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

Review of the Department's Contractor Personnel Security Process

March 2013

I-2013-003

EXECUTIVE DIGEST

INTRODUCTION

The Office of the Inspector General (OIG) evaluated the time it took the Department of Justice (Department or DOJ) to complete the personnel security process for contractors, how well the Department meets the timeliness and reciprocity requirements of the *Intelligence Reform and Terrorism Prevention Act of 2004* (IRTPA) and other directives, whether certain positions take longer to process, and whether the Department ensures that only individuals with favorably adjudicated background checks have access to sensitive and National Security Information.[1]

Background investigations for the Department are conducted by one of three investigative agencies: the Office of Personnel Management (OPM), the Federal Bureau of Investigation (FBI), and the Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF).[2] Individuals in positions that require access to National Security Information (information classified at the Top Secret, Secret, or Confidential level) generally require more in-depth investigations than individuals whose positions do not require access to classified information (typically termed Public Trust positions).

IRTPA requires agencies that are authorized to grant National Security Information clearances to complete at least 90 percent of the clearances within an average of 60 days – 40 days to complete the background investigation and 20 days to complete the adjudication determination.

Background investigations and adjudications for Public Trust positions are not subject to the IRTPA guidelines. However, OPM requires that an agency both complete the adjudication process and report to OPM its determination within 90 days of receiving a completed background investigation.[3]

[1] Pub. L. No. 108-458, 118 Stat. 3638.

[2] Until October 2012, the U.S. Marshals Service conducted background investigations for one specific category of contractors, Court Security Officers.

[3] 5 C.F.R. § 732.302(b) and Executive Order 10450 (signed in 1953).

RESULTS IN BRIEF

While the Department generally completed personnel security reviews for Public Trust contractor positions in a timely manner, nearly 10 percent of adjudications exceeded OPM's 90-day timeliness requirement: Public Trust contractors accounted for 90 percent (3,434 of 3,797) of the contractor security cases the Department completed during our timeframe. Overall, the Department averaged 82 days to complete personnel security approvals for Public Trust cases. Further, the Department averaged 36 days to complete the adjudication phase of the process, falling well within OPM's 90-day requirement. However, nearly 10 percent (326 of 3,434) of Public Trust adjudications took more than 90 days to complete, the majority of which involved BOP contractors. Given that contractors generally receive a waiver to start work prior to the completion of the personnel security process, and given that they may work in close proximity to sensitive systems and information, the OIG is concerned that delays in the personnel security process for these individuals may present a security risk to the Department.

The Department failed to meet the 60-day IRTPA time guideline: The OIG found that from the first quarter of fiscal year (FY) 2010 through the first quarter of FY 2011, the Department as a whole did not meet the statutory timeliness guidelines for National Security Information clearances, primarily due to the length of time it took for the FBI to complete background investigations for its contractors. The FBI accounted for almost all (99 percent, or 359 of 363) of the Department's cases and averaged 108 days to complete National Security Information clearances for its contractors. The OIG found that the FBI's processing time was affected by the time taken to complete security clearances for contract linguists, who often have extensive foreign connections that must be assessed, slowing the investigative process. During the time period covered by this review, security clearances for FBI contract linguists took 67 days longer on average compared with other FBI contractors (166 days versus 99 days).

Components do not effectively track contractor personnel security information: During the time period covered by our review, procedures for tracking contractor personnel security information varied significantly throughout the Department, and some components did not maintain accurate personnel security information on their contractors. For example, in data ATF submitted to the OIG, 250 of 372 contractors were mistakenly listed as occupying National Security Information positions when in fact they should have been listed as occupying Public Trust positions.

There is no comprehensive Department-wide security policy for contractors: The Justice Management Division's Security and Emergency Planning Staff (SEPS) is responsible for issuing Department-wide security policies. However, SEPS has issued only minimal guidance for components to follow in managing their contractor security programs, and none of it is binding. Nor does the guidance provide standards for maintaining accurate rosters on contract employees or periodic reinvestigations. As a result, components frequently have to seek clarification from SEPS.

RECOMMENDATIONS

We make four recommendations in this report to improve the Department's management of its personnel security process for contractors. These recommendations include establishing procedures to identify Public Trust cases that have exceeded OPM's 90-day adjudication requirement and continuing to use OPM to conduct background investigations for Court Security Officers. We also recommend that SEPS require components to maintain rosters of their active contractors and that SEPS issue a Department-wide contractor security policy.

TABLE OF CONTENTS

BACKGROUND

The Office of the Inspector General (OIG) conducted a two-part review to assess whether the Department of Justice (Department or DOJ) is effectively administering the personnel security process for government employees and contractors to meet component mission and security requirements. The first report focused on the process for employees, while this second report addresses the process for contractors.[4]

In both parts of the review, we evaluated how the Department was meeting the requirements of the *Intelligence Reform and Terrorism Prevention Act of 2004* (IRTPA) and related executive branch directives.[5] IRTPA requires agencies that are authorized to grant National Security Information clearances to complete at least 90 percent of the clearances within an average of 60 days.[6] During the time period covered by this review, agencies were to take no more than 40 days to complete the investigative phase and no more than 20 days to complete the adjudicative phase of a clearance.[7]

In addition, IRTPA's reciprocity provision mandates that agencies accept a background investigation completed by any other authorized federal investigative or adjudicative agency, provided that the clearance is

[4] See U.S. Department of Justice Office of the Inspector General, *The Department's and Components' Personnel Security Process,* Evaluation and Inspections Report I-2012-003 (September 2012). See Appendix II for prior OIG reports finding that certain Department components did not have effective personnel security processes.

[5] Pub. L. No. 108-458, 118 Stat. 3638. Prior to IRTPA, Executive Order 12968 (signed in 1995) called for a uniform federal personnel security program for individuals being considered for access to classified information, established policies for protecting classified information, and detailed individual access levels and reciprocity procedures among federal agencies.

[6] The OIG used the IRTPA guideline to measure the Department's performance because, although IRTPA does not establish a specific deadline for completing individual cases, it does establish a general guideline for completing cases within average time periods that is accepted government-wide. Further, both the Office of Personnel Management and the Office of the Director of National Intelligence use the fastest 90 percent of National Security Information cases in measuring agencies' performance against the IRTPA time guidelines.

[7] On October 1, 2012, the Director of National Intelligence signed an order lengthening the time to complete investigations for certain, more complex investigation levels from 40 to 80 days. The adjudication goal remained at 20 days. However, this report will use the standards as they existed during the time period covered by this review.

not temporary or interim and the background investigation was favorably adjudicated, was at the appropriate security clearance level for the position, and was completed within the past 5 years.[8]

National Security Information and Public Trust Positions

Individuals in positions that require access to classified information are granted National Security Information clearances at the Top Secret, Secret, or Confidential level. The higher the clearance level, the more in depth the background investigation must be. IRTPA provides guidelines that these clearances must meet.

Individuals who do not require access to classified information but who may be involved in policy making, major program responsibility, or other sensitive roles are typically considered to be in Public Trust positions. Public Trust positions are assigned a risk level of High, Moderate, or Low based on the potential harm actions of individuals in those positions could cause the federal government.

Background investigations and adjudications for Public Trust positions are not subject to the IRTPA guidelines. There is, however, a requirement that agencies must both complete the adjudication and report the determination to the Office of Personnel Management (OPM) within 90 days of receiving a completed investigation.[9] Additionally, agencies must apply reciprocity for Public Trust cases and cannot make a new determination for a person who has already been determined suitable.[10]

Appendix III details the types of National Security Information clearances and Public Trust risk levels and the background investigation required for each position.

