the background investigation process that are not included in the field investigation or adjudication phases. For example, there are three categories of cases for which an additional review is conducted between completion of the field investigation and SEPS's adjudication: (1) political appointees undergoing confirmation, whose files are reviewed by the Senate; (2) attorneys, whose files are reviewed by the Office of Attorney Recruitment and Management; and (3) non-attorney personnel at the U.S. Attorneys' Offices, whose files are reviewed by EOUSA.

Even in cases in which there is no additional review before the files are transmitted to SEPS, it can take several weeks to physically transmit the paper case files between the investigative and adjudication offices. Table 10 shows the average time lapse between when field investigations were completed and when the case files reached SEPS for adjudication during the last 5 fiscal years. In some cases, the time needed for additional reviews between the field investigation and the adjudication would make difficult, or preclude, meeting the timeframes of the Intelligence Reform Act.

⁶¹ Correspondence an OPM Investigations Program Specialist e-mailed to PERSG concerning FY 2004 indicated that OPM was generally satisfied with the Department's timeliness. (E-mail October 27, 2004, subject "Adjudication"; e-mail August 13, 2004, "Another Achievement for DOJ.")

Table 10: Average Days Between Field Investigation Completion and SEPS's Receipt*					
Field Investigation Reviewed Before Forwarding to SEPS	FY 2000	FY 2001	FY 2002	FY 2003	FY 2004
Senate-confirmed political appointees	145	89	101	50	—
Attorneys	52	37	48	73	43
EOUSA cases	185	165	199	161	129
Field Investigation Sent Directly to SEPS	40	38	26	19	10

Source: SEPS TRAQ

* For all employees

Requirements of HSPD-12

HSPD-12, issued by the President in August 2004 and scheduled to be implemented in stages beginning October 27, 2005, will expand SEPS's oversight responsibilities to include monitoring identification card recertifications for all employees and contractors, and checking hiring practices for contractors who are investigated and hired locally. The directive establishes minimum government-wide background investigation requirements for entry on duty and requires an identification card recertification process every 5 years for employees and contractors. Although the Department and SEPS had not fully decided how to implement the Directive during our fieldwork, we can describe the impact of HSPD-12 requirements on SEPS's oversight responsibilities.

Pre-Employment Background Checks. HSPD-12 requires that agencies conduct several background checks in order to issue official identification cards to employees. The minimum National Agency Checks required are the Security/Suitability Investigations Index, Defense Clearance Investigation Index, FBI Name Check, and the FBI National Criminal History Fingerprint check. In addition, HSPD-12 requires that written inquiries be sent to verify past employment, education, residences, and references. It also requires a check of law enforcement databases for addresses where the applicant has lived. This background investigation is called the NACI (National Agency Checks with Inquiries). As initially issued, HSPD-12 required that all steps of the investigation except the paper inquiries be completed before employees could be issued identification cards. In FY 2004, this process took an average of 89 days to complete, according to information that OPM provided to SEPS regarding the NACI process.

In May 2005, Department officials from SEPS and the OCIO involved in implementation of HSPD-12 raised concerns about the length of time necessary to complete the NACI process. They were particularly concerned about delays encountered in the FBI Name Check process.⁶² In August 2005, OMB amended the guidance on the directive to state that if the results of the National Agency Checks were not received within five days, only completion of a favorable fingerprint check would be required prior to issuance of a building access identification card.

Identification Card Recertifications. HSPD-12 requires that background checks be verified every 5 years in order to renew each employee's identification card. As described to us by OCIO staff, the recertification will not require a new NACI check. Instead, the office that issues the identification card will check the employee's personnel security record to verify that an HSPD-12 certification was completed when the identification card was originally issued. As long as the check of the employee's personnel record does not reveal any other prohibiting factors, the card may be recertified.

