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

Background Investigations Conducted by the United States Marshals Service

Report Number I-2005-002

February 2005

EXECUTIVE SUMMARY

The Department of Justice's (Department) Office of the Inspector General (OIG) reviewed the United States Marshals Service's (USMS's) program for conducting background investigations of new applicants and periodic reinvestigations of current employees and contractors. We assessed whether the USMS ensured that background investigations and reinvestigations were timely, thorough, and complied with federal regulations and Department policies. To conduct this evaluation, we reviewed policies and procedures, interviewed officials involved in the process, and analyzed selected sample files for USMS employees and contractors.

The USMS background investigation process is divided into two distinct phases: the field investigation, when information is gathered on personnel; and the adjudication, when any potentially derogatory information is assessed and suitability for employment is determined. Investigations on USMS employees and contractors are conducted by the Federal Bureau of Investigation (FBI) for USMS political appointees and attorneys, the Office of Personnel Management (OPM) or its contractors for other USMS employees and some contractors, and the USMS itself for contract court security officers (CSOs) and certain contract guards. Adjudications are conducted by the Department's Security and Emergency Planning Staff (SEPS), the USMS Human Resources Division, and the USMS Judicial Security Division.

RESULTS IN BRIEF

Our review found that the USMS placed employees and contractors in national security or public trust positions only after the field investigation was completed or it issued a waiver, in accordance with federal regulations and USMS policy. However, we identified deficiencies in both the field investigation and adjudication phases of the USMS background investigation program. Due to incomplete and outdated policy guidance, inconsistent procedures, and incomplete and inaccurate data systems, the USMS did not ensure that field investigations or adjudications were timely or thorough. In fact, our analysis showed that investigations were slow, and neither investigations nor adjudications were consistently thorough.

Specifically, we found that the USMS placed or retained personnel in national security or public trust positions without complete investigative information. We also found that OPM investigations of USMS personnel

were not consistently timely or thorough. USMS field managers sometimes rejected the adjudicators' recommendations without providing written justification and the USMS hired or retained a few of these employees who subsequently engaged in significant misconduct. We also found that some reinvestigations were overdue. Furthermore, the USMS did not require reinvestigations for CSOs who have law enforcement responsibilities and carry firearms, regardless of how many years they worked at the USMS. By correcting these deficiencies, the USMS can better ensure that the individuals assigned to its national security and public trust positions have been thoroughly screened.

USMS policies and procedures for conducting background investigations are out of date and incomplete.

The most recent USMS policy guidance about its background investigation process was a draft 2001 Policy Directive on Personnel Security. USMS management told the OIG that the draft 2001 Policy Directive was intended to replace the 1995 USMS Security Policy and Procedures Manual, but it has never been completed or officially adopted. Moreover, neither document includes procedures to guide staff in implementing each step in the background investigation process.

In lieu of USMS policy guidance, USMS managers we interviewed indicated that they follow policy guidance provided by OPM and the Department through SEPS. With the exception of the 1995 and 2001 documents, we found no evidence that the USMS had prepared written guidance for its staff on how to implement OPM and SEPS policies to meet USMS personnel security requirements. In addition, USMS managers told us that they had implemented some changes without updating written policy, such as the transfer of authority from SEPS to the USMS for completing all national security background investigations at the Top Secret and lower levels.

We believe an organization the size of the USMS should have written guidance for ensuring personnel security. The USMS has 94 field offices nationwide and more than 4,000 employees and 12,000 contractors subject to background investigations. Its background investigation program is decentralized, with two internal organizations and SEPS sharing management responsibilities. The lack of written policies and procedures makes it difficult for the USMS to ensure that its background investigation program is consistent, effective, and accountable.

The databases used by the USMS to manage its background investigation program did not have complete and accurate information.

We found that the USMS relies on databases that are inadequate to monitor and assess its background investigation process. Because of these deficiencies, we could use them only in a limited way for our review. Our examination of the two Human Resources Division databases created to track background investigations of USMS employees and non-CSO contractors revealed that they were incomplete for identifying current personnel, inaccurate for tracking key event dates, and not structured to allow monitoring of compliance with significant regulatory and Departmental timeliness requirements. For example, the databases could not identify all current personnel whose background investigations had been conducted at headquarters; key data fields, such as the initiation or completion of an adjudication, were incomplete in over one-third of the records; and the USMS used the same field to record initial and subsequent background investigations, making it difficult to determine whether the USMS had complied with regulations and Department policy in initial hires because historical data was overwritten. In contrast, the USMS Judicial Security Division's database for tracking the status of CSOs' background investigations, medical suitability issues, and credit checks was current and complete. However, it did not contain information that Judicial Security Division management could use to facilitate planning, budget formulation, and assessment for its background investigation program.

Although field investigations conducted by all three entities on USMS employees and contractors were slow, adjudications of these investigations were generally timely.

There are no federal regulations that require that field investigations be completed within a specified number of days. We found that average investigation times ranged from 63 days for the field investigations USMS deputy marshals conducted on CSOs to 115 days for the field investigations the FBI conducted on USMS political appointees and attorneys. OPM investigations averaged 96 days for USMS employees and 104 days for USMS contractors.

Federal regulations require that adjudications of field investigations take place within 90 days. We found that adjudications of field investigations were generally timely. Both the Judicial Security Division and the Human Resources Division completed adjudications on average in less than 90 days. However, SEPS adjudications averaged 180 days to complete.

The USMS made adjudications based on incomplete files.

During our review, we found that 9 (14 percent) of the 66 employee investigation files and 8 (35 percent) of the 23 non-CSO contractor investigation files we examined lacked required documentation, such as internal affairs checks from prior law enforcement positions and employer references. Some of those files contained statements that OPM had not and would not attempt to obtain the missing information. The USMS adjudicators stated that they obtained some information themselves, but did not consistently obtain each document or reference omitted by OPM before adjudicating the case. We conducted a separate analysis of the background investigation files of employees who had been cited at a later time for misconduct and found that their files were more likely to have been incomplete than those of the employees in our general sample. This suggests that a complete field investigation is important for a background investigation to be effective in identifying potentially unsuitable personnel. We found that although the USMS adjudicators were not consistently completing the deficient OPM field investigation files, they were thorough in addressing potentially derogatory issues that surfaced during the background investigation process.

We also found that the Judicial Security Division issued security approvals to CSOs based on incomplete information. Our review indicated that required documents related to criminal history were missing from a quarter to a third of the 33 files in our sample. In addition, the Judicial Security Division conducted credit checks for only 16 (48 percent) of 33 files and verified medical suitability issues for 9 (50 percent) of the 18 files in our sample that contained medical issues.

USMS field managers sometimes pressured the Human Resources Division to set aside adjudicators' recommendations.

In reviewing the background investigation files of 28 USMS employees who had sustained misconduct charges, we found the adjudicators had recommended that 3 of the employees not be granted security approval. In each of these cases, a Human Resources Division supervisor added a memorandum to the file stating that the derogatory information was not sufficiently serious to justify denying a security approval for the individual.

When we asked about these cases, a senior Human Resources Division official said he had received verbal pressure in at least one of these cases from a high-level field manager to grant the security approval and, in response, had written a memorandum arguing that security approval be

granted despite the adjudicator's negative recommendation. He stated that it was not uncommon to receive input, usually by phone, from people outside his office who sought to influence decisions that are being made by the Human Resources Division on particular employees or applicants. This influence often comes from a U.S. Marshal in a district office who knows the applicant or employee. Unlike the files of those later cited for misconduct, the files in our general sample of 89 employees and contractors contained no Human Resources Division adjudicator recommendations against security approval.[1]

Reinvestigations were overdue for some employees, and the USMS did not reinvestigate contract CSOs who served in law enforcement positions.

The USMS's policy requires that it initiate reinvestigations every five years for employees and contractors serving in national security positions and for employees holding high- and moderate-risk public trust positions. In our sample of 54 cases, we found 2 instances in which reinvestigations had not been initiated within five years and 5 in which they had been initiated but not completed within five years.

In our general sample of employees, 54 of the 66 had worked longer than five years and were subject to reinvestigation, while in our misconduct caseload 26 of the 28 were subject to reinvestigation. We therefore also looked at two areas where delays in initiating or completing reinvestigations might have serious consequences: instances involving employee misconduct and instances in which security clearances lapsed. In the first area, we found that a higher percentage (19 percent, or 5 of 26) of employees with sustained misconduct charges had reinvestigations that were initiated but not completed than did employees in our general sample (9 percent, or 5 of 54). In the second area, we found that the USMS took the necessary steps to initiate reinvestigations. If holders of clearances failed to submit an application for reinvestigation, the USMS suspended their security approval. The Human Resources Division stated that there are currently no employees with lapsed clearances who require access to national security information.

[1] This includes the 66 employees and 23 contractors, including those with investigations conducted by other agencies, whose cases were adjudicated by the USMS Human Resources Division.

While the Judicial Security Division requires extensive background investigations before hiring contract CSOs (who serve in law enforcement positions and carry firearms), it does not reinvestigate them as a matter of policy. Our analysis of Judicial Security Division data showed that 2,208 (51 percent) of its 4,323 CSOs had been employed for five or more years. As a result of this policy, the USMS does not have the same assurances for CSOs that it requires for its employees with similar law enforcement duties.