Personnel Security Process

Each component has a Security Programs Manager who determines the appropriate risk level for each contractor position, certifies that the requirements for granting security clearances are adequate, and monitors

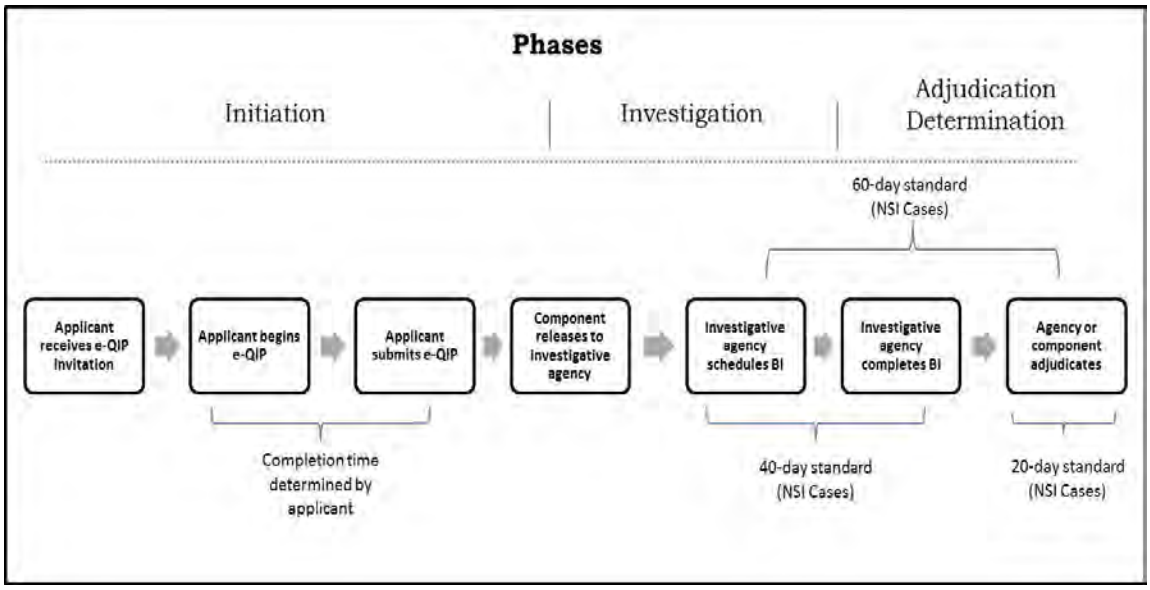
[8] Executive Orders 12968 and 13381 (signed in 2005) also include the requirement for reciprocity.

[9] 5 C.F.R. § 732.302(b) and Executive Order 10450 (signed in 1953).

[10] Executive Order 13488 (signed in 2009) and Executive Order 13467 (signed in 2008).

compliance.[11] Although the process can vary, Figure 1 depicts the typical personnel security process.

Figure 1: Personnel Security Process



Abbreviations: BI = Background Investigation; e-QIP = Electronic Questionnaires for Investigations Processing system.

Source: OIG.

To initiate the personnel security process, individuals must provide background information related to their family members, residence, education, employment, finances, and criminal history. Since 2005, individuals have typically entered the information online using OPM's Electronic Questionnaires for Investigations Processing (e-QIP) system. Once the component requesting the investigation verifies the information is complete, the information is sent to the agency responsible for conducting the investigation. The investigative agency conducts the investigation, which consists of verifying residence, education, employment, financial state, and criminal history. Investigators generally interview the individual, as well as family members, neighbors, and personal acquaintances.

The results of the investigation, which usually include a summary of any interviews and database checks, are sent to the adjudicating authority. The adjudication process examines more than a dozen variables over a sufficient period of a person's life to determine whether the person is eligible for access to classified information or to serve in a Public

[11] Justice Acquisition Regulations 2804.470-2.

Trust position. Information about a person's past and present, favorable and unfavorable, is used to make determination decisions.

Authorities to Conduct Background Investigations and Adjudications

Within the Department, background investigations for contractors in National Security Information or Public Trust positions are conducted by one of three authorized investigative entities.[12] The Federal Bureau of Investigation (FBI) and the Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF) are authorized to conduct investigations of their Public Trust contractors and certain categories of contractors in National Security Information positions. An external agency, OPM, conducts the background investigations for all other components of the Department.[13] Although the investigative entities' processes differ slightly, as discussed below, all background investigations must meet the same government-wide minimum standards.[14]

For adjudications, OPM authorized the Justice Management Division's (JMD) Security and Emergency Planning Staff (SEPS) to make determinations for National Security Information and Public Trust positions.[15] For contractors, SEPS further delegated adjudication authority to 21 of the Department's components, including ATF, the Federal Bureau of Prisons (BOP), the Drug Enforcement Administration (DEA), the FBI, and the U.S. Marshals Service (USMS). Appendix IV lists all of the components with delegated authority over their contractors.

[12] Contractors who require access to National Security Information frequently work under commercial contracts and have clearances granted by the Department of Defense's Defense Industrial Security Clearance Office (DISCO). The Department accepts these individuals' clearances under reciprocity. Because the Department is not responsible for the timeliness of clearances completed by DISCO, we did not include these contractors in our analysis. Contractors having an employer-employee relationship with the government are not cleared through DISCO. The Department manages the clearance process for these individuals. For the purposes of this review, we examined only this latter group of contractors.

[13] The U.S. Marshals Service conducted background investigations for one specific category of contractors, Court Security Officers. We discuss this further in Chapter I of this report.

[14] Executive Order 12968 and Executive Order 13467.

[15] 28 C.F.R. § 17.11(c) and Executive Order 12968 give the Department the authority to grant, suspend, and revoke security clearances and to delegate its authority to the components. In 5 C.F.R. § 731, OPM delegated to agencies the authority to adjudicate Public Trust positions.

DOJ Personnel Security Process

SEPS is the primary office responsible for establishing Department-wide personnel security policy and for providing oversight of the Department's personnel security clearance process.

SEPS also manages the Justice Security Tracking and Adjudication Record System (JSTARS), a web-based personnel security processing application that tracks all elements of the Department's personnel security process for employees and contractors, such as background investigations, adjudications, reinvestigations, clearance levels, pre-employment waivers, reciprocity actions, and clearance certifications. As of December 2012, all components had moved their data to JSTARS. Although the FBI reports its personnel security data to JSTARS for Department-wide tracking purposes, it continues to use its internal systems to track personnel security data as well.

The following sections describe the three primary personnel security processes used within the Department.

Background Investigations Completed by the FBI

The FBI conducts the background investigations and makes the adjudication determinations for some of its own contractors. Some FBI applicants, such as contract linguists, must also pass polygraph examinations. In addition, certain positions may require the applicant to pass a physical or medical examination. All FBI contractors are cleared at the Top Secret or Secret level; there are no Public Trust positions in the FBI. The FBI may use either contract investigators or its own special agents to conduct the background investigations.

Background Investigations Completed by ATF

ATF conducts the background investigations and makes the adjudication determinations for its Public Trust contractors and some contractors in National Security Information positions. Most ATF investigations are conducted by contract investigators. However, ATF does sometimes use OPM to conduct lower-level background investigations that do not require field work.

Background Investigations Completed by OPM

Many Department components, including JMD and the OIG, rely on OPM to conduct background investigations. OPM uses contractors to conduct investigations. When an investigation is completed, OPM releases the information to the appropriate agency for adjudication.

PURPOSE, SCOPE, AND METHODOLOGY OF THE OIG REVIEW

The purpose of the second phase of the OIG's review is to assess whether the Department is effectively administering the personnel security process for contractors to meet component mission and security requirements. This phase of the review focused on the time it takes to complete background investigations and adjudications for contractors, the Department's success in meeting IRTPA's timeliness guidelines, whether certain positions take longer to process than others, whether the Department provides sufficient oversight of components' contractor personnel security process, and whether the Department ensures that only individuals with the necessary security approvals have access to sensitive and National Security Information.[16]

This review examined the Department's timeliness for the end-to-end process, regardless of whether the investigative agency was part of the Department (the FBI and ATF) or outside the Department (OPM).

We analyzed data from all the Department's components. Among those we reviewed were ATF, the Antitrust Division, the BOP, the Civil Division, the Civil Rights Division, Community Oriented Policing Services, the Community Relations Service, the Criminal Division, the DEA, the Environment and Natural Resources Division, the Executive Office for United States Attorneys (EOUSA), the FBI, JMD, the Office of Justice Programs (OJP), and the USMS. Our review included interviews, data analysis, document reviews, and site visits.