One potential increase in SEPS's reinvestigation workload could occur because the timeframes established by HSPD-12 for renewing identification cards do not coincide with existing OPM requirements for background reinvestigations. HSPD-12 guidelines require that identification cards be renewed no more than 5 years after issuance, whereas OPM's standards consider a reinvestigation to be current if it is initiated within 5 years after the previous background investigation was completed. Therefore, an employee's HSPD-12 identification card must be recertified before SEPS is required to complete a reinvestigation. SEPS officials told us that the possibility of requiring a reinvestigation before an HSPD-12 identification card is renewed had not been ruled out as of July 2005. However, if SEPS conducts these actions separately, the number of cases SEPS will have to track and manage each year will increase.⁶³ Conversely, if the decision is made to conduct

⁶² According to the Section Chief of the FBI National Name Check Program, the FBI Name Check can take extended period of time because of a number of factors, including the steady increase in the number of routine and expedited requests that have resulted from government-wide changes to security, citizenship, and visa application policies; understaffing in the FBI's National Name Check Program office that processes the name check requests; and the need for a manual review of case files that are identified by the FBI database as possible hits.

⁶³ According to TRAQ, about 2,400 employees were reinvestigated in each of the last 5 years.

reinvestigations early so that they are completed concurrent with the HSPD-12 recertification, that would effectively shorten the reinvestigation cycle, which would in turn result in an increase in the number of reinvestigations that SEPS would have to conduct each year.

Oversight of Contractors. Our review of the SEPS oversight program found that it will have to be expanded if it is to cover components' compliance with all HSPD-12 requirements regarding contractors. Staff from SEPS and the OCIO confirmed that HSPD-12 requirements will extend to certain contractors who are currently investigated and hired at the local level without centralized oversight. At present, SEPS obtains no case processing information on contractors hired locally by components. CRS security staff told us that when they visit a site that has locally-hired contractors, they request a roster and check the files kept on site. CRS will also talk to the General Services Administration about shared contract staff, such as janitors.⁶⁴ The lack of a central Department-wide database prevents SEPS from easily identifying whether contractors from sites it has not visited have received the proper background check or even whether they are still employed.

⁶⁴ Prior OIG reports found that these contractors' employment status cannot be easily verified because they are not always paid through the centralized National Finance Center payroll system. See "Background Investigations Conducted by the United States Marshals Service," OIG Evaluation and Inspections Division Report I-2005-002, February 2005. A May 2005 OIG Audit report indicated concern that the USMS could not document the background investigations of over half its locally hired contractors. See "United States Marshals Service's Use of Independent Contractors as Guards," Audit Report 05-24, May 2005.

CONCLUSIONS AND RECOMMENDATIONS

As the Department's primary security office, SEPS is responsible for adjudicating background investigations, initiating reinvestigations, and providing security clearances for approximately 27,000 of the Department's approximately 103,000 employees and about 7,000 contractors. In addition, SEPS is responsible for developing, implementing, and disseminating security policies to all Department components. It must also oversee the physical, personnel, contractor, information, computer, emergency preparedness and communications security programs of the Department's 3,000 to 3,500 field offices.

To compensate for the increase in background investigation workload during FY 2000 through FY 2004, SEPS prioritized its responsibilities, placing the greatest emphasis on adjudicating background investigations and on processing and verifying SCI clearances. As a result, in FY 2004, it met federal regulatory requirements for adjudicating background investigations within 90 days in 99 percent of its highest priority cases and in 85 percent of cases overall. Department components also expressed satisfaction with the service SEPS provided on SCI clearances and clearance verifications for Department employees and contractors. However, SEPS did not process lower priority reinvestigations on time and did not fully meet other important responsibilities related to policy and oversight. Moreover, new standards for background investigations contained in the Intelligence Reform Act and HSPD-12 will significantly change the standards the Department must meet in completing background investigations.

Policy Guidance. The policy guidance SEPS provides on the management of background investigations is inconsistent, outdated, and not widely and readily accessible. SEPS has not issued a complete revision of DOJ Order 2610.2A since 1990. Instead, SEPS has issued over 40 separate update memorandums between 1990 and 2005. Moreover, the guidance does not reflect changes in the security environment since September 11, 2001. SEPS's personnel security staff told us that it has been unable to issue updated security policies and guidance because of limited staff, a small budget, and an increasing caseload. We also found that SEPS has not effectively used available technology, such as the Department's intranet, to disseminate updates to policy and guidance. As a result, Security Programs Managers indicated in surveys that they find the guidance confusing.