RECOMMENDATIONS

In this report we make seven recommendations to help the USMS ensure that its background investigation program identifies applicants and employees who are not suitable for national security and public trust positions. The recommendations focus on revising policies and procedures, upgrading the databases that are used to manage background investigations, improving the thoroughness of adjudications, developing controls to monitor the background investigation process, and requiring that contractors fulfilling law enforcement duties be reinvestigated. We recommend that the USMS take the following actions:

1. Revise and formally adopt written policies and procedures that address all aspects of the background investigation process to reflect current federal regulations and Department policy.

2. Develop an adequate structure for the Human Resources Division database to ensure that essential data are not overwritten and to enable both the Human Resources Division and the Judicial Security Division to monitor compliance with regulations and Department policy.

3. Implement procedures to routinely review the accuracy of the databases that the Human Resources Division and the Judicial Security Division use to manage the background investigation program.

4. Require periodic written reviews on the efficiency and effectiveness of the background investigation program to determine if process improvements are needed.

5. Develop guidelines for adjudicators that include instructions on how to proceed when an OPM investigation is incomplete and criteria for recommending security approvals and disapprovals that are consistent with OPM and Department policy.

6. Require that the Chief of Human Resources Services fully document comments from field managers on an adjudicator's recommendation regarding a security approval for an applicant or employee.

7. Require reinvestigations every five years for contractors who are assigned law enforcement duties.

TABLE OF CONTENTS

BACKGROUND

UNITED STATES MARSHALS SERVICE MISSION

The mission of the United States Marshals Service (USMS) is to protect the members of the federal judiciary, including more than 2,000 federal judges, in 94 districts nationwide; execute federal warrants by pursuing and arresting fugitives; house and transport federal prisoners; ensure the security, health, and safety of government witnesses and their dependents; provide security at federal courthouses; and manage assets seized from criminal enterprises. In addition, the USMS regularly participates in the Joint Terrorism Task Forces. To accomplish its mission, the USMS employs more than 4,000 employees and 12,000 contractors who serve in positions of public trust or need access to sensitive information.

FEDERAL REQUIREMENTS FOR BACKGROUND INVESTIGATIONS

All federal agencies have programs to ensure that they hire and retain trustworthy personnel and that they properly clear personnel who need access to sensitive information. These programs involve conducting background investigations on prospective employees and contractors and reinvestigations for personnel remaining on the job beyond a specified period. An effective background investigation program identifies individuals who are unsuitable for jobs that involve national security or public trust responsibilities.

Agencies must develop policies and procedures that define a process for accomplishing background investigations in compliance with federal regulations and must establish safeguards to ensure that background investigations are timely and thorough. Agencies must also identify national security and public trust positions, and maintain current and accessible data on the status of background investigations for personnel assigned to those positions.

Under Executive Order 10450, the Office of Personnel Management (OPM) has broad oversight authority for federal personnel security programs, including background investigation programs. OPM exercises this authority primarily through regulations contained in Title 5 of the Code of Federal Regulations (CFR) Part 731, “Suitability”; Part 732, “National Security Positions”; and Part 736, “Personnel Investigations.” OPM enters into contracts with private companies to conduct the investigations and

reinvestigations of many federal employees and to report the results of the investigations to the employees' hiring agencies. Some agencies, such as the Federal Bureau of Investigation (FBI), have been delegated authority to conduct their own investigations of their employees and contractors.

The sensitivity level of the position and the employee's need to access national security information determine the scope of a background investigation.[2] Each federal agency designates the sensitivity levels of its positions according to the degree of public trust associated with the duties performed. For example, positions designated as special-sensitive entail access to Top Secret national security information and require the most extensive background investigations. Investigations for these positions involve detailed interviews with family and associates, and a wider range of checks of administrative, financial, criminal, and national security records. Table 1 on page 3 shows how the extent of the background investigation is related to the position responsibilities and access to national security information.

Reports on completed field investigations are sent to the applicants' hiring agencies for adjudication. There, adjudicators examine potentially derogatory issues uncovered by the investigations and determine whether the issues are likely to affect the applicants' reliability in safeguarding classified information or serving in public trust positions. The adjudicator makes a recommendation to approve or disapprove an applicant, depending on whether the potentially derogatory issues have been favorably resolved. Adjudications must take place within 90 days after the investigation is received.[3]

[2] Executive Orders 12958, "Classified National Security Information," prescribes a uniform system for classifying, safeguarding, and declassifying national security information. National security information is defined as information that, if released without authorization, could cause "harm to the national defense or foreign relations of the United States."

[3] Executive Order 10450, Section 14 (c), "Security Requirements for Government Employees," April 23, 1953.

Table 1: Sensitivity Levels and Security Clearances

Position Sensitivity	National Security Information Access	Background Investigation
Special-sensitive	Top Secret	Single-scope (extensive personal interviews and record checks) background investigation
Critical-sensitive	Secret and Confidential[a]	National security information (access) checks, and national agency checks and inquiries
High-risk public trust	None	Standard full field background investigation
Moderate-risk public trust	None	Minimum background investigation
Low-risk public trust	None	National agency checks and inquiries

Source: SEPS and USMS

[a] The USMS does not have any employees or contractors cleared at the Confidential level.

Because background investigations can be lengthy and there may be urgency in filling some positions, Executive Orders and OPM regulations allow agencies to hire an employee or contractor on a waiver while the full background investigation is proceeding. In such cases, the background investigation is completed after the individual begins work, and derogatory information uncovered after the applicant enters on duty can result in termination. Waivers require certain initial background checks, which are more comprehensive as security levels rise. The Department has issued guidance on waiver requirements, which is more stringent than OPM standards.[4] See Table 2 on page 4 for regulatory, Department, and USMS background investigation requirements.

[4] Department of Justice Order 2610.2A, "Employment Security Regulations," August 21, 1990.

Table 2: Background Investigation Requirements

	Federal Regulation **5 CFR § 736.201(c)[a]**	Department **Policy 2610.2A, August 1990, 6(b)**	USMS **Policy and Procedures March 1, 1995**
NATIONAL SECURITY POSITIONS			
Background Investigations (BI)			
Employees			
Top Secret or higher clearance	Field investigation completed or waiver before entering on duty (EOD)	Full BI or waiver before EOD, 180-day waiver limit	Field investigation completed or waiver before EOD
Secret clearance	Field investigation initiated or waiver obtained before EOD	Full BI or waiver before EOD, 180-day waiver limit	Field investigation completed or waiver before EOD
Contractors			
Top Secret or higher clearance	Field investigation completed or waiver before EOD	No additional requirements, 180-day waiver limit	No additional requirements
Secret clearance	Field investigation initiated or waiver obtained before EOD	No additional requirements, 180-day waiver limit	No additional requirements
Reinvestigations (RI)			
All employees and contractors	RI initiated, interim clearance required for access to NSI	No additional requirements	No additional requirements
PUBLIC TRUST POSITIONS			
Background Investigations (BI)			
Employees			
Deputy marshals (all categorized as high-risk public trust)[b]	Field investigation initiated within 14 days after EOD or waiver obtained	Full BI or waiver before EOD	Field investigation completed before EOD[c]
Contractors			
All contractors	Field investigation initiated within 14 days after EOD or waiver obtained	Waiver and proof field investigation initiated	No additional requirements
Reinvestigations (RI)			
Employees[d]	No RIs required	RIs initiated within 5 years	No additional requirements
Contractors	No RIs required	No additional requirements	No additional requirements

See Table Notes on the following page[5]

USMS BACKGROUND INVESTIGATION PROCESS

In addition to governmentwide requirements, the USMS is governed by Department policy and its own policies regarding the consistency of its background investigation process. At the Department level, the Security and Emergency Planning Staff (SEPS) recommends Department policy regarding such issues as circumstances and requirements for hiring applicants on waivers and for reinvestigating employees and contractors. SEPS also develops guidance on background investigations and monitors USMS compliance with regulations and Department policy. In addition, SEPS acts as the Department liaison with OPM.[6]

Within the USMS, the Operations Support Division develops policy and procedures for protecting national security information and other sensitive information, as well as for protecting personnel, facilities, and other assets. The USMS Human Resources Division oversees the implementation of these policies and procedures in day-to-day operations and maintains a list of its national security and public trust positions for which security approvals are required.

[5] Below are the table notes for Table 2 on page 4:

[a] Regulation 5 CFR § 736.201(c) encompasses guidance provided in Executive Order 10450 and in 5 CFR Part 732 and 5 CFR Part 731. The text reads: "Timing of investigations. Investigations required for positions must be initiated within 14 days of placement in the position except for: Positions designated Critical-Sensitive under part 732 of this chapter must be completed pre-placement, or post-placement with approval of a waiver in accordance with §732.202(a) of this chapter; and for positions designated Special-Sensitive under part 732 of this chapter must be completed pre-placement." Because 5 CFR Part 732 concerns only national security positions, the requirement for a complete investigation or waiver does not apply to high-risk public trust positions.

[b] Deputy marshals are routinely upgraded to Secret clearances after they have entered on duty and completed basic law enforcement training.

[c] The policy requiring that deputy marshals have a completed field investigation before entering on duty was introduced after the March 1995 policy and procedures were implemented.

[d] Department and USMS policies do not require reinvestigations of low-risk public trust employees.

[6] The SEPS Compliance Review Group visits USMS districts to monitor compliance with regulations and policy concerning personnel and physical security, and makes recommendations for improvement to the USMS Operations Support Branch Assistant Director.