The review covered the period from fiscal year (FY) 2010 through the first quarter of FY 2011 (October 1, 2009, through December 31, 2010). We conducted our fieldwork from March 2011 through July 2011.

Interviews

We interviewed officials and staff members at the various components' headquarters and field offices. We also interviewed Government Accountability Office personnel to discuss its previous reviews as well as OPM personnel regarding investigation and clearance procedures.

[16] We could not evaluate whether the Department and its components were meeting the reciprocity requirements of IRTPA or whether clearances for specific positions took longer to process because information needed for such analyses was not consistently captured across the Department. The one exception was clearances for FBI contract linguists, addressed in Chapter II of this report.

Data Analyses and Document Reviews

We analyzed component data on security and personnel information from FY 2010 through the first quarter of FY 2011 (October 1, 2009, through December 31, 2010). We chose this period based on when agencies were required to start meeting the IRTPA guideline of completing 90 percent of clearances within an average of 60 days.[17] The data included when the background investigation was initiated, when the background investigation was completed, when the adjudication determination was made, the risk or sensitivity level, and the job position. We also reviewed relevant laws, regulations, policies, procedures, internal reviews, and a sampling of security files for completed background investigations. See Appendix V for a detailed description of the OIG's methodology used for each analysis.

Site Visits

We conducted 13 site visits to ATF and FBI field offices, USMS and United States Attorneys' Offices' (USAO) district offices, DEA division offices, and BOP confinement facilities in Los Angeles and Atlanta. We also visited JMD and each law enforcement component's headquarters, as well as the Civil Division, the Civil Rights Division, the Criminal Division, and EOUSA.

[17] On October 1, 2012, the Director of National Intelligence changed the timeliness standard for completing single scope background investigations from 40 to 80 days. Single scope background investigations are more complex and are generally completed for individuals receiving access to Top Secret information. However, because this change did not apply to cases completed during the time period covered by our review, we used the 40-day investigation standard.

RESULTS OF THE REVIEW

CHAPTER I: PUBLIC TRUST POSITIONS

The Department averaged 82 days to complete background investigations and adjudication determinations for Public Trust contractor positions. However, OPM's 90-day timeliness requirement was exceeded in nearly 10 percent of adjudications, the majority of which involved BOP contractors. One component, the USMS, used its own personnel to conduct background investigations for certain Public Trust contractor positions. These investigations took longer to complete on average than investigations completed by OPM or ATF, and diverted the USMS's personnel from other tasks.

The background investigation and adjudication process for Public Trust positions averaged 82 days to complete, but nearly 10 percent of adjudications exceeded OPM's 90-day timeliness requirement.

Public Trust cases accounted for 90 percent (3,434 of 3,797) of the Department's contractor job positions reviewed for this analysis. Overall, the personnel security process for Public Trust cases took an average of 82 days to complete. The background investigation phase took an average of 46 days and the adjudication phase took an average of 36 days.[18] However, nearly 10 percent (326 of 3,434) of adjudications exceeded OPM's 90-day timeliness requirement. The majority (221 of 326) of these cases were completed at the BOP.[19]

Individuals in Public Trust positions generally start work under a waiver while the background investigation and adjudication phases of the personnel security process are being completed. During the OIG's earlier review of the security clearance process for Department employees, we found that employees in Public Trust positions who started work under a waiver routinely had access to sensitive information and systems for significant periods of time before their background investigation or

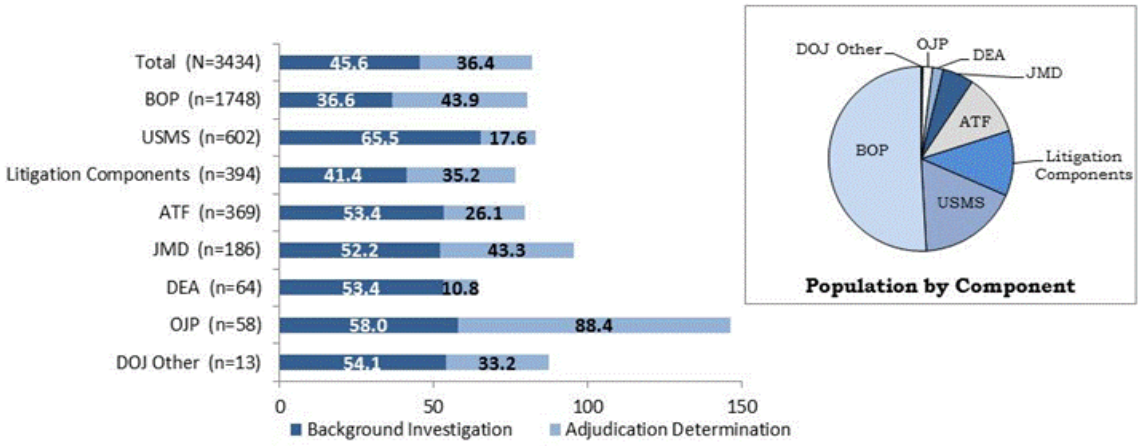
[18] The majority of these investigations were completed by OPM. However, ATF and the USMS did conduct investigations for some of their Public Trust contractors.

[19] These cases represented 13 percent (221 of 1,748) of the total Public Trust cases the BOP completed during our review's time period.

adjudication was completed. In response to this finding, SEPS implemented procedures to identify and adjudicate lengthy employee cases.[20] The OIG believes that the Department would benefit from a similar process for identifying contractor cases that have been pending for a significant period of time and have exceeded OPM's 90-day adjudication requirement.

One component, the Office of Justice Programs (OJP), took much longer than the Department's average to complete personnel security approvals for its Public Trust contractors. As a result, 58 OJP contractors worked in the Department for an average of 146 days without completed adjudication determinations (Figure 2).

Figure 2: Timeliness of Completed Public Trust Cases, October 1, 2009, through December 31, 2010



Note: "DOJ Other" consists of Community Oriented Policing Services (eight cases), the Community Relations Service (one case), the OIG (three cases), and the United States Parole Commission (one case).

Source: OIG analysis.

Although the Department as a whole took an average of 36 days to adjudicate Public Trust cases, OJP took an average of 88 days to adjudicate its cases. In addition, OJP exceeded OPM's 90-day adjudication requirement for more than 63 percent (37 of 58) of its cases. By comparison, the DEA completed a similar number of cases (64) and took only an average of 11 days to complete adjudications.

[20] The BOP also issued a memorandum on November 28, 2012, formalizing its procedures for ensuring that Public Trust background investigations for both employees and contractors are adjudicated within 90 days of the investigation completed date.

Security Specialists at OJP told the OIG that during the time period covered by our review they experienced staffing shortages that contributed to delays in their adjudication process. OJP told the OIG that, starting in June 2010, OJP took corrective measures to hire and train additional staff. OJP told the OIG that it also reorganized staff responsibilities during the first quarter of 2011 to better manage its workload of contractor adjudications.[21]

USMS background investigations of certain Public Trust contractor positions took longer to complete and diverted USMS personnel from other mission-critical tasks.

During the time period covered by this review, the USMS used its own personnel to conduct background investigations for one category of Public Trust contractors, Court Security Officers (CSO). We found that these background investigations took longer to complete on average than investigations completed by OPM or ATF and diverted the USMS's personnel from other mission-critical tasks.

The USMS's Background Investigations

Most DOJ components use OPM's investigative service or, in the case of ATF, contract field investigators, to conduct background investigations for contractors in Public Trust positions.[22] However, during the time period covered by our review, the USMS used Deputy U.S. Marshals in the local districts to perform background investigations for contractors hired as CSOs.[23] CSOs are Public Trust contractors and perform security duties at federal judiciary facilities for the judicial branch's Administrative Office of the U.S. Courts (AOUSC). The USMS's Office of Court Security, under the Judicial Security Division, administers the CSO program on AOUSC's behalf. This includes overseeing the CSO contracts and screening, training, and managing the CSOs. The Judicial Security Division is funded exclusively by the AOUSC, including the cost of conducting background investigations for the CSOs. The USMS allots $900,000 of its Judicial Security Division budget for CSO investigations each year.