Limited Oversight. CRS serves as the primary vehicle for conducting oversight of the personnel security operations of components with delegated authority for managing background investigations. However, we found that CRS reviews are limited both in number and in the scope of the examination related to personnel security. With only three Security Specialists in CRS, SEPS is generally unable to meet its goal of conducting 60 security compliance reviews each year. Even if it could complete 60 reviews, that would be about 2 percent of the Department's offices. Further, personnel security constitutes a small portion of each review, and Security Specialists do not perform substantive reviews of adjudication or investigation quality. We concluded that this minimal oversight is insufficient to ensure that the Department is in compliance with personnel security regulations.

SEPS also relies on outdated technology for case tracking. Because TRAQ is a stand-alone system unavailable to other components, SEPS employees and security officials in other components have no centralized source for background investigation data. Further, because TRAQ was not designed as a case management database, it lacks internal quality controls or image scanning capabilities. SEPS therefore must rely on manual quality reviews and paper-based background investigation files. The reliance on paper-based files, which are all stored in one location, presents a security risk in the event those records are destroyed or inaccessible. According to TRAQ managers, the application has reached system capacity and frequently crashes, causing file corruption. Further, because there is no Department-wide database of background investigation information, SEPS cannot perform systematic oversight of the components to identify weaknesses in the Department's personnel security program, such as components' failure to comply with NSI requirements.

SEPS Not Well Positioned to Meet New Requirements. With its current resources, processes, and authority, SEPS will have difficulty both in meeting the performance requirements of the Intelligence Reform Act and HSPD-12, and in providing oversight of the Department's compliance with those requirements. The Intelligence Reform Act requires that, by the end of 2006, 80 percent of NSI adjudications must be completed within 30 days, and by 2009, 90 percent of NSI adjudications must be completed within 20 days. SEPS will have to significantly improve its timeliness to meet the standards mandated by the Intelligence Reform Act, because in FY 2004, SEPS completed only 59 percent of its NSI adjudications within 30 days. At current staffing

levels, SEPS will not be able to speed up adjudications to meet these requirements.

Also, HSPD-12, which mandates a standardized identification card for government employees and contractors, will change the Department's hiring practices. HSPD-12 will require that SEPS expand its oversight program to monitor the background investigation process for locally hired contractors. However, until a consolidated Department-wide background investigation database is implemented, SEPS has neither the technological infrastructure nor the staff to monitor compliance with these requirements.

While we believe that SEPS has taken reasonable steps to use the resources available to meet its case processing workload, SEPS nonetheless cannot fully meet existing and future regulatory requirements. To effectively carry out its responsibilities, SEPS must improve its capabilities for managing background investigations, providing timely and accurate policy guidance for the Department, and conducting oversight to ensure the effective administration of the background investigation program in the Department.

RECOMMENDATIONS

We make six recommendations to help improve SEPS's performance of its personnel security responsibilities and better position the Department to meet the requirements of the Intelligence Reform Act and HSPD-12.

We recommend that the Department:

1. Develop a Department-wide plan for implementing the personnel security requirements of the Intelligence Reform Act and HSPD-12, and identify the resources that will be needed to enable the Department to meet the new requirements.
2. Develop a Department-wide database with imaging capability to enable uniform processing and tracking of employee and contractor personnel security actions, permit central oversight of personnel security operations, and reduce the vulnerability caused by reliance on paper records.

We recommend that SEPS:

3. Once OPM provides the necessary policy decisions, expeditiously issue an updated Department personnel security policy, DOJ Order 2610.2A.
4. Develop a plan for conducting routine oversight of components with delegated authority that provides reasonable coverage and ensures that the background investigations and adjudications meet established standards for both quality and timeliness.
5. Institute an annual report to the Deputy Attorney General to describe the performance of the Department and each component in adjudicating background investigations and in complying with Department personnel security regulations and policies.
6. Establish procedures to identify the policies, documents, and other information necessary for personnel security operations, and in coordination with the Department's Office of the Chief Information Officer, make the documents available through the SEPS web site.