For high-level USMS employees SEPS is responsible for the field investigations, reinvestigations, adjudications, and clearances. For all other USMS employees and contractors, SEPS has delegated the management of background investigations, reinvestigations, waivers, adjudications, and clearances to the USMS. Of the background investigations and reinvestigations the USMS manages, most are handled by the Human Resources Division. Another USMS unit, the Judicial Security Division, manages the background investigations for contract court security officers (CSOs). Details on these three processes are provided below.

Table 3 summarizes the division of responsibility for USMS waivers, background investigations, and reinvestigations, and it shows the number completed in calendar years (CYs) 2002 and 2003. The chart in Appendix I depicts the USMS units with personnel security responsibilities.

Table 3: USMS Waivers, Background Investigations, and Reinvestigations, CYs 2002 and 2003

Organizational Unit	Population Covered	Waivers, BIs, and RIs approved	
		2002	2003
DOJ Security and Emergency Planning Staff	Political appointees, attorneys, specially designated positions, and any USMS employee or contractor who requires a clearance above the Top Secret level[a]	94	30
USMS Human Resources Division	Employees and contractors with clearances at the Top Secret and lower levels, and public trust positions	718	1,549
USMS Judicial Security Division	Contract court security officers	512	556
Total		**1,324**	**2,135**

Source: USMS and SEPS databases

[a] Top Secret is the highest level of clearance, but this report refers to clearances "above the Top Secret level." Some information is so sensitive that access must be further restricted and requires a more extensive background investigation. The term "Sensitive Compartmented Information" (SCI) describes this type of information.

Background Investigations of USMS Political Appointees, Attorneys, and Other Designated Positions

SEPS directly manages the entire background investigation process for high-level USMS positions including the Director, the 94 U.S. Marshals, other political appointees, and attorneys. It also manages the background investigation process for other designated positions such as the Chief of Human Resources Services, who is responsible for the background investigations of most other USMS employees and contractors. In addition to managing the process for this group of some 127 individuals, SEPS also manages all background investigations for USMS employees needing access to Sensitive Compartmented Information (SCI) which refers to particular categories of classified information with special handling requirements. According to SEPS, political appointees and attorneys in the Department, including those at the USMS, normally enter on duty with waivers. Other USMS employees SEPS manages fall under general Department policies requiring either a completed background investigation or a waiver.

Background Investigations of Employees and Non-CSO Contractors

The USMS Human Resources Division manages the background investigation process for deputy marshals and all other employees not managed by SEPS, as well as all non-CSO contractors. The USMS's contractor personnel are grouped into two categories: contract CSOs, who are managed by the Judicial Security Division, and non-CSO contractors, who are managed by the Human Resources Division. In most instances, OPM (using its own contractors) conducts the field investigations and reinvestigations for the non-CSO contractors, and the Human Resources Division staff adjudicates them. (An exception is the intermittent contract guards discussed at the end of this section.) The same approach is used for USMS employees.

Since 2001, the number of deputy marshals – who represent approximately three quarters of all permanent USMS employees – has increased steadily. Prior to 2001, the USMS hired about 100 deputy marshals a year. However, during the past three years, increased national security responsibilities led to the hiring of approximately 700 new deputy marshals. To manage the large number of new hires, the USMS introduced a "big tent" hiring strategy. The USMS brings applicants who pass a written test and preliminary screening to one location on a single day for an interview with a panel of deputy marshals, an interview with an OPM investigator, and a medical screening. For applicants who are tentatively

selected for employment, the USMS initiates a full background investigation for which OPM investigates all issues necessary for both the high-risk public trust and national security Secret levels. Through this process, the USMS believes it saves resources and eliminates the need to hire deputy marshals on waivers. After the background investigations are completed, applicants who have been approved are hired at the high-risk public trust level and sent to USMS basic training. After basic training is completed, the USMS routinely requests Secret clearances for the new deputy marshals.

Although SEPS has retained authority for SCI clearances, it has delegated to the USMS final approval authority for national security clearances at the Top Secret and lower levels for its employees and contractors. The USMS Human Resources Division manages the process for clearances through the Top Secret level and forwards requests for SCI clearances to SEPS for investigation, adjudication, and approval.

An exception to the Human Resources Division's general approach to background investigations is the management of certain intermittent low-risk public trust positions. For example, contract security guards, who are usually current or retired local law enforcement personnel, are hired to work alongside regular USMS security personnel in courthouses. Background investigations for low-risk public trust positions consist of an FBI name search, employment inquiries, and a local criminal record search. Field offices perform the adjudications, with approval or disapproval granted by the district's U.S. Marshal or a delegated deciding official.

Consistent with Department policy, the USMS requires the reinvestigation of all employees every five years – or sooner if requested – except employees in low-risk public trust positions (a category that includes less than 1 percent of USMS employees). However, contractors are not required to undergo reinvestigations unless they have national security clearances at the Secret or higher level. If a clearance expires before a reinvestigation is completed, the USMS can grant an interim clearance if it has adequate justification.[7]

Reinvestigations include a check of the individual's official personnel file (maintained by the Human Resources Division) and a check with the Office of Internal Affairs in the Operations Support Division to determine

[7] If their clearance has expired, SEPS can issue an interim clearance for political appointees, attorneys, or individuals with a clearance above Top Secret.

whether there are any sustained misconduct charges against the individual or any pending investigations.

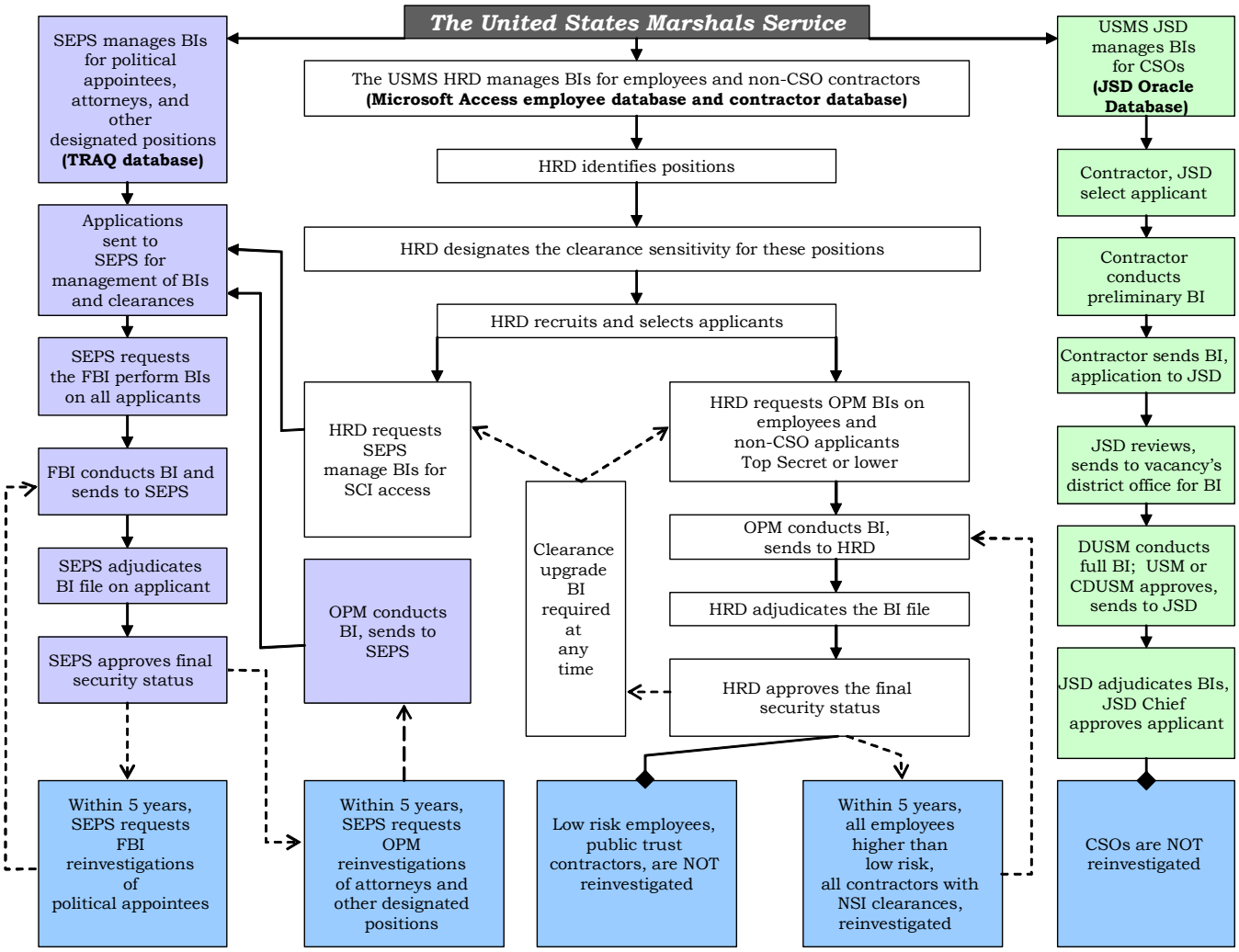
Background Investigations of Contract Court Security Officers

The Judicial Security Division manages the background investigation process for contract CSOs who screen visitors, patrol federal court property, control traffic, and provide armed escorts in and around federal court facilities. Unlike the rest of the USMS's operations, which are funded through executive branch appropriations, the judicial branch funds the CSO program. Under procurement authority from the General Services Administration, the USMS contracts with private companies to secure the services of CSOs for all 94 judicial districts.