[21] Given the time period under review, the OIG was not able to determine if OJP's timeliness in completing adjudications improved as a result of these measures.

[22] The FBI does not have any Public Trust contractors.

[23] For all contractors in Public Trust positions other than the CSOs, the USMS used OPM's investigative service to conduct background investigations.

CSOs received a background investigation comparable to a 5-year scope background investigation.[24] The OIG compared the time it took the USMS, OPM, and ATF to complete 5-year scope background investigations. We found that the USMS took 9 days longer on average to complete investigations of CSOs than OPM did to complete similar investigations of other Public Trust contractors in the Department and 22 days longer on average than ATF (Table 1).

Table 1: Five-Year Scope Background Investigations of Public Trust Cases, October 1, 2009, through December 31, 2010

Investigating Agency	Mean Days	Number of Cases
ATF	57.3	54
OPM	70.0	22
USMS (CSOs)	79.4	336
All	**76.0**	**412**

Source: OIG analysis.

The USMS's personnel security process was slower, in part, because CSO applicants must pass the USMS's medical screening requirements before the agency's adjudicators can make a favorable determination. USMS officials told the OIG that because CSO applicants are often retired law enforcement officers and are generally older than other Department contractors, they are more likely to have medical issues that can cause delays in the personnel security process.[25] The OIG reviewed a sample of six CSO case files and found that the medical screening process affected the length of the personnel security process in four of the six cases, with the time to complete the medical screening ranging from a little over 3 months to more than 9 months. These case files were generally consistent with the USMS's explanation that medical screening requirements accounted for at least some of the delays in its background investigations.

Also contributing to the slower investigations was the USMS's use of Deputy Marshals in the local districts, to whom CSO investigations were assigned as a collateral duty. Unlike the contract field investigators used to conduct background investigations for ATF, USMS Deputy Marshals are

[24] A 5-year scope background investigation covers the past 5 years of a subject's activities and includes verification of citizenship and date and place of birth, as well as national agency records checks on the subject's spouse or cohabitant, interviews with selected references, and former spouses.

[25] According to USMS officials, the average age of a CSO is 61.

criminal investigators and are required to balance their operational duties with the CSO background investigations. This situation contributed to the length of time it took the USMS to complete CSO investigations, and it directly affected the Deputy Marshals' ability to focus on their other mission-critical tasks.

USMS's Management of the CSO Program

Unlike ATF, the USMS did not have specific guidelines or written procedures on how to conduct CSO investigations. ATF has developed a Special Investigator Manual that is used to ensure that ATF contract field agents follow the same process and conduct background investigations in accordance with OPM requirements. This includes instructions on the type of sources that should be included in an investigation and standard protocols for conducting interviews. In contrast, the USMS did not provide its Deputy Marshals with any detailed written guidelines for conducting CSO investigations. USMS security personnel told the OIG that they believed the standardized forms Deputy Marshals filled out during the course of a CSO investigation were "self-explanatory." However, the USMS's forms do not explain what constitutes derogatory information and contain only general interview requirements. Without clear guidelines, we were unable to determine if all Deputy Marshals followed the same investigative standards or if CSO investigations were consistent with OPM requirements. USMS officials also told the OIG that CSO investigations were not aligned with DOJ agency processes and, consequently, would not be accepted by other agencies under federal reciprocity requirements.[26]

In addition to lacking standard investigation procedures, the USMS was not able to measure the costs of its CSO investigations accurately. Deputy Marshals are required to document the time they spend on CSO investigations using a project code that the USMS then uses to reimburse itself from the AOUSC budget allotment. Despite this requirement, the USMS was not able to determine an average or per-unit cost for its investigations. Initially, the USMS told the OIG that it cost $3,189 to conduct a CSO investigation. However, USMS managers subsequently told the OIG that this number was not based on the actual cost of a CSO investigation, but rather was the amount OPM charges to conduct a background investigation at the same level.

During the course of the OIG's review, the USMS conducted its own internal evaluation to determine the most effective method for conducting

[26] We did not independently verify these statements, as the issues of whether CSO investigations were aligned with DOJ or OPM standards and whether they meet reciprocity requirements were outside the scope of the review.

CSO background investigations. The USMS concluded that it should begin using OPM to conduct all CSO background investigations starting in FY 2013.[27] The USMS also determined that, under OPM's guidelines, CSOs required only an investigation at the minimum background investigation (MBI) level as opposed to the 5-year scope background investigations the USMS had been conducting.[28] The primary difference between the 5-year scope background investigation and the MBI is the number of interviews that are required. The USMS found that since 2010 less than 3 percent (35 of 1,184) of CSO applicants were denied based on information gleaned from interviews and, consequently, USMS managers did not believe conducting an MBI would result in an unacceptably greater risk.[29] Since OPM charges $752 for an MBI versus $3,189 for a BI, USMS managers believed using OPM and switching to an MBI-level investigation would not only meet the agency's investigative needs, but would also result in future cost savings. USMS officials estimate that this revised process would reduce the annual CSO investigation budget of $900,000 by $120,000 a year for the first 5 years and then by $360,000 a year after that.

In addition to the potential cost savings, the USMS determined that using OPM to conduct investigations would free Deputy Marshals to focus on other mission-critical tasks, improve the consistency of investigations, and reduce the USMS's processing times. As a result of these findings, the USMS began using OPM to conduct CSO investigations in October 2012.

Conclusions and Recommendations

Overall, the Department averaged 82 days to complete personnel security approvals for Public Trust contractor cases. The Department averaged 36 days to complete the adjudication phase of the process, which is well within OPM's 90-day requirement. However, nearly 10 percent of Public Trust adjudications exceeded the OPM requirement, the majority of which involved BOP contractors. Given that these individuals may work in

[27] OPM contract investigators will conduct the background investigations, and AOUSC will reimburse the USMS for the cost. The transition to using OPM will phase in over 5 years, since all current CSOs will need to be processed through OPM's e-QIP system when they are due for a reinvestigation. All new applicants for CSO positions will be processed through e-QIP.

[28] An MBI consists of a personal subject interview and written inquiries covering a subject's employment, education, credit, and residence.

[29] The OIG did not attempt to assess the sufficiency of an MBI-level background investigation for CSOs. Accordingly, we do not have a basis for evaluating whether using the MBI results in an unacceptably greater level of risk.

close proximity to sensitive systems and information, the OIG is concerned that delays in the security process may present a security risk to the Department.

The USMS's investigations of CSOs took longer to complete, on average, than investigations completed by OPM or ATF. Further, because these investigations were completed by Deputy Marshals rather than contract field investigators, the time spent on CSO investigations directly affected the Deputy Marshals' ability to work on other mission-critical tasks. The OIG also found that, although standardized forms were in use, the USMS did not have standardized procedures for its CSO investigations. In October 2012, the USMS began using OPM to conduct CSO investigations at the MBI-level, which the USMS believes will result in improved consistency and potential cost savings.

To improve components' timeliness in completing Public Trust cases and to ensure that USMS resources are efficiently deployed for mission-critical operations, we recommend that:

1. SEPS implement procedures to identify contractor cases that are pending for a significant period of time and have exceeded OPM's 90-day adjudication requirement; and

2. The USMS continue to use OPM's investigative services to complete background investigations for its CSOs.

CHAPTER II: NATIONAL SECURITY INFORMATION POSITIONS

The Department did not complete at least 90 percent of the National Security Information clearances for contractors within the 60-day IRTPA time guideline, primarily because of the time taken by the FBI to complete background investigations for its contractors.

As a whole, the Department averaged 107 days to complete security clearances for National Security Information contractor positions.[30] However, National Security Information positions represent a small minority (10 percent, or 363 of 3,797) of the Department's contractor cases completed during this review.

FBI National Security Cases

The FBI accounted for almost all (99 percent, or 359 of 363) of the Department's cases and averaged 108 days to process National Security Information clearances for its contractors. Of these cases, 86 percent (307 of 359) exceeded the 60-day IRTPA timeliness guideline. The FBI took an average of 93 days to complete the background investigation phase of the process, exceeding the 40-day IRTPA guideline, but only took an average of 15 days to complete adjudications, which was well below the 20-day IRTPA guideline.