APPENDIX I: Components With Delegated Authority

Delegated Authority Related to Background Investigations			
Office of the Attorney General Office of the Deputy Attorney General Office of the Associate Attorney General (authority not delegated)			
	With Delegated Authority?		With Delegated Authority?
Office of the Solicitor General		Federal Bureau of Prisons	✓
Office of the Inspector General	✓	Drug Enforcement Administration	✓
Office of Legal Counsel		Federal Bureau of Investigation	✓
Office of Legal Policy		Bureau of Alcohol, Tobacco, Firearms, and Explosives	✓
Office of Intelligence Policy and Review		U.S. Marshals Service	✓
Office of Professional Responsibility		INTERPOL - U.S. National Central Bureau	✓
Office of Legislative Affairs		Executive Office for Immigration Review	✓
Office of Intergovernmental and Public Liaison		Office of the Pardon Attorney	
Office of Information and Privacy		U.S. Parole Commission	✓
Office of Public Affairs		Executive Office for U.S. Trustees	✓
Office of Dispute Resolution		Community Relations Service	✓
Justice Management Division		Foreign Claims Settlement Commission	
Executive Office for U.S. Attorneys	✓	Office of Justice Programs	✓
Antitrust Division	✓	Office of Community Oriented Policing Services -- COPS	
Civil Division	✓	National Drug Intelligence Center	✓
Civil Rights Division	✓	Professional Responsibility Advisory Office	
Criminal Division	✓	Office of the Federal Detention Trustee	
Environment and Natural Resources Division	✓	Office on Violence Against Women	
Tax Division	✓		

Source: Department of Justice Public Website (<http://www.usdoj.gov/jmd/mps/mission.htm>)

Components With Delegated Authority to Conduct and Adjudicate Background Investigations and Reinvestigations				
Components	With Delegated Authority to Conduct Field Investigations for:^a		With Delegated Authority to Conduct Adjudications for:	
	Employees	Contractors	Employees	Contractors
OIG				✓
Executive Office for United States Attorneys				✓
Antitrust Division				✓
Civil Division				✓
Civil Rights Division				✓
Criminal Division				✓
Environmental and Natural Resources Division				✓
Tax Division				✓
Federal Bureau of Prisons			✓	✓
DEA			✓	✓
FBI ^b	✓	✓	✓	✓
ATF ^c	✓	✓	✓	✓
USMS ^d		✓	✓	✓
INTERPOL				✓
Executive Office for Immigration Review				✓
U.S. Parole Commission				✓
Executive Office for United States Trustees			✓	✓
Community Relations Service				✓
Office of Community Oriented Policing Services				✓
National Drug Intelligence Center			✓	✓