In its contracts with the private companies that supply CSOs, the USMS specifies the criteria for identifying suitable individuals for public trust positions and for processing background investigations. After a vacancy has been announced in a district facility, the contractor recruits an applicant and conducts a preliminary investigation to verify qualifications and suitability. If the applicant passes this preliminary investigation, a deputy marshal in the district conducts a more extensive field investigation and sends the results to the Judicial Security Division to be adjudicated. The Chief Inspector of the Judicial Security Division makes the final security determination. CSOs are not reinvestigated after five years, but receive annual medical examinations to ensure that they are physically fit to perform their assigned duties.

Chart 1 shows the three background investigation processes used for USMS personnel.

Chart 1: Background Investigation Processes



BI	Background investigation
CDUSM	Chief Deputy U.S. Marshal
CSO	Contract court security officers
DUSM	Deputy U.S. Marshal
FBI	Federal Bureau of Investigation
HRD	Human Resources Division
JSD	Judicial Security Division
OPM	Office of Personnel Management
NSI	National security information
SEPS	Security & Emergency Planning Staff
SCI	Sensitive Compartmented Information
USM	United States Marshal
USMS	United States Marshals Service

→	=	Required for all cases
⇢	=	Required for upgrades & reinvestigation
◆	=	Final step, no reinvestigations occur

□	=	Process managed by HRD
	=	Process managed by JSD
	=	Process managed by SEPS
	=	Actions after initial BI completed

PURPOSE, SCOPE, AND METHODOLOGY

The Office of the Inspector General (OIG) reviewed the USMS background investigation program for new applicants and the periodic reinvestigations of current employees and contractors to determine whether the USMS complied with federal regulations and Department policy; whether its investigations and adjudications were timely and thorough; and how it monitored and assessed its process for conducting background investigations and reinvestigations of employees, CSOs, and other contractors whose investigations were adjudicated by USMS headquarters.

To conduct this review, we examined regulations, policies, procedures, and contracts that governed the background investigation process. We interviewed USMS and Department officials involved in the process, including Human Resources Division and Judicial Security Division managers and adjudicators, SEPS officials tasked with oversight and managing adjudications, OPM managers, and USMS and OIG officials responsible for misconduct investigations. We also analyzed 183 random and 29 selected background investigation files to determine whether OPM, FBI, and USMS field investigations and USMS and SEPS headquarters adjudications were thorough, whether the USMS and SEPS analyzed information obtained in the investigations in accordance with OPM and Departmental guidance, and whether the background investigation program had sufficient oversight. Finally, we reviewed USMS databases used in tracking background investigations, both to obtain information and to evaluate their capabilities for case tracking and program management. Full details on the scope and methodology of this review are in Appendix II.

RESULTS OF THE REVIEW

PROGRAM MANAGEMENT: IMPLEMENTATION AND OPERATIONS

The USMS policies and procedures for conducting background investigations are out of date, incomplete, and, in some cases, unwritten. Adjudications and security approvals were not consistently thorough because they were based on files that were incomplete and may not have included all potentially derogatory information. In addition, the USMS used multiple databases that lack accurate and complete information needed to manage the background investigation program. Consequently, the USMS cannot track the time required to complete background investigations. The practice of granting security approvals without complete information increases the risk that the USMS may hire untrustworthy individuals for national security and public trust positions.

We found that the USMS generally complied with federal regulations requiring an investigation or waiver prior to placement in a national security or public trust position. However, the USMS does not have current, complete written operational policies and procedures for conducting its background investigation program. For example, we found that the USMS does not have a policy defining what information must be included in an investigation file before it can be adjudicated or specific procedures for adjudicators on completing investigation files that are missing information. The most recent policy guidance that the USMS could provide was a draft 2001 Policy Directive on Personnel Security that was intended to replace the 1995 USMS Security Policy and Procedures manual. However, neither the draft 2001 guidance nor the cleared 1995 guidance adequately addresses many aspects of the USMS background investigation process. USMS management told us that the 2001 draft policy was intended to replace cleared 1995 guidance, but that it had never been completed and officially adopted. A USMS official stated that policy formation takes a long time and that the draft policy is kept on the intranet as a "work in progress" and updated as issues develop.

USMS managers indicated that they follow policy guidance on background investigations that is provided by OPM and the Department through SEPS. With the exception of the 1995 and 2001 documents, we

found no evidence that the USMS had prepared written guidance for its staff on how to implement OPM and SEPS policies to meet USMS personnel security requirements. In addition, USMS managers told us that they had implemented some changes without updating written policy, such as the transfer of authority from SEPS to USMS for completing all national security background investigations at the Top Secret and lower levels. Therefore, the existing written guidance becomes less useful each year.

We believe it is unacceptable for an organization of 4,000 employees and 12,000 contractors, with field offices nationwide, to rely on unwritten guidance for ensuring personnel security. Adding to our concern is the fact that the USMS background investigation program is decentralized, with two internal organizations and SEPS sharing management responsibility for conducting background investigations of different groups of USMS employees and contractors.

The impact of the lack of written policy and procedures on the USMS's background investigation process is illustrated by weaknesses in the adjudication process. This process begins when the USMS adjudicator receives an OPM or USMS background investigation file. The file contains documents that the OPM or USMS investigator has collected or created for use in the adjudication. If the USMS adjudicators find that documents are missing, they search for the missing information and, in some cases, may obtain it through telephone calls. However, the adjudicators work without written guidance on what documents must be in a file for it to be considered complete enough for review, and there is no official checklist on which to record a file's contents. Adjudicators also have no written guidance on how to document information that they obtain over the telephone when seeking information missing from a file. Therefore, each adjudicator uses discretion in determining the documents to be reviewed. Moreover, supervisors have no written guidance that defines the criteria and procedures for granting or denying security approvals or that explains what documentation is required for their decisions.

The USMS uses multiple databases that lack accurate and complete information to manage the background investigation process. The USMS relies on databases that are structurally inadequate and have an unacceptably high level of inaccurate or missing data. As a result of the poor quality, the USMS cannot use the databases effectively to monitor and assess its background investigation process, and because of these deficiencies we could use them only in a very limited way for our review. Databases are important tools for accumulating information, such as the entered-on-duty date and the timing of reinvestigations, on each USMS

employee and contractor to facilitate monitoring activities. Databases can also assist management in tracking the names and job positions of personnel with security clearances. In addition, if the USMS had adequate databases, it could utilize them for evaluating its background investigations program. A description of the weaknesses in the databases used by the Human Resources Division and Judicial Security Division follows.[8]

Human Resources Division Databases for USMS Employees and Non-CSO Contractors

We examined the two databases created by the Human Resources Division to track background investigations of USMS employees and non-CSO contractors. In each of the two databases, current personnel records were incomplete, key event dates were inaccurate, and the overall structure did not allow significant regulatory and Department timeliness requirements to be tracked. For example:

- *Completeness:* Of the 66 employees and 58 contractors we selected at random from the two databases, we found 35 instances in which the databases included personnel who should not have been in the database, excluded personnel who should have been in the database, or included personnel whose paper records could not be located. More specifically:
  - Although the contractor database was designed to track contractors who had been adjudicated at headquarters, 28 records identified low-risk contract guards whose background investigations were managed and retained at the local level and who should not have been in the Human Resources Division contractor database.
  - When we requested one contractor file, we received instead the file of a contractor with the same name and a different date of birth and social security number. This contractor was not in the employee or contractor database.
  - The records of one employee were erroneously included in the contractor database.

[8] SEPS separately maintains the data for political appointees, attorneys, and other designated positions as part of its responsibility for managing the background investigations of those categories of USMS employees.

- The records of another employee who had been deceased for several months had not been moved to the USMS's archive database.
- The files of four contractors in the database could not be located at headquarters or in field offices, and it was not possible to determine when, or by whom, they had been investigated.

Human Resources Division officials told us that until we requested the random sample of files, they had not been aware that contractors who were adjudicated in field offices had been erroneously included in the Human Resources Division database. They also explained that the quality of data on contractors is poor because field offices do not inform them of contractor personnel changes. Without a current and complete list of all current personnel over which the Human Resources Division has jurisdiction, the USMS cannot ensure that all its personnel have appropriate security approvals.

- *Accuracy:* Our review compared 66 employee files and 23 contractor files that were available for review to the tracking database. We found that three key event dates (the dates a background investigation was requested, adjudicated, and approved) were missing or inaccurate for 43 percent (86 of 198) of the key fields in the employee database and for 51 percent (35 of 69 fields) of the key fields in the contractor database.

- *Structure:* The database is structured so that subsequent upgrades or reinvestigations overwrite the dates of earlier investigations, thereby leaving no permanent record of earlier event dates. This practice, and the fact that paper files are periodically purged of older records, made it impossible to determine whether the USMS met the requirements for initiating and completing investigations for employees and contractors who had been upgraded or reinvestigated.