The time the FBI took to complete background investigations for its contractors steadily increased from 60 days in the first quarter of FY 2010 to 116 days in the first quarter of FY 2011. During this time, the FBI also experienced a significant increase in the number of National Security Information cases that it completed, from 9 cases in the first quarter of FY 2010 to 97 cases in the first quarter of FY 2011.

Factors Affecting Timeliness

Department human resources and security personnel told the OIG that security clearance approvals for contractors with a large number of

[30] The numbers in this chapter represent the overall averages for the fastest 90 percent of cases for the entire Department, rather than the average of 100 percent of the total investigations completed. The OIG selected the fastest 90 percent of the cases because this is the methodology OPM and the Office of the Director of National Intelligence use in measuring agencies' performance against the IRTPA time guidelines. Further, these numbers do not include contractors working under a commercial contract who received clearances through DISCO.

foreign connections or extensive overseas travel usually take longer to complete because investigators may have to conduct additional work to contact references and verify information overseas. If the contractor has connections to particular countries that may pose a higher risk, the hiring component may conduct an additional analysis to ensure the individual does not pose a risk to national security.

Human resources and security staff stated that contract linguists in particular are more likely to have connections to these countries. During the time period covered by our review, contract linguists accounted for only 13 percent (46 of 359) of the FBI's National Security Information cases. However, the time taken to complete their security clearances had a disproportionate effect on the FBI's overall processing times, adding nearly 9 days to the FBI's average. Security clearances for FBI contract linguists took, on average, 67 days longer to complete than security clearances for other FBI contractors (166 days versus 99 days). The OIG reviewed the five longest contract linguist cases and found that each of these cases involved subjects who had significant foreign connections and overseas travel that required the FBI had to conduct additional checks, contributing to the length of the security process for these individuals.

Non-FBI National Security Information Cases

The remaining four National Security Information cases took an overall average of 66 days to complete. Of these, three cases belonged to ATF and one to the USMS. ATF averaged 47 days to complete the background investigations for its 3 cases and 15 days to complete the adjudication. The background investigation for the USMS case, which was completed by OPM, took 59 days, and the adjudication took 11 days.

Conclusions

The Department as a whole is not meeting the overall IRTPA time guideline of 60 days when completing security clearances for contractors in National Security Information positions, primarily because of the time taken by the FBI to complete background investigations for its own contractors. The FBI accounted for almost all (99 percent) of the Department's cases and averaged 108 days to complete National Security Information clearances for its contractors. One factor that contributes to the FBI's lengthy processing times is the time taken to complete security clearances for contract linguists, which took, on average, 67 days longer than security clearances for other FBI contractors.

CHAPTER III: PROGRAM MANAGEMENT AND TRACKING

Components could not ensure that contractors have the required personnel security approval because personnel security data for contractors is not consistently tracked and managed across the Department. No comprehensive Department-wide contractor security policy exists, and what guidance does exist is outdated and inconsistent.

Personnel security data for contractors is not consistently tracked and managed across the Department.

Because personnel security data for contractors is not consistently tracked and managed across the Department, components cannot always ensure that contractors have the appropriate clearance or sensitivity level for their positions.

During the time period covered by our review, procedures for tracking contractor personnel security information varied significantly throughout the Department. No single data source existed for tracking contractor personnel security information, and the various components often kept information in multiple systems or, at times, in paper files.

Maintaining separate collections of data resulted in components having conflicting or incomplete personnel security information for the contractors they employed, and in some cases components were not able to identify all of the individuals working for them. We found four specific instances of this at three different components:

- Security personnel in one USMS field office stated that they have had problems with USMS headquarters losing copies of contractor security files. In one specific instance, the field office had to send the same files three times within a 9-month period. USMS headquarters told the field office that the issue was due to staff changes at headquarters.

- Security personnel working in the Office of Security Programs at USMS headquarters stated that they had found instances where contractors were not in the USMS's tracking system. These contractors had completed adjudications and were working in USMS facilities, but there was no record of the contractors at USMS headquarters.

- In data ATF submitted to the OIG, 250 of 372 contractors were mistakenly listed in a human resources database as occupying National Security Information positions when in fact they should have been listed as occupying Public Trust positions. ATF's Personnel Security Group discovered the error in August 2011 when ATF deployed the DOJ-wide system, JSTARS, to help it track and manage information on its contractors. ATF was not able to determine when the issue first began or the total number of cases affected, but these 250 individuals had worked in the Department for up to 15 months before ATF identified the error. ATF officials told the OIG that none of the 250 contractors would have been allowed to access National Security Information because this error was limited to a human resources database that ATF did not use to verify clearances for contractor personnel.[31]

- Security staff at EOUSA discovered that they did not have a complete list of all the contractors with access to EOUSA space and information systems. This issue was discovered when EOUSA was preparing its data for JSTARS and caused delays in the JSTARS deployment process.

As of December 2012, all components had moved their data to JSTARS. Using JSTARS should improve components' ability to track and manage information on their contractors and reduce the potential for inaccurate or inconsistent personnel security data. However, using JSTARS will not address many of the tracking issues identified in this review, and vulnerabilities still remain in how components administer their contractor personnel security processes. For instance, SEPS officials told the OIG that components continue to identify additional contractors that components were not aware of and that were not reported to JSTARS. Addressing these issues and other issues identified in this review will require components to take actions in addition to the deployment of JSTARS.

There is no comprehensive Department-wide contractor security policy, and what guidance does exist is outdated and inconsistent.

Providing Department-wide policy is a fundamental part of SEPS's responsibilities. However, there is currently no Department-wide security policy for contractors. Since 1998, SEPS has issued seven memoranda specific to the personnel security process for contractors. These memoranda provide general information on how to assign risk levels to

[31] After discovering the issue with the human resources database, ATF security officials told us that they implemented additional measures to ensure that contractor security and clearance information is reported correctly in that system.

contractors and conduct background checks for contractors who require escorted or unescorted access to DOJ facilities, but do not provide any comprehensive or binding policy for components to follow in managing their contractor security programs. Further, SEPS has not issued any Department-wide contractor policy in response to critical changes in the security environment regarding uniform standards in background investigations, policies for access to classified information, and reciprocity.[32]

The Department's Employee Security Order requires that both its National Security Information and Public Trust employees be reinvestigated every 5 years. However, the Department has not issued a policy with a similar requirement for Public Trust contractors.[33] This issue was previously identified in a 2005 OIG report.[34] At the time, SEPS officials stated that a reinvestigation policy for contractors was necessary to ensure the Department's security and that SEPS was taking steps to draft a reinvestigation policy for contractors. However, a policy was never issued.

SEPS officials told the OIG that, because there is no comprehensive Department-wide contractor security order, components frequently come to them for clarification on contractor issues and to ask when a Department-wide security order will be released. Similarly, security officials at ATF told the OIG that a single, Department-wide contractor security order would help them ensure they are following consistent standards. In the past, they have had to ask SEPS for guidance on the Department's reinvestigation requirements and on how to categorize certain contractors.

During our current review, SEPS officials stated that they have been working on drafting a comprehensive contractor policy since 2002, but issuing this document has not been a priority because they have been

[32] Examples of such changes include Executive Order 13467 and IRTPA, which mandate the use of consistent guidelines in background investigations and adjudication determinations across the federal government. Along with Executive Orders 12968 and 13381, they also establish government-wide standards regarding reciprocity.

[33] Contractors in National Security Information positions are subject to the reinvestigation requirements of IRTPA and must receive a reinvestigation at least every 5, 10, or 15 years, depending on their investigation level. OPM is in the process of implementing new reinvestigation standards that will require contractors in Public Trust positions to receive a reinvestigation every 5 years. However, as of January 23, 2013, these new standards were not yet in effect.

[34] *Review of the Security and Emergency Planning Staff's Management of Background Investigations,* Evaluation and Inspections Report I-2005-010 (September 2005).

focused on implementing policies such as IRTPA. Further, because Department security policies are constantly evolving, SEPS officials stated that they have struggled to develop a comprehensive policy for contractors. In January 2011, SEPS provided the OIG with a draft Department-wide contractor security policy that was being circulated for review by the components.[35] The OIG believes this policy should play a critical role in ensuring components follow consistent standards in managing their contractor security programs.