Source: SEPS

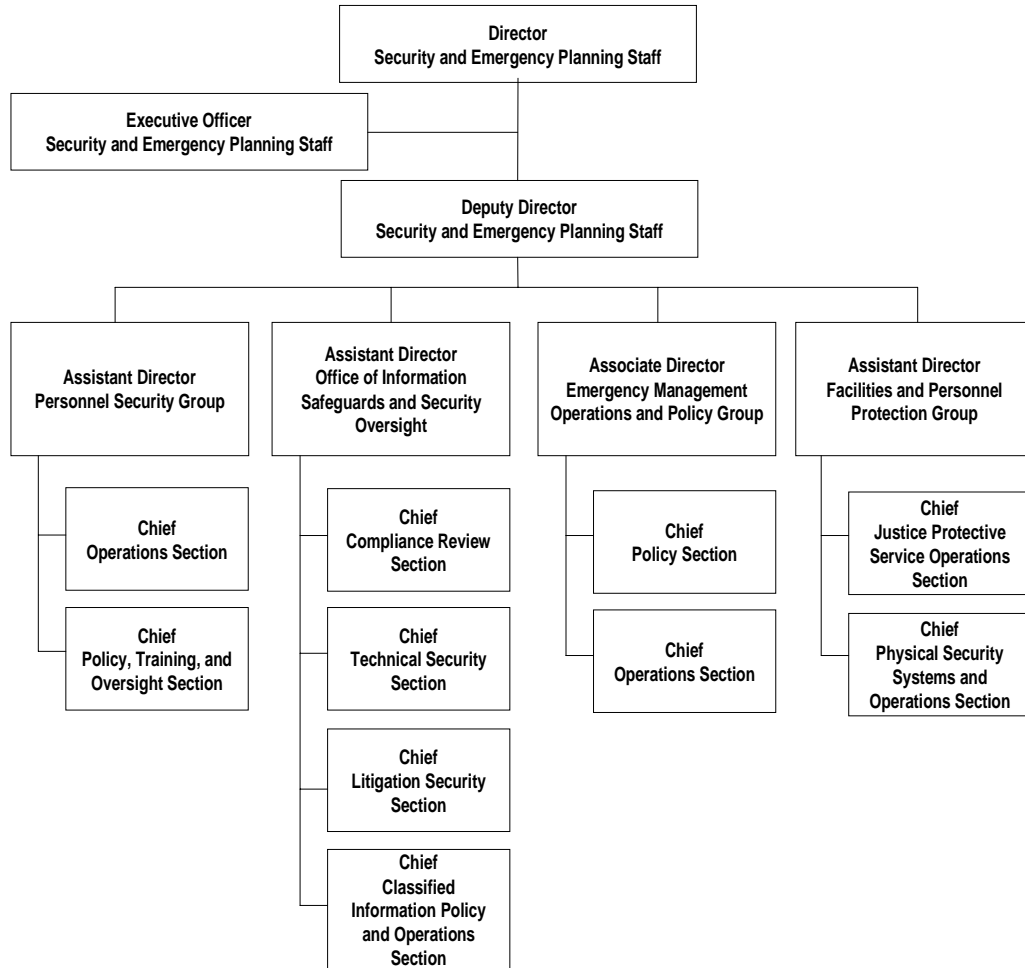
^a OPM conducts field investigations for all Department employees and contractors, except for political appointees, attorneys, and the specific categories of employees or contractors in the ATF, FBI, and USMS.

^b The FBI conducts field investigations for all of the Department's political appointees and attorneys, as well as for its own employees and contractors.

^c The ATF conducts field investigations for all its employees and contractors except political appointees and attorneys.

^d The USMS conducts background investigations of Court Security Officers and some contractors who are hired directly by USMS Districts.

APPENDIX II: SEPS's Organization



Source: SEPS

APPENDIX III: The Justice Management Division's Response



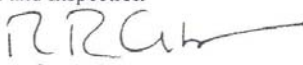
U.S. Department of Justice

Washington, D.C. 20530

SEP 09 2005

MEMORANDUM

TO: Paul A. Price
Assistant Inspector General
for Evaluation and Inspection

FROM: Paul R. Corts 
Assistant Attorney General
for Administration

SUBJECT: Response to DRAFT Inspector General Report on Review of
the Security and Emergency Planning Staff's Management
of Background Investigations

We have reviewed your draft report on the Security & Emergency Planning Staff's (SEPS) management of background investigations, and we have several comments.

Recommendation #1: Develop a Department-wide plan for implementing the personnel security requirements of the Intelligence Reform Act and HSPD-12, and identify the resources that will be needed to enable the Department to meet the new requirements.

JMD Response: We concur. The Department has an HSPD-12 plan that includes the personnel security requirements imposed by that Directive. The Department's final implementation plan was submitted to the Office of Management and Budget on August 27, 2005. With respect to the Intelligence Reform Act, SEPS will develop a plan by September 30, 2005 to implement the personnel security requirements of that statute for adjudicating background investigations.

Recommendation #2: Develop a Department-wide database with imaging capability to enable uniform processing and tracking of employee and contractor personnel security actions, permit central oversight of personnel security operations, and reduce the vulnerability caused by reliance on paper records.

JMD Response: We concur. A Department-wide database to track both employee and contractor personnel security actions is part of the HSPD-12 plan and budget. Although the database will not include imaging capability, record copies of all SEPS' background investigations are maintained separately by the investigating agencies. In addition, under the Office of Personnel Management's

(OPM) e-gov initiative, all investigative agencies will eventually move to electronic records of background investigations and a paperless environment for their customers.