In addition to these defects in structure and accuracy in the two Human Resources Division databases, we found that they were not designed for more advanced program management and data analysis functions. For example, the databases did not identify instances in which the USMS received investigation files from OPM that were missing information. The

databases also did not record the amount of time adjudicators spent processing each case.[9]

Judicial Security Division Database for Contract Court Security Officers

In contrast, the Judicial Security Division's database for tracking the status of CSOs' background investigations, medical suitability issues, and credit checks was current and complete. However, the system is not integrated with Operations Support and Human Resources Division personnel databases. Therefore, although the Operations Support and Human Resources Divisions have overall responsibility for personnel security, they do not have access to automated information on CSO background investigations.

[9] Regulation 5 CFR §732.302 (b) states: "In accordance with section 14(c) of E.O. [Executive Order] 10450, agencies shall report to OPM the action taken with respect to individuals investigated pursuant to Executive Order 10450 as soon as possible and in no event later than 90 days after receipt of the final report of investigation."

USMS EMPLOYEES AND NON-CSO CONTRACTORS

The USMS generally complied with its policy requiring that field investigations be completed – or waivers issued – before employees and contractors entered on duty. USMS adjudicators generally met regulatory timeliness requirements for adjudicating the investigations it received. While the USMS did not ensure that the files were complete, its adjudicators addressed any potentially derogatory issues that were discovered during the field investigation. USMS field managers sometimes rejected adjudicators' recommendations that candidates not be given security approval without explaining their actions in writing. In addition, a few of the reinvestigations that the USMS must conduct every five years on a large portion of its personnel were overdue. The background investigations of USMS employees managed by SEPS generally complied with regulations and Department policy, and the investigations and adjudications, while thorough, were consistently slow.

The USMS generally complied with its policy requiring that it complete field investigations before allowing employees or contractors to enter on duty.[10] Under certain circumstances, the USMS issued a waiver that allowed an employee or contractor to begin work before the investigation was complete.

In our review, the USMS complied with its policy to complete the field investigation or issue a waiver for all but three of the employees and contractors whose files we examined. Files for 18 of the 66 employees and 20 of the 25 non-CSO contractors in our sample contained the information we needed to determine what steps the USMS had completed before the employees entered on duty. We found that the USMS had completed the required steps before 15 of the employees and 18 of the contractors entered

[10] USMS Security Policy and Procedure, March 1, 1995, requires that an investigation be completed, or a waiver issued, before entry on duty. DOJ Order 2610.2A dated August 3, 1990, requires that all positions be filled only by persons on whom complete investigations have been conducted, adjudicated, and approved, unless a waiver of that requirement has been obtained.

on duty.[11] Two employees and one contractor had entered on duty without a waiver after an OPM field investigation was completed but before the adjudicator's recommendation was approved, a practice allowed by USMS guidance. All employees and contractors with national security clearances had completed background investigations before they entered on duty; none in our sample was hired with a waiver or an unadjudicated OPM field investigation. Table 4 summarizes our findings.

Table 4: Phase of Background Investigation Process Under Which Employees and Contractors Entered on Duty

Entered on duty:	Employees	Contractors
In compliance with Department policy		
Full background investigation process completed	10	1
Waiver issued	5	14
Clearance issued by another agency	N/A	3
In violation of Department policy		
Field investigation completed and adjudicated but not yet approved, no waiver issued	2 [a]	1 [a]
Investigation initiated but not completed	1[a]	1[a]
Total reviewed	**18**	**20**

Note: Contractors are permitted to enter on duty under national security clearances granted by other federal agencies; employees are not. (Executive Order 12829, January 6, 1993, "National Industrial Security Program.")

[a] These employees and contractors were hired in public trust positions. Allowing them to enter on duty met federal regulatory requirements, but not Department and USMS policy.

A USMS official explained that in the early 1990s, USMS field offices conducted field investigations and granted waivers. Beginning in 2000, OPM gradually started doing more of the field investigations for deputy marshals and the USMS granted fewer waivers. Currently, the USMS rarely grants a waiver for a new deputy marshal because hiring a deputy marshal on a waiver is considered too great a risk. The USMS waiver requirements include checks of prior employment, references, internal affairs records, and FBI fingerprint and name checks. A full OPM field investigation provides, in addition, a 7-year credit check, a check of residence and education, an in-person interview with the applicant, a review of prior federal background investigations and federal databases, a check of court records, and additional law enforcement checks. An OPM field investigation may also

[11] Three of the contractors had clearances from other agencies, which allowed them to enter on duty at the USMS without waivers before the USMS's background investigation process was complete.

include in-person or telephone interviews with former employers, neighbors, and references.

Because there were too few recently hired deputy marshals in our sample to evaluate whether the USMS was following this policy of not allowing deputy marshals to enter on duty with just a waiver, we checked data in the USMS employee database.[12] For the 366 most recently hired deputy marshals for whom information was available, we determined that in 352 cases, or 96 percent, OPM provided the USMS with a field investigation report before the deputy marshals entered on duty.[13] Consequently, we concluded that the USMS appears to be following its policy.

USMS adjudicators generally meet regulatory timeliness requirements for adjudicating the investigations. There are no federal regulations requiring that field investigations be completed within a specified number of days. Insight into completion times can be gained from the categories OPM used until 2003 to charge agencies different rates for investigations completed within different time frames: 35, 75, or 120 days.[14] The average OPM field investigation completion time for the employees in our sample was 96 days and for contractors in our sample, 104 days. When we asked OPM about the timeliness of its field investigations, OPM responded that even priority field investigations now average 175 days, as OPM has had difficulty responding to the sharp increase in demand for field investigations governmentwide.

Once a field investigation is completed, Executive Order 10450 requires that adjudications be completed within 90 days.[15] We found that USMS adjudicators generally met this requirement, with an average completion time of 75 days for employees in our sample and 86 days for contractors.

[12] Our file review included three deputy marshals who had been hired since 2001 for whom we could determine whether the investigation was completed before hire. Two of the deputy marshals had completed OPM investigations, and one had a partial OPM investigation.

[13] An additional 38 records were excluded because dates were missing and it was not possible to determine whether the background investigation had been completed before the applicant entered on duty.

[14] After 2003, agencies were offered a choice of Code A (priority), Code B (accelerated), or Code C (standard) investigations, but OPM no longer defines the categories by the estimated time involved.

[15] Executive Order 10450, Section 14 (c), "Security Requirements for Government Employees," April 23, 1953.

USMS adjudicators addressed potentially derogatory issues, but the USMS did not ensure that the investigation files were complete. We examined two aspects of the thoroughness of the USMS's background investigation process: whether the files were complete and whether the adjudicators addressed any potentially derogatory issues that could have a negative effect on an applicant's suitability for a national security or public trust position. During our review, we found files that were missing required documentation. Some of those files contained statements that OPM had not and would not attempt to obtain the missing information. We conducted a separate analysis of the background investigation files of employees who had been cited at a later time for misconduct and found that their files were more likely to have been incomplete than those of the employees in our general sample. We also found that although the USMS was not consistently thorough in completing background investigation files, the USMS adjudicators were thorough in addressing potentially derogatory issues that surfaced during the background investigation process.

Completeness of files. We examined the files of 66 employees and 23 non-CSO contractors to see whether they contained either the documentation required by OPM regulations and Department guidance or references to that documentation indicating that the regulations and guidance had been followed.[16] We checked the files for the following information:

- Evidence that OPM identified and investigated any discrepancies in paperwork the applicant provided;
- Documentation of all required credit, administrative, and criminal history checks (including fingerprint checks and the applicant's signed Lautenberg statement attesting that he or she has not been convicted of a domestic violence misdemeanor);[17]
- Source checks, including prior background investigations, employment records, and Selective Service records;

[16] While our sample of contractors' background investigations files totaled 25, for this portion of our review we were able to use only 23. These 23 files were those kept at USMS headquarters, adjudicated by USMS headquarters, and containing OPM investigations. The other two files did not have copies of the OPM investigation conducted when the contractors worked at another agency, which had cleared them before they went to the USMS.

[17] The Lautenberg Amendment (18 U.S.C. § 922(d)(9) & (g)(9)), enacted in September 1996 and effective retroactively, bans individuals convicted of such crimes from carrying a weapon, which has the effect of excluding them from law enforcement positions.

- Evidence of internal affairs checks for prior law enforcement or military positions; and
- Documentation of potentially derogatory issues identified in the investigation, such as material negative comments from a former employer, as needed.

We found that of the 89 employee and contractor files that we reviewed, 17 files did not include basic required documentation such as fingerprint checks, references from prior employers, and internal affairs checks from prior law enforcement positions. Human Resources Division officials told us that when they receive incomplete investigation files from OPM, the adjudicators attempt to obtain the missing documentation necessary for conducting an adjudication because they believe that would be faster than returning the incomplete files to OPM. Even with the adjudicators' efforts, 9 (14 percent) of the 66 employee background investigation files in our sample lacked required documentation. Four of the nine files contained statements from OPM saying that it had not obtained and would not attempt to obtain required information, including fingerprint checks and interviews with references. For non-CSO contractors, we found that OPM closed 8 (35 percent) of the 23 cases without obtaining required information. In four of those eight cases, OPM noted that responses to inquiries sent to references or requests for employment records had been "undeliverable"; in the other four cases, the information was missing without an explanation.