Conclusions and Recommendations

During the time period covered by our review, procedures for tracking contractor personnel security information varied significantly throughout the Department. There was no single data source for tracking contractor personnel security information, and the various components kept information in multiple systems or, at times, in paper files. As a result, some components did not maintain accurate security information on their contractors. For example, in data ATF submitted to the OIG, 250 of 372 contractors were mistakenly listed as occupying National Security Information positions when in fact they should have been listed as occupying Public Trust positions. The USMS and EOUSA also had issues with maintaining accurate information on their active contractors.

There is currently no comprehensive Department-wide security policy for contractors. SEPS has issued only minimal guidance that serves as a reference for components but does not provide any binding policy for components to follow in managing their contractor security programs. The issued guidance also does not provide standards regarding contractor tracking or reinvestigations. As a result, components frequently have to seek clarification and informal guidance from SEPS.

To ensure that personnel security data for contractors is consistently tracked and managed across the Department, we recommend that:

3. SEPS require components to maintain rosters of their active contractors, including information on each contractor's clearance or risk level; and

4. SEPS issue a contractor security policy similar to the Department's employee security policy, including a contractor reinvestigation requirement that is consistent with the Department's employee reinvestigation requirement.

[35] SEPS officials told the OIG they plan to issue this policy by spring 2013.

CONCLUSION AND RECOMMENDATIONS

Public Trust cases accounted for 90 percent (3,434 of 3,797) of the Department's contractor cases. Overall, the Department averaged 82 days to complete personnel security approvals for Public Trust cases. The Department averaged 36 days to complete the adjudication phase of the process, which was well within OPM's 90-day requirement. However, nearly 10 percent of Public Trust adjudications exceeded the OPM requirement, the majority of which involved BOP contractors. Given that these individuals may work in close proximity to sensitive systems and information, the OIG is concerned that delays in the personnel security process may present a security risk to the Department.

One component, the USMS, used its own personnel to conduct background investigations for CSOs during the OIG's review period. These investigations took longer to complete on average than investigations completed by OPM or ATF and diverted the USMS's resources from other mission-critical tasks. The OIG also found that, although standardized forms were in use, the USMS did not have standardized procedures for its CSO investigations. In October 2012, the USMS began using OPM to conduct CSO investigations at the MBI level.

The Department as a whole did not meet the overall IRTPA time guideline of 60 days when completing security clearances for contractors in National Security Information positions, primarily because of the time taken by the FBI to complete background investigations for its own contractors. The FBI accounted for almost all (99 percent) of the Department's National Security Information cases and averaged 108 days to complete clearances for its own contractors. One factor that contributed to the FBI's lengthy processing times was the time taken to complete security clearances for contract linguists. During the time period covered by this review, security clearances for FBI linguists took 67 days longer on average than for other FBI contractors (166 days versus 99 days) and added 9 days to the FBI's average total processing times.

Also during the time period covered by our review, procedures for tracking contractor personnel security information varied significantly throughout the Department. There was no single data source for tracking contractor personnel security information, and the various components kept information in multiple systems or, at times, in paper files. As a result, some components could not maintain accurate security information on their contractors. For example, in data ATF submitted to the OIG, 250 of 372 contractors were mistakenly listed as occupying National Security

Information positions when in fact they should have been listed as occupying Public Trust positions.

There is currently no comprehensive Department-wide security policy for contractors. SEPS has issued only minimal guidance that serves as a reference for components and does not provide any binding policy for components to follow in managing their contractor security programs. The guidance also does not provide standards regarding contractor tracking or reinvestigations. As a result, components frequently have to seek clarification from SEPS.

To improve the Department's management of the contractor personnel security process and to ensure that only individuals with the appropriate clearance level have access to sensitive and classified information, we recommend that:

1. SEPS implement procedures to identify contractor cases that are pending for a significant period of time and have exceeded OPM's 90-day adjudication requirement;

2. The USMS continue to use OPM's investigative services to complete background investigations for its CSOs;

3. SEPS require components to maintain rosters of their active contractors, including information on each contractor's clearance or risk level; and

4. SEPS issue a contractor security policy similar to the Department's employee security policy, including a contractor reinvestigation requirement that is consistent with the Department's employee reinvestigation requirement.

APPENDIX I: ACRONYMS

AOUSC	Administrative Office of the United States Courts
ATF	Bureau of Alcohol, Tobacco, Firearms and Explosives
BI	Background investigation
BOP	Federal Bureau of Prisons
CSO	Court Security Officer
DEA	Drug Enforcement Administration
DOJ	Department of Justice
e-QIP	Electronic Questionnaires for Investigations Processing
EOUSA	Executive Office for United States Attorneys
FBI	Federal Bureau of Investigation
FY	Fiscal year
IRTPA	*Intelligence Reform and Terrorism Prevention Act of 2004*
JMD	Justice Management Division
JSTARS	Justice Security Tracking and Adjudication Record System
MBI	Moderate background investigation
OIG	Office of Inspector General
OJP	Office of Justice Programs
OPM	Office of Personnel Management
SCI	Sensitive Compartmented Information
SEPS	Security and Emergency Planning Staff
SSBI	Single scope background investigation
USAO	United States Attorney's Office
USMS	United States Marshals Service

APPENDIX II: RELATED OIG REPORTS

The OIG reports listed below found that certain Department components did not have effective personnel security processes, which resulted in untimely background investigations and adjudications, personnel having unauthorized access to sensitive Department data and facilities, and other problems with the personnel security process.

- *Implementation of the Contractor Personnel Security Program in Selected Offices, Boards, and Divisions,* Evaluation and Inspections Report I-01-004 (March 2001).

- *Background Investigations Conducted by the United States Marshals Service,* Evaluation and Inspections Report I-2005-002 (February 2005).

- *United States Marshals Service's Use of Independent Contractors as Guards,* Audit Report 05-24 (May 2005).

- *The Federal Bureau of Investigation's Efforts to Hire, Train, and Retain Intelligence Analysts,* Audit Report 05-20 (May 2005).

- *Review of the Security and Emergency Planning Staff's Management of Background Investigations,* Evaluation and Inspections Report I-2005-010 (September 2005).

- *Follow-up Audit of the Federal Bureau of Investigation's Efforts to Hire, Train, and Retain Intelligence Analysts,* Audit Report 07-30 (April 2007).

- *The Federal Bureau of Investigation's Foreign Language Translation Program,* Audit Report 10-02 (October 2009).

- *Audit of the United States Marshals Service's Oversight of its Judicial Facilities Security Program,* Audit Report 11-02 (November 2010).

APPENDIX III: RISK LEVELS ASSOCIATED WITH BACKGROUND INVESTIGATION REQUIREMENTS

Each Department contractor position is assigned a position sensitivity level depending on the position's potential to adversely affect the integrity and efficiency of the agency's service.[36] Positions are designated as Public Trust unless access to National Security Information is required. If the position requires access to National Security Information, it is assigned a sensitivity designation of Special-Sensitive, Critical-Sensitive, or Non-Critical Sensitive. Positions with a Special-Sensitive designation require access to Sensitive Compartmented Information (SCI) and are assigned to individuals with Top Secret clearances. Table 2 summarizes the various position sensitivity levels and the background investigation required for each position.[37]

Table 2: Risk and Sensitivity Levels and Their Required Background Investigations

Position Sensitivity Level	Access level				Initial Background Investigation Required
	Confidential	Secret	Top Secret	SCI	
National Security Information Positions					
Special Sensitive				X	SSBI
Critical Sensitive			X		SSBI
Non-Critical Sensitive	X	X			National Agency Check with Law and Credit
Public Trust Positions					
High Risk	NO ACCESS				BI (5-year scope)
Moderate Risk					MBI
Low Risk					National Agency Check and Inquiries

Source: OIG.

A single scope background investigation (SSBI) covers the past 7 years of a subject's activities (or to age 18, whichever is less). It includes a personal subject interview; various law enforcement checks; national

[36] DOJ Security and Emergency Planning Staff, Contractor Personnel Security Guidance, September 1998.