Recommendation #3: Once OPM provides the necessary policy decisions, expeditiously issue an updated Department personnel security policy, DOJ Order 2610.2A.

JMD Response: We concur. By November 21, 2005, JMD will circulate a revised DOJ Order 2610.2A for comment by the components.

Recommendation #4: Develop a plan for conducting routine oversight of components with delegated authority that provides reasonable coverage and ensures that the background investigations and adjudications meet established standards for quality and timeliness.

JMD Response: We concur. Although authority to conduct background investigations is delegated by the Office of Personnel Management, we agree that SEPS should include in its compliance reviews oversight of the quality and timeliness of these investigations. Also, as your report notes, oversight of components with delegated adjudicative authority from SEPS is currently conducted by SEPS' Compliance Review Section during security compliance reviews. We are currently seeking three additional positions in the FY 07 budget for the Compliance Review Section to enhance its ability to conduct effective oversight. In the meantime, SEPS will develop a plan by September 30, 2005, to ensure that personnel security issues receive more attention during security compliance reviews.

Recommendation #5: Institute an annual report to the Deputy Attorney General to describe the performance of the Department and each component at adjudicating background investigations and complying with personnel security regulations and Department policy.

JMD Response: We concur. Following implementation of the enhanced oversight plan, the Assistant Attorney General for Administration will report annually to the Deputy Attorney General the performance of each component with delegated adjudicative authority in complying with the Department's adjudication regulations and policies.

Recommendation #6: Establish procedures to identify policies, documents, and other information that is necessary for personnel security operations and, in coordination with the Department's Office of the Chief Information Officer, make the documents available through the SEPS Web site.

JMD Response: We concur. SEPS is already implementing this recommendation.

We appreciate the opportunity to review the draft report. If you have any questions or require additional information, please contact James Dunlap on (202) 514-2094 or via email at James.L.Dunlap@doj.gov.

APPENDIX IV: THE OIG'S ANALYSIS OF JMD'S RESPONSE

On August 11, 2005, the Office of the Inspector General (OIG) sent copies of the draft report to the Assistant Attorney General for Administration with a request for written comments. The Assistant Attorney General for Administration provided the Justice Management Division's (JMD) final written comments to us in a memorandum dated September 9, 2005 (Appendix III).

JMD concurred with all six of our recommendations. However, we will require additional details regarding JMD's proposed plans to assess their effectiveness in meeting the intent of the recommendations. Our analysis of JMD's response to each recommendation follows.

RECOMMENDATIONS

Recommendation 1: Develop a Department-wide plan for implementing the personnel security requirements of the Intelligence Reform and Terrorism Prevention Act of 2004 (Intelligence Reform Act) and Homeland Security Presidential Directive 12 (HSPD-12), and identify the resources that will be needed to enable the Department to meet the new requirements.

Status: Resolved – Open

Summary of JMD's Response: JMD stated that the Department has an HSPD-12 plan that includes personnel security requirements imposed by that Directive. The Department's final implementation plan was submitted to the Office of Management and Budget on August 27, 2005. With respect to the Intelligence Reform Act, JMD stated that the Security and Emergency Planning Staff (SEPS) will develop a plan by September 30, 2005, to implement the personnel security requirements of that statute for adjudicating background investigations.

OIG's Analysis: To enable the OIG to assess these plans, please provide the OIG with copies of both implementation plans by October 3, 2005.

Recommendation 2: Develop a Department-wide database with imaging capability to enable uniform processing and tracking of employee and contractor personnel security actions, permit central

oversight of personnel security operations, and reduce the vulnerability caused by reliance on paper records.

Status: Resolved – Open

Summary of JMD’s Response: JMD stated that a Department-wide database to track both employee and contractor personnel security actions is part of the HSPD-12 plan and budget. The database will not include imaging capability, but JMD stated that copies of all of SEPS’s background investigations are maintained separately by the investigating agencies. JMD also stated that under the Office of Personnel Management’s (OPM) e-Gov initiative, all investigating agencies will eventually move to electronic records of background investigations and a paperless environment for their customers.