We also checked a separate sample of background investigation files for employees who incurred sustained misconduct charges to ascertain if there was a correlation between incomplete background investigations and misconduct. To create this sample, we selected 28 employees listed in the OIG Investigations Division's records as having committed misconduct, in most cases involving violence or threats, and obtained their background files. Of these files, 21 (75 percent) were missing at least one document. We took special note of the 19 deputy marshals among the 28 employees in this sample. Nine (47 percent) of these deputy marshals' background investigation files contained no evidence that the investigator or the adjudicator performed the required checks of the internal affairs records at the applicants' most recent law enforcement employers. Overall, the background investigation files of employees with misconduct charges were missing more documentation than those of USMS employees in our general sample. An incomplete file increases the possibility that the adjudicator will not be aware of all potentially derogatory issues in making a security approval recommendation.

Several USMS and SEPS officials raised concerns with us about the completeness of OPM field investigations. Their perception was that the completeness of field investigations was deteriorating because OPM did not provide adequate training and quality assurance monitoring for the new staff its contractors were hiring to cope with the increased demand for background investigations. When asked why they did not address completeness issues with OPM, the USMS and SEPS officials stated that they are part of relatively small entities and do not have leverage to influence OPM standards. When we asked the OPM Customer Service Group Chief about any problems with the completeness of investigations, he stated that OPM was not aware that the USMS had an issue with completeness and that problems should be brought to OPM's attention. He stated further that the rising demand for background investigations has created problems for OPM's contractors in recruiting and training staff. He said that OPM does conduct quality assurance reviews and that OPM expects that the experienced Department of Defense adjudicators being transferred to OPM in 2005 will also improve background investigations.

To further review the completeness issue, we compared the background investigation files of deputy marshals in the misconduct sample with those of the deputy marshals in our general sample of employees. We found that internal affairs checks were missing in 3 (12 percent) of the 26 files of the deputy marshals in the general employee sample compared with 9 (47 percent) of the 19 files for deputy marshals with sustained misconduct charges. We found that the Lautenberg statement was missing in 10 (38 percent) of the 26 files of the deputy marshals in the general employee sample compared with 12 (63 percent) of the 19 files for deputy marshals with sustained misconduct charges. Our data suggest that when the background investigation file is incomplete, the risk is greater that a security approval will be issued to an employee who subsequently engages in misconduct.

Derogatory issues addressed. The second aspect of thoroughness we examined was whether the USMS adjudicators applied OPM guidelines on evaluating potentially derogatory issues. These guidelines require adjudicators to analyze the type of position the applicant is to hold, the nature and seriousness of the derogatory issue, the length of time since it occurred, the circumstances that contributed to or mitigated the issue, and the assistance sought by the applicant in resolving the issue.[18] In our

[18] Additional considerations may include exacerbating or mitigating circumstances, the extent the act was pertinent to the individual case, statutory or regulatory bars, and the existence of material and intentional falsification.

sample review, we found that for all 84 files with completed USMS adjudications, the adjudicators followed OPM guidelines when addressing the potentially derogatory issues that had been documented.[19] For example:

- In each case involving an applicant's disclosure of prior drug use, the adjudicator confirmed that the use was minimal and not recent.
- In one case involving serious credit problems, the adjudicator determined that all delinquencies were related to a divorce, obtained the required 3-month history of timely payments, and only then recommended approval.
- In one case in which an applicant had been fired from a previous position for leaving a vault open, the adjudicator took into account that the incident occurred seven years earlier, that co-workers from that position recommended the applicant, and that the applicant was in a moderate-risk position without access to money or classified information.

USMS field managers sometimes requested that the Human Resources Division set aside adjudicators' recommendations that candidates not be given security approval and did not provide written justifications. In reviewing the 28 background investigation files of employees who had sustained misconduct charges, we found that the adjudicators had recommended that 3 of the employees not be granted security approval. In each of these cases, a Human Resources Division supervisor added a memorandum to the file presenting an argument that the derogatory information was not sufficiently serious to justify denying the individual a security approval. In all three cases, after security approval was granted the employees committed misconduct that resulted in discipline or removal.

When we asked about these cases, a senior Human Resources Division official said that he had received verbal pressure in at least one of these three cases from a high-level field manager and, in response, had written a memorandum arguing that security approval be granted despite the adjudicator's negative recommendation. He stated that it was not uncommon to receive input, usually by phone, from people outside his office who seek to influence decisions by the Human Resources Division on

[19] There were 66 cases in our USMS employee sample, 5 of which were adjudicated by SEPS (4 attorneys and a U.S. Marshal). There were 25 USMS contractors in our sample, 2 of whom did not have the completed OPM investigation in their files. Therefore, we reviewed 84 files in which it was possible to evaluate whether a USMS adjudicator addressed potentially derogatory information.

particular employees or applicants. This influence often comes from a U.S. Marshal in a district office who knows the applicant or employee personally. Unlike the files of those later cited for misconduct, the files in our general sample of 89 employees and contractors contained no Human Resources Division adjudicator recommendations against security approval. Of these 89 cases, none had sustained allegations involving violence or threats, criminal behavior, or other serious misconduct.[20] In one case, the adjudicator had made a recommendation for a temporary downgrade, which was still under consideration at the time of our review.

A few of the reinvestigations that the USMS is required to conduct every five years on a large portion of its personnel were overdue. USMS policy requires that it initiate reinvestigations every five years of employees and contractors in national security positions and of employees holding high- and moderate-risk public trust positions. This means that virtually all of its 4,000 employees and an undetermined number of contractors with national security duties must be reinvestigated every five years. In our sample of 66 files, we found only 2 instances in which reinvestigations were overdue.

In our general sample of employees, 54 of the 66 employees had worked for more than five years, and therefore required reinvestigation at least once. Of the 54, 47 (87 percent) had been reinvestigated within the required time, 5 (9 percent) had investigations that were more than five years old and had reinvestigations in progress at the time of our review, and 2 (4 percent) were overdue and had no reinvestigations in progress. In one of these two instances, the employee was in a national security position and the reinvestigation was two years overdue. In the other instance, the employee was in a moderate-risk public trust position and the reinvestigation was one year overdue. A USMS official stated that 18 reinvestigations currently were overdue, not just the 2 in our sample. He said that most of the cases were employees without national security clearances who were reluctant to submit the required documentation and often had to be asked repeatedly to do so, even to the extent of getting their supervisors to put pressure on them to complete this task.

[20] This includes the 66 employees and 23 contractors, including those with investigations conducted by other agencies, whose cases were adjudicated by the USMS Human Resources Division.

Of the 25 contractors in our sample, 6 had worked more than five years. Five of the contractors were in public trust positions, not national security positions, and the USMS was not required to reinvestigate them regardless of how long they had held their positions. One was in a national security position and had a current background investigation at the time he resigned.

We specifically looked at two areas where delays in initiating reinvestigations might have serious consequences: instances involving employee misconduct and instances in which security clearances lapse. In the first area, we found that a higher percentage of employees with sustained misconduct charges were overdue for reinvestigation than employees in our general sample. In our sample of 26 employees with sustained misconduct charges, 5 (19 percent) had been overdue for reinvestigation at the time the misconduct occurred. In six cases (23 percent), employees with two or more sustained allegations of misconduct during the previous five years were overdue for reinvestigation, indicating that although the USMS had reason to believe employees had problems, it had not pursued reinvestigations on a timely basis. In five of these six cases, issues related to later misconduct had already been identified at the time of the last investigation, and in the remaining case an allegation directly related to the misconduct had already been investigated but not substantiated. This pattern may indicate that the USMS is not tracking and placing priority on the reinvestigation of employees with identified behavioral problems.

Potential Results of Failing to Reinvestigate on Time

We found one example of particular concern – that of a supervisory deputy marshal who had not been reinvestigated for more than ten years despite several misconduct issues. His file indicated that he had been reinvestigated in July 1993 and was due for reinvestigation in 1998. His reinvestigation was not initiated until June 2004. In the intervening years, his peers had provided a signed statement alleging that, in addition to misconduct at work, he had been arrested on a statutory rape charge in December 1993. Two misconduct charges – one for employee violence, one for a non-violent arrest for driving while intoxicated – had been substantiated since 1999. His reinvestigation was still pending at the time we reviewed his background investigation file in July 2004. When asked about this particular case, a USMS official explained that the delay in performing a reinvestigation was not unusual because this employee did not have a national security clearance. Prior to 2001, few reinvestigations were done on employees who did not hold clearances and were not considered a priority. This employee was on extended sick leave and scheduled to retire in January 2005.

In examining the second area of consequences resulting from delayed reinvestigations, we asked USMS managers what they do when a security clearance expires and the reinvestigation has not been completed. They told us that they take the necessary steps to initiate reinvestigations, but will not suspend a clearance unless the holder of the clearance failed to submit

an application for reinvestigation. Of the 54 employees subject to reinvestigation, 32 had received a national security clearance. Four (13 percent) of these 32 employees were working with expired security clearances – their reinvestigations were incomplete or not yet begun. When asked whether these four employees were in positions that required access to national security information, the Chief of Human Resources Services stated that they were not. The file of one employee with a current reinvestigation showed that access to a secure database had been terminated when the previous clearance expired.