[37] The investigative standards for contractors in Non-Critical Sensitive positions are less intrusive than the investigative standards for employees in similar positions. Employees in these positions receive a 5-year scope or MBI level investigation.

agency records checks on the subject's spouse or cohabitant; interviews with selected references and former spouses; and verification of an individual's employment, education, residence, citizenship, and date and place of birth.

A 5-year scope background investigation is similar to a SSBI, except it only covers the past 5 years of a subject's activities.

A moderate background investigation (MBI) consists of a personal subject interview and written inquiries covering a subject's employment, education, credit, and residence.

A national agency check with law and credit investigation consists of searches covering an individual's background during the past 5 years, as well as a credit search for the past 7 years. It does not include a personal subject interview.

A national agency check and inquiries investigation consists of searches covering an individual's background during the past 5 years. It does not include a personal subject interview.

APPENDIX IV: COMPONENTS WITH DELEGATED AUTHORITY FOR THE CONTRACTOR PERSONNEL SECURITY PROCESS

Component	Conduct Initial Investigations	Adjudicate Investigations
Bureau of Alcohol, Tobacco, Firearms and Explosives	Yes	Yes
Antitrust Division	OPM	Yes
Bureau of Prisons	OPM	Yes
Civil Division	OPM	Yes
Civil Rights Division	OPM	Yes
Community Oriented Policing Services	OPM	Yes
Community Relations Service	OPM	Yes
Criminal Division	OPM	Yes
Drug Enforcement Administration	OPM	Yes
Environment and Natural Resources Division	OPM	Yes
Executive Office for United States Attorneys	OPM	Yes
Executive Office for Immigration Review	OPM	Yes
Executive Office for U.S. Trustees	OPM	Yes
Federal Bureau of Investigation	Yes	Yes
Interpol Washington	OPM	Yes
Justice Management Division	OPM	Yes
Office of the Inspector General	OPM	Yes
Office of Justice Programs	OPM	Yes
Tax Division	OPM	Yes
United States Marshals Service	OPM	Yes
United States Parole Commission	OPM	Yes
All Other Components	OPM	SEPS

APPENDIX V: METHODOLOGY

For this review, the OIG conducted 13 site visits and interviewed more than 60 security officials and staff at the following components: ATF, BOP, Civil Division, Civil Rights Division, Consolidated Executive Office, Criminal Division, DEA, EOUSA, FBI, OIG, OPM, SEPS, USAOs in Los Angeles and Atlanta, and USMS.

We conducted four types of analyses to examine both the overall timeliness and quarterly timeliness of National Security Information and Public Trust cases. We also analyzed the timeliness of specific types of background investigations completed for Public Trust security cases. We performed a distribution analysis of National Security Information and Public Trust cases to determine the total number of job positions that could be identified by the Department. Lastly, we analyzed timeliness for one specific job category, contract linguists.[38] The methodology for each analysis is described below.

Selecting Cases for Analysis

The OIG analyzed cases handled either by OPM or the components that contained a "background investigation initiated" date, a "background investigation completed" date, and an "adjudication completed" date.[39] These cases represent those that have completed all phases of the security clearance process and are not pending in status. Each of these dates is exclusive to an individual case. We excluded cases that did not have both a "background investigation completed" date and an "adjudication completed" date because, without both dates, we could not account for timeliness of each of the phases required to complete the security process. Further, cases that did not have an "investigation initiated" date were excluded from our analysis because we could not determine when the security process started for those cases. We discuss each of our required dates below.

We calculated the difference between the "adjudication completed" date and the "investigation initiated" date to determine the total number of days taken to complete the security clearance process. Likewise, we

[38] Information on reciprocity and job series was not consistently captured across the Department. As a result, we were unable to evaluate whether the Department and its components were meeting the reciprocity requirements of IRTPA and whether clearances for specific positions take longer to process.

[39] We did not include any cases where a clearance was granted through DISCO.

calculated the difference between the "background investigation completed" date and the "background investigation initiated" date to determine the total number of days taken to complete investigation phase of the security clearance process. We also calculated the difference between the "adjudication completed" date and the "background investigation completed" date to determine the total number of days taken to complete the adjudication phase of the security clearance process.

Measuring Timeliness for National Security Information Positions

The OIG measured the average time to complete a National Security Information clearance for the fastest 90 percent of cases completed between October 1, 2009, and December 31, 2010, by quarter.[40] We used the "adjudication completed" date to determine which cases were completed in each quarter. The data available for analysis contained 402 cases.

We conducted a separate analysis to identify the fastest 90 percent of cases within each quarter. A total of 363 cases were identified among the three investigative agencies – ATF (3 cases), the FBI (359 cases), and OPM (1 cases). We used these cases to calculate the average time taken to complete background investigations and adjudication determinations for National Security Information clearances for the entire Department. This analysis also included a distribution analysis through which the percentage of the Department's National Security Information cases exceeding the 60-day IRTPA guideline was determined. We identified 310 of the Department's 363 National Security Information cases (85 percent) processed from October 1, 2009, through December 31, 2010, that failed to meet the overall IRTPA time guideline.

Measuring Timeliness for Public Trust Positions

To measure the average time to complete a background investigation and adjudication for Public Trust cases completed between October 1, 2009, and December 31, 2010, by quarter, we used the "adjudication completed" date. Based on our criteria, the data available for analysis contained 3,434 cases. The average was taken using 100 percent of cases because the IRTPA timeliness guidelines do not apply to Public Trust

[40] The OIG used the IRTPA guideline to measure the Department's performance because, although IRTPA does not establish a specific deadline for completing individual clearances, it does establish a general guideline and is accepted government-wide. Both OPM and the Office of the Director of National Intelligence use the fastest 90 percent of National Security Information cases in measuring agencies' performance against the IRTPA time guidelines.

positions. This analysis also included a distribution analysis through which the percentage of the Department's Public Trust cases exceeding the 90-day OPM adjudication requirement was determined. We identified 326 of the Department's 3,434 Public Trust cases (10 percent) processed from October 1, 2009, through December 31, 2010, that failed to meet OPM's requirement for completing and reporting adjudications.

Analyzing Cases by Job Series

The OIG was able to conduct a job series analysis only for the FBI's contract linguists because it was the only job series clearly and consistently identified in the data we received from components. More than 1,100 unique job titles were used for the 3,797 contract cases analyzed during this review. There did not appear to be any standard naming conventions across components or within specific components, making it impossible to reliably group and analyze jobs series. Contractor position information ranged from descriptive titles such as "Food Service Officer" and "Fire and Safety Manager" to ambiguous titles such as "General Clerk II" or simply "Analyst."

We analyzed FBI data for security clearances completed between October 1, 2009, and December 30, 2010, to determine timeliness delays between the fastest 90 percent of the cases for both FBI contract linguists and all other FBI contractor employees. We determined that 13 percent (46 of 359 cases) of all FBI contractors were contract linguists. The FBI averaged 166 days to complete all phases of the security process for these 46 cases.

Reviewing Case Files

We selected and reviewed 60 files to determine causes for potential timeliness delays among certain National Security Information and Public Trust contractor cases. We selected files from various components that used each of the three investigative agencies – the FBI, ATF, and OPM. We selected both long and short cases across the Department to identify commonalities. We also reviewed USMS files to ensure the analysis included sub-groups of the Department.

APPENDIX VI: THE SECURITY AND EMERGENCY PLANNING STAFF RESPONSE TO DRAFT REPORT

U.S. Department of Justice

Justice Management Division

Security and Emergency Planning Staff

Washington, D.C. 20530

FEB 22 2013

TO: JASON R. HIGLEY
ACTING ASSISTANT INSPECTOR GENERAL
EVALUATION AND INSPECTIONS DIVISION

FROM: JAMES L. DUNLAP
DEPARTMENT SECURITY OFFICER

SUBJECT: Office of Inspector General's Report Entitled: *Review of the Department's Contractor Personnel Security Process, Assignment Number A-2012-006*

This responds to the Office of Inspector General's (OIG) report entitled: *Review of the Department's Contractor Personnel Security Process, Assignment Number A-2012-006.*

I welcome and appreciate this review regarding the contractor personnel security process in the Department. I believe the recommendations from this report will have a positive impact in our personnel security and compliance review programs. The OIG staff was very thorough and their professionalism was greatly appreciated.