OIG’s Analysis: By January 13, 2006, please provide the OIG with a copy of the plan for a Department-wide database for tracking employee and contractor personnel security actions that meets OPM’s requirement for a paperless process and that addresses the interoperability, oversight, and continuity of operations requirements identified in our review. As the response indicates that the imaging capability may be distributed among investigative agencies, the plan should include JMD’s proposal to ensure that JMD and the components with delegated investigative authority develop and implement compatible systems that meet OPM requirements. The plan should confirm that the systems will also provide electronic storage capability for documents generated by components with adjudicative responsibility. The plan should include details on how these systems will interact to enable SEPS to conduct centralized oversight of the timeliness and quality of investigations and adjudications.

Recommendation 3: Once OPM provides the necessary policy decisions, expeditiously issue an updated Department personnel security policy, DOJ Order 2610.2A.

Status: Resolved – Open

Summary of JMD’s Response: JMD stated that by November 21, 2005, it will circulate a revised DOJ Order 2610.2A for comment by components.

OIG's Analysis: The action described by JMD is responsive to our recommendation. By January 13, 2006, please provide the revised DOJ Order 2610.2A. If the revision has not been completed, please provide a timeline for incorporating comments and issuing the updated Order.

Recommendation 4: Develop a plan for conducting routine oversight of components with delegated authority that provides reasonable coverage and ensures that the background investigations and adjudications meet established standards for both quality and timeliness.

Status: Resolved – Open

Summary of JMD's Response: JMD agreed that SEPS should include in its compliance reviews oversight of the quality and timeliness of those investigations. JMD also stated that, as our report notes, SEPS provides oversight of the components it has delegated adjudicative authority to through its Compliance Review Section's security compliance reviews. JMD is seeking three additional positions in the FY 2007 budget for the Compliance Review Section to enhance its ability to conduct effective oversight. In the meantime, JMD stated that SEPS will develop a plan by September 30, 2005, to ensure that personnel security issues receive more attention during security compliance reviews.

OIG's Analysis: Please provide the OIG with a copy of the plan for improving personnel security oversight by October 3, 2005. The plan should identify all additional elements that SEPS will introduce to ensure reasonable oversight of the quality and timeliness of the Department's background investigations. Additional staffing, if received, would increase SEPS's ability to conduct oversight. But even assuming the proposed doubling of SEPS's Compliance Review Section employees occurs, a six-member staff will be able to review only a limited portion of the Department's offices each year because these SEPS employees must address other security requirements as well. Therefore, the plan should identify any additional methods by which JMD can ensure personnel security issues receive sufficient attention.

Recommendation 5: Institute an annual report to the Deputy Attorney General to describe the performance of the Department and each component in adjudicating background investigations and in complying with Department personnel security regulations and policies.

Status: Resolved – Open

Summary of JMD's Response: JMD stated that following implementation of the enhanced oversight plan, the Assistant Attorney General for Administration will report annually to the Deputy Attorney General on the performance of each component with delegated authority in complying with the Department's adjudication regulations and policies.

OIG's Analysis: The action described by JMD is responsive to our recommendation. By January 13, 2006, please provide written procedures describing how SEPS will report to the Deputy Attorney General on components' compliance with all federal and Department regulations and policy for which it has oversight responsibility, including compliance with HSPD-12 and the Intelligence Reform Act requirements.

Recommendation 6: Establish procedures to identify the policies, documents, and other information necessary for personnel security operations, and in coordination with the Department's Office of the Chief Information Officer, make the documents available through the SEPS web site.

Status: Resolved – Open

Summary of JMD's Response: JMD stated that SEPS is implementing this recommendation.

OIG's Analysis: The action described by JMD is responsive to our recommendation. By January 13, 2006, please provide: (1) the date by which existing materials will be posted to the web site if such posting is not already complete and (2) written procedures for SEPS's coordination with the e-Gov staff within the Office of the Chief Information Officer to ensure that new materials are posted to the web site in a timely manner.