The background investigations of USMS employees managed by SEPS complied with regulations, and the field investigations and adjudications, while slow, were consistently thorough. SEPS managed the background investigation process for 127 USMS employees, including political appointees, attorneys, and other designated positions. SEPS relied on the FBI rather than OPM to conduct the field investigations. SEPS officials informed us that it is their policy to allow these applicants to enter on duty with a waiver and to complete the background investigation process after they begin work. We noted that of the 14 random sample employees for whom the SEPS investigation was their first at the USMS, all had a completed FBI investigation as well as a waiver before they entered on duty, which exceeds requirements. The FBI field investigations in our sample averaged 115 days to complete. The SEPS adjudications exceeded the 90-day timeliness requirement, averaging 180 days to complete.

The FBI investigations were consistently thorough. Of the 26 files we reviewed, less than 10 percent were missing credit check authorizations or evidence that routine law enforcement database checks had been conducted. The remaining documentation was complete, and FBI investigators consistently followed up on potentially derogatory issues raised through document checks and interviews with associates.

SEPS adjudications also consistently addressed potentially derogatory information identified during investigations. In the 26 sample case files we reviewed, 16 (62 percent) contained potentially derogatory issues, most often related to financial problems or lawsuits filed against U.S. Marshals when they served in a prior official law enforcement capacity. The adjudicator addressed the financial issues or lawsuits and determined that the issues were resolved, settlements were reached, or the applicant was not personally responsible for the issues raised in the lawsuit. We found no political appointees or attorneys in the misconduct cases we reviewed.

COURT SECURITY OFFICERS

In accordance with its policy, the USMS initiated the background investigation process before CSOs entered on duty and prohibited CSOs from starting work before at least an interim approval was issued. We found, however, that the Judicial Security Division issued interim approvals to CSOs based on incomplete information. Documentation, including criminal history-related information, was missing from some of the background investigation files for CSOs whose hiring had been approved. For approximately half of the CSOs we reviewed, the Judicial Security Division did not obtain credit checks. In addition, the Judicial Security Division did not verify medical suitability in cases where it requested additional medical information. Although CSOs served in law enforcement positions and carried firearms, the Judicial Security Division decided as a policy matter not to reinvestigate them routinely.

The USMS complied with its policy requiring it to initiate the background investigation process before CSOs entered on duty. The USMS policy governing the hiring of CSOs differs from the policy that applies to USMS employees and non-CSO contractors. The CSO policy requires that the Judicial Security Division initiate the background investigation process before a CSO enters on duty. If the process cannot be completed before the CSO is needed on the job, the Judicial Security Division must assess a subset of the documentation required for a background investigation to determine whether an interim approval can be issued to allow the CSO to begin work while the background investigation proceeds.

For the 33 CSOs in our sample, the Judicial Security Division initiated 32 investigations before the CSOs entered on duty and completed the background investigation process for 26 of them. The files for the six remaining CSOs contained interim approvals. One file – that of a CSO hired in 1985 – showed that the background investigation process was not initiated and that no interim approval had been issued at the time of his hiring, although that background investigation was subsequently completed within the year.

The Judicial Security Division issued interim approvals to CSOs based on incomplete information. USMS policy requires that the following information be included in a CSO's background investigation file before the Judicial Security Division considers issuing an interim approval:

- A positive recommendation from the CSO's previous supervisor,
- A medical examination showing no obvious medical issues,
- An FBI National Crime Information Center (NCIC) check reflecting no police record,[21] and
- An internal affairs check showing no serious problems at the CSO's previous place of employment.

We found that the Judicial Security Division issued some interim approvals without obtaining all of the required information. Of the six interim approvals that Judicial Security Division granted to CSOs in our sample, all were missing a recommendation from the previous supervisor, and four were missing at least one of the other required documents listed above.

Field investigations were slower than required by Judicial Security Division policy, but adjudications were consistently timely. USMS Directive 10.38 states that a CSO background investigation must be conducted within 21 days after the request is received at the district office. In our sample, deputy marshals averaged 63 days to complete the investigation. We found the adjudications conducted by the Judicial Security Division averaged 68 days. When we asked about the slow investigations, Judicial Security Division management acknowledged that the time required to complete investigations varies by district due to size and resource differences. In addition, investigations of applicants with long careers, and particularly those with military service, require more time.

Required documentation was missing from CSO background investigation files. In reviewing 33 CSO files, we considered a file thorough if it contained the documentation required by the USMS listed in Table 5 and the documentation itself was complete. We also considered a file thorough if a document was missing but written evidence in the file showed it had existed (for instance, a note to the file documenting the date that an FBI fingerprint or name check was completed).

[21] The FBI's NCIC is a computerized index of criminal justice information (e.g., information on criminal records, fugitives, stolen property, missing persons), which is available to federal, state, and local law enforcement and other criminal justice agencies.

Table 5: Required Documents for CSO Field Investigations

Required Documents	Evidence in File	Percentage of Total
Law enforcement certificate	32	97%
USM-234: Personnel qualification statement	31	94%
OPM/USMS background investigation	31	94%
USM-333: Weapons authorization	30	91%
CSO-010 (identifies the CSO, the applicant the CSO would replace, EOD date, etc.)	29	88%
FBI National Crime Information Center (NCIC) check	29	88%
USM-229: Authorization for a medical records search	29	88%
Memo from field investigator with a background investigation summary	26	79%
Internal affairs check	25	76%
Lautenberg statement	24	73%
Preliminary contractor background investigation	24	73%
Memo from HQ showing final approval	24	73%
FBI fingerprint check	22	67%

Source: CSO sample file review

[a] The Lautenberg Amendment (18 U.S.C. § 922(d)(9), (g)(9)), enacted in September 1996 and effective retroactively, bans individuals convicted in any court of a misdemeanor crime of domestic violence from carrying a weapon, which effectively excludes them from law enforcement positions. CSO applicants must sign a Lautenberg statement indicating they have not been convicted of a misdemeanor crime of domestic violence.

[b] Thirty-two files contained fingerprint cards, but ten of those files lacked proof that an FBI fingerprint check had been conducted. We accepted various forms of proof including a dated note by the adjudicator in a case summary, a dated FBI facsimile or fingerprint check printout, an FBI stamped confirmation letter, or a statement verifying the fingerprint check within the deputy investigator's background investigation case summary.

We regarded documents related to criminal history and misconduct most important because the CSOs serve in law enforcement positions. Our sample review indicated that required documents related to criminal history - such as FBI fingerprint checks, Lautenberg statements, and internal affairs checks – were missing from about a quarter to about a third of the 33 files:

- Thirty-two files contained FBI fingerprint cards, but only ten (31 percent) contained any evidence that the FBI had conducted the fingerprint checks for which the cards were to be used.[22]
- Nine (27 percent) files were missing Lautenberg statements from the applicants regarding any past convictions for misdemeanor crimes of domestic violence.[23]
- Eight (24 percent) of the files were missing evidence of internal affairs checks, which can reveal issues that arose during applicants' previous law enforcement jobs, including trustworthiness issues and misconduct exhibited with co-workers or the public.[24]

We also found instances in which required documentation was present but incomplete. For example, the personal qualification statement (USM-234) was present and filled out in 94 percent of the files, but eight of the statements (26 percent) had no date, and three (10 percent) had forms on which the date, signature, or both had been taped over or "whited out." A Judicial Security Division official confirmed that the form should be dated at the time it is submitted and said Judicial Security Division managers were unaware of the omissions. Neither we nor the Judicial Security Division could identify any advantage that the Judicial Security Division, the contracting organization, or the applicant gained from these omissions and changes. Undated documents, however, are not valid, and deleting a signature is of particular concern if the form authorized inquiries into personal information (for example, medical and credit checks) or affirmed that the information provided was true. We concluded that some files in our sample did not provide legal authorization for personnel inquiries or affirmations that the applicants had provided truthful information for the background investigation.

Furthermore, the Judicial Security Division did not consistently follow its policy for conducting credit checks and verifying medical suitability. For approximately half of the CSOs in our sample, the Judicial Security Division did not obtain credit checks as required by USMS Directive 10.39(9). Of the 33 files we reviewed, only 16 (48 percent) files contained evidence that a credit check had been conducted. Those credit checks had been performed

[22] Background investigations conducted after 1997 showed FBI fingerprint checks in 84 percent of the files.

[23] Background investigations conducted after 1997 showed Lautenberg statements in 92 percent of the files.

[24] Background investigations conducted after 1997 showed internal affairs checks in 84 percent of the files.

at the district level, not at the headquarters level. A Judicial Security Division manager said that the USMS relies on the financial information applicants provide on the USM-234 form and follows up with credit checks if applicants disclose significant financial problems, such as bankruptcy.

We also determined that Judicial Security Division management does not consistently follow up on issues raised by the medical suitability reviews used to assess whether applicants are physically capable of fulfilling CSO responsibilities. In our sample of 33 files, 18 (55 percent) referred to medical issues that required additional information to meet Judicial Security Division standards. Each contained a memorandum to the prime contractor requesting additional medical information, but only 9 of the 18 files contained a memorandum from Judicial Security Division management certifying that the CSO was medically suitable for a CSO position. Although Judicial Security Division officials reported that they reject CSO applicants most often for medical reasons, we could find no evidence that they followed up on the medical issues in half of our sample files for which the Judicial Security Division requested additional medical information.

Although CSOs serve in law enforcement positions and carry firearms, the Judicial Security Division does not routinely reinvestigate them. Neither regulations nor Department policy requires routine reinvestigation of contractors in public trust positions. However, CSOs carry firearms, protect judges, and have unescorted access to court facilities. The Judicial Security Division currently reinvestigates CSOs only if it becomes aware of misconduct issues that required disciplinary action. The Judicial Security Division's data showed that 2,208 (51 percent) of its current 4,323 CSOs had been employed for five or more years. See Table 6 for details on the length of CSOs' service. We believe that CSOs should be reinvestigated routinely every five years to ensure that USMS can identify issues that could lead to misconduct.