The OIG report contains three recommendations for my Staff. As requested, I will address the reports's recommendations and provide the appropriate plan of action for each. The recommendation numbers below correspond to those in the OIG report.

1. **SEPS should implement procedures to identify contractor cases that are pending for a significant period of time and have exceeded OPM's 90-day adjudication requirement.**

   We concur with this recommendation. A query has been written to extract this information from JSTARS, the Department's personnel security system. SEPS is planning to modify JSTARS' reporting capability to include this query, so components can generate the report as needed. Given budgetary constraints in today's economic environment, however, this modification will not be available until FY 14. In the meantime the JSTARS Service Desk will generate the query for all components, as requested.

   Next Steps:

   - The Personnel Security Group will communicate this plan to the Department via an e-mail to Department Security Programs Managers by March 1, 2013.

2. **The United States Marshals Service is responsible for replying to this recommendation.**

3. **SEPS should require components to maintain rosters of their active contractors, including information on each contractor's clearance or risk level.**

   We concur with this recommendation. This requirement is included in the draft Contractor Policy Statement scheduled to be issued by April 5, 2013.

4. **SEPS should issue a contractor security policy similar to the Department's employee security policy, including a contractor reinvestigation requirement that is consistent with the Department's employee reinvestigation requirement.**

   We concur with this recommendation. As stated above, SEPS plans to issue the Contractor Policy Statement by April 5, 2013. The current draft includes reinvestigation requirements as established by applicable laws.

I am committed to a strong and effective personnel security program, and recognize that there is always room for improvement. Therefore, you have my commitment that SEPS will work diligently to implement the recommendations to the best of its ability and as quickly as possible.

Should you have any questions or require additional information, please contact me directly at (202) 514-2094, or Dorianna Rice, Assistant Director, Personnel Security Group, at (202) 514-2351.

APPENDIX VII: OIG ANALYSIS OF THE SECURITY AND EMERGENCY PLANNING STAFF RESPONSE

The Office of the Inspector General provided a draft of this report to the Justice Management Division's Security and Emergency Planning Staff (SEPS) for its comment. SEPS's response is included in Appendix VI to this report. The OIG's analysis of SEPS's response and the actions necessary to close the recommendations are discussed below.

Recommendation 1: SEPS implement procedures to identify contractor cases that are pending for a significant period of time and have exceeded OPM's 90-day adjudication requirement.

Status: Resolved.

SEPS Response: SEPS concurred with this recommendation. SEPS stated that it has developed a query to extract this information from JSTARS. SEPS is planning to modify JSTARS so components can generate a report with this information on an as-needed basis. Due to budgetary restrictions, this report feature will not be available until FY 2014. However, the JSTARS Service Desk will generate the report for individual components on request. SEPS plans to issue an e-mail to component Security Program Managers in March 2013 with instructions on how to request the query.

OIG Analysis: SEPS's planned actions are responsive to our recommendation. By May 3, 2013, please provide a copy of the e-mail instructing components on how to use the JSTARS query. In addition, please provide documentation, including copies of any policy statements issued to the components, showing how SEPS will use the JSTARS query to ensure components are meeting OPM's adjudicative goals.

Recommendation 3: SEPS require components to maintain rosters of their active contractors, including information on each contractor's clearance or risk level.

Status: Resolved.

SEPS Response: SEPS concurred with this recommendation. SEPS stated that it planned to issue a Contractor Policy Statement by April 5, 2013, that requires components to maintain rosters of their active contractors, including information on each contractor's clearance or risk level.

OIG Analysis: SEPS's planned actions are responsive to our recommendation. Please provide a copy of the final Contractor Policy Statement by May 3, 2013.

Recommendation 4: SEPS issue a contractor security policy similar to the Department's employee security policy, including a contractor reinvestigation requirement that is consistent with the Department's employee reinvestigation requirement.

Status: Resolved.

SEPS Response: SEPS concurred with this recommendation. SEPS stated that it planned to issue a Contractor Policy Statement by April 5, 2013. The current draft of the policy includes a contractor reinvestigation requirement.

OIG Analysis: SEPS's planned actions are responsive to our recommendation. Please provide a copy of the final Contractor Policy Statement that includes the contractor reinvestigation requirement by May 3, 2013.

APPENDIX VIII: THE U.S. MARSHALS SERVICE RESPONSE TO DRAFT REPORT

U.S. Department of Justice

United States Marshals Service

Associate Director for Operations

Alexandria, Virginia 22301-1025

MEMORANDUM TO: Jason R. Higley
Acting Assistant Inspector General
for Evaluation and Inspections

FROM: David Harlow
Associate Director for Operations

SUBJECT: Response to the Draft Review of the Department's Contractor Personnel Security Process, A-2012-006

Attached is the United States Marshals Service (USMS) response to the Office of the Inspector General (OIG) regarding the draft Review of the Department's Contractor Personnel Security Process, Assignment Number A-2012-006.

Should you have any questions regarding these responses, please contact Ms. Isabel Howell at 202-307-9744.

Attachments

cc: Carl W. Caulk
Assistant Director
Judicial Security Division

Donald O'Hearn
Chief of Staff

Isabel Howell
Audit Liaison
United States Marshals Service

Louise Duhamel
Acting Director, Audit Liaison Group
Justice Management Division

Mary T. Myers
Audit Liaison Specialist, Audit Liaison Group
Justice Management Division

Response to Draft Report
Review of the Department's Contractor Personnel Security Process
Report Number A-2012-006

Recommendation 2: The USMS continue to use the Office of Personnel Management's (OPM) investigative services to complete background investigations for its Court Security Officers (CSOs).

Response: Concur.

The USMS will continue to use OPM's investigative services to complete background investigations for CSOs. In fiscal year (FY) 2010, the USMS Judicial Security Division performed extensive research into Executive Orders, as well as OPM policies and regulations as they relate to background investigations for CSOs. Internal discussions were held within the USMS, and information was gathered regarding other government agencies' practices for conducting contractor background investigations. As a result of these discussions, the review of other government agencies' best practices, and a review of background investigation costs for the last three fiscal years, it was determined that changes were needed to arrive at a more efficient and cost effective manner of conducting CSO background investigations.

In FY 2012, an implementation plan was drafted outlining procedures and cost analyses to transition CSO background investigation services to OPM. This plan was presented to the Administrative Office of the United States Courts (AOUSC) for FY 2013 funding consideration and approval. The AOUSC concurred with the implementation plan and approved funding to take effect at the beginning of FY 2013. The USMS considers the switch to using OPM investigative services for CSO background investigations to be a permanent change for the agency. We will continue to monitor OPM's success in completing background investigations in a timely manner and will work with OPM to solve any issues that arise.

APPENDIX IX: OIG ANALYSIS OF THE U.S. MARSHALS SERVICE RESPONSE

The Office of the Inspector General provided a draft of this report to the U.S. Marshals Service (USMS) for its comment. The USMS's response is included in Appendix VIII to this report. The OIG's analysis of the USMS's response and the actions necessary to close the recommendations are discussed below.

Recommendation 2: The USMS continue to use OPM's investigative services to complete background investigations for its CSOs.

Status: Closed.

USMS Response: The USMS concurred with this recommendation. In FY 2010, the USMS evaluated its process for conducting investigations for CSOs and determined that its existing processes were not cost-effective and were not aligned with other government agencies' best practices. In FY 2012, the USMS developed a white paper examining the CSO background investigation process, including a cost analysis and an implementation plan to begin using OPM's investigative services. The AOUSC, which provides funding for the CSO program, concurred with the USMS's decision to use OPM and the changes were implemented in FY 2013. The USMS also provided the OIG with a copy of the FY 2012 white paper with the USMS's plan for implementing OPM's investigative services for CSO background investigations.

OIG Analysis: Based on the actions reported by the USMS establishing its plans to continue to use OPM's investigative services for CSO background investigations, this recommendation is closed.