Table 6: CSOs' Length of Service

Years of Service	Number of CSOs	Percentage
5 years or less	2,115	49%
5 years to 10 years	1,478	51%
10 years to 15 years	511	
15 years to 20 years	219	
Total	**4,323**	**100%**

Source: Judicial Security Division database

CONCLUSION

An effective background investigation program reduces the risk that an agency will hire or retain unsuitable employees and contractors. To be effective, a program must have policies that provide direction on agency compliance with federal regulations and agency personnel security requirements and should consistently produce thorough and timely background investigations. In addition, a program must be supported by adequate data systems. By addressing the issues identified in this report, we believe that the USMS can better ensure that its background investigation program meets these basic goals.

Our review concluded that the USMS does not have adequate written policies and procedures to guide its background investigation program. The most recent USMS policy guidance -- issued in 1995 -- was incomplete, and the draft 2001 update was never completed. In addition, the USMS did not have detailed written procedures for the routine administration of its program.

The USMS databases for tracking and managing background investigations varied in quality. While the Judicial Security Division database for contract CSOs was adequate for monitoring the status of background investigations, the Human Resources Division databases for employees and non-CSO contractors were not sufficiently accurate or complete for monitoring purposes.

We found that although OPM and USMS deputy marshals were slow in completing field investigations of USMS employees and contractors, the USMS adjudicators in both the Human Resources Division and the Judicial Security Division generally met regulatory timelines. SEPS adjudications, however, of USMS political appointees, attorneys, and other designated personnel were not timely.

We found that adjudicators consistently addressed derogatory issues identified in the background investigation file, but the adjudicators were making decisions based on incomplete investigations. Neither OPM nor USMS investigators consistently provided all required interviews and documentation, and there was no written guidance on processing cases when the OPM or USMS investigation was incomplete or inadequate. Nor

did the USMS collect the information necessary to provide OPM with evidence of inadequate investigations.

The process for hiring or retaining employees whom adjudicators have found unsuitable is not transparent. The Human Resources Division did not require field managers to provide written justifications when they wanted to hire or retain individuals despite adjudicators' negative recommendations, so they were not held accountable when such an individual later engaged in misconduct.

While USMS policy requires that public trust employees who carry weapons and perform law enforcement or guard duties be routinely reinvestigated every five years, contract CSOs and other contractors who carry weapons and, in effect, perform law enforcement functions, are not routinely reinvestigated.

RECOMMENDATIONS

We make seven recommendations to help the USMS ensure that its background investigation program identifies applicants and employees who are not suitable for national security and public trust positions. The recommendations focus on revising policies and procedures, upgrading the databases that are used to manage background investigations, improving the thoroughness of adjudications, developing controls to monitor the background investigation process, and requiring that contractors fulfilling law enforcement duties be reinvestigated. We recommend that the USMS take the following actions:

1. Revise and formally adopt written policies and procedures that address all aspects of the background investigation process to reflect current federal regulations and Department policy.

2. Develop an adequate structure for the Human Resources Division database to ensure that essential data are not overwritten and to enable both the Human Resources Division and the Judicial Security Division to monitor compliance with regulations and Department policy.

3. Implement procedures to routinely review the accuracy of the databases that the Human Resources Division and the Judicial Security Division use to manage the background investigation program.

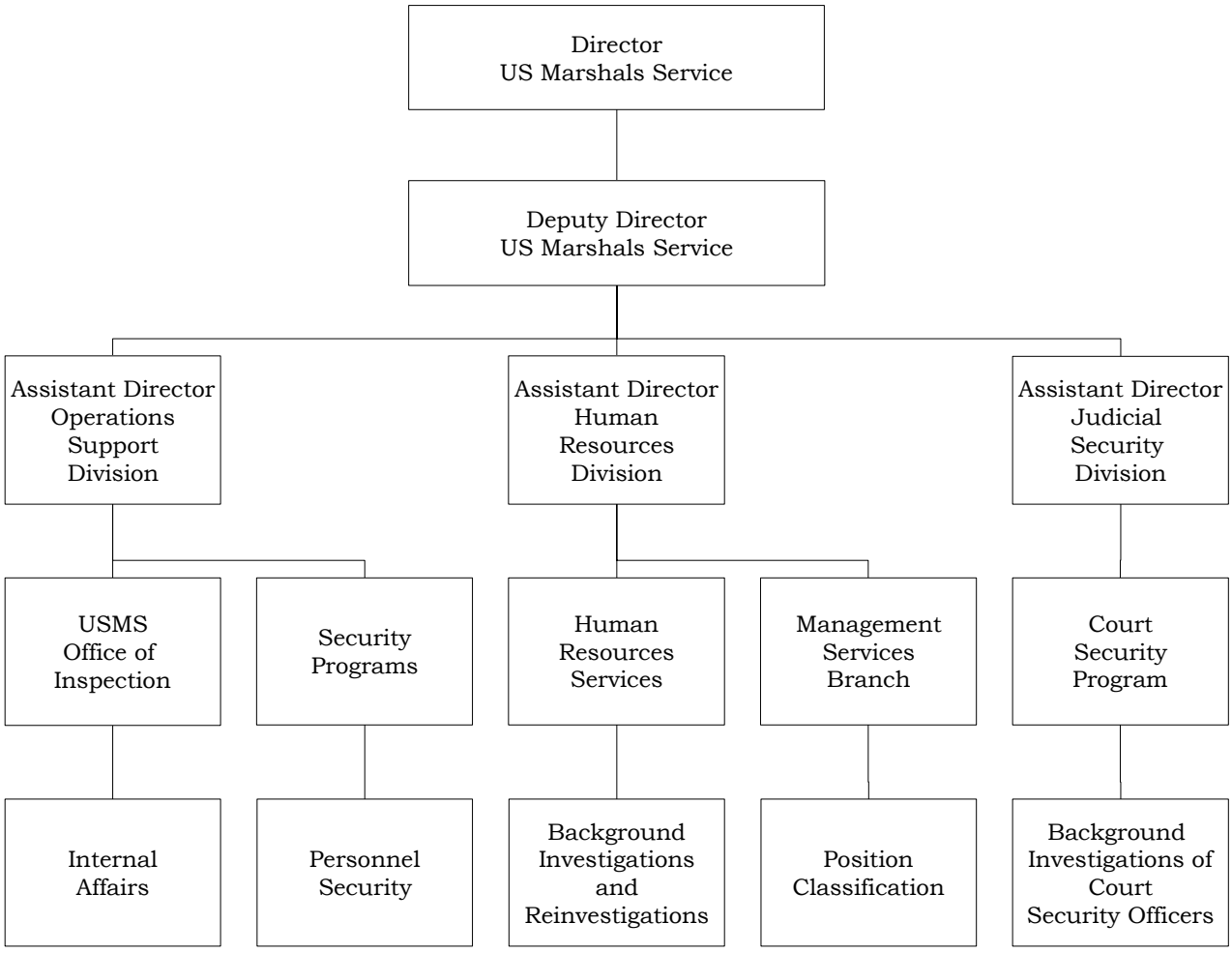
4. Require periodic written reviews on the efficiency and effectiveness of the background investigation program to determine if process improvements are needed.

5. Develop guidelines for adjudicators that include instructions on how to proceed when an OPM investigation is incomplete and criteria for recommending security approvals and disapprovals that are consistent with OPM and Department policy.

6. Require that the Chief of Human Resources Services fully document comments from field managers on an adjudicator's recommendation regarding a security approval for an applicant or employee.

7. Require reinvestigations every five years for contractors who are assigned law enforcement duties.

APPENDIX I: USMS UNITS WITH PERSONNEL SECURITY RESPONSIBILITIES



Source: SEPS and USMS materials

APPENDIX II: SCOPE AND METHODOLOGY

SCOPE

We reviewed the process for all background investigations and reinvestigations of employees, CSOs, and other contractors whose field investigations are adjudicated by USMS headquarters personnel in either the Human Resources Division or the Judicial Security Division. We did not review low-risk contractors whose field investigations and adjudications are conducted at the district office level.

METHODOLOGY

Specifically, we reviewed policies and procedures, interviewed officials involved in the process, and analyzed selected files to determine whether the USMS provides timely and thorough background investigations and reinvestigations that comply with federal regulations and Department policy for its employees and contractors.

Interviews

We conducted 21 interviews, listed below, at USMS headquarters in Arlington, Virginia, and at SEPS's offices in Washington, D.C.

USMS Headquarters

- Human Resources Division
  - Chief of Human Resources Services
  - Chief of the Operational Security Branch, Human Resources Services
  - Chief of the Personnel Security Branch, Human Resources Services
  - Acting Assistant Director, Management Services Branch
  - Chief of Adjudications, Human Resources Services
  - Two Personnel Security Specialists (adjudicators), Human Resources Services
- Operations Support Division
  - Chief Inspector for Internal Affairs

- Judicial Security Division
  - Chief of the Judicial Protective Service
  - Chief Inspector of the Judicial Security Division
  - Senior Inspector
  - Information Technology Administrator

SEPS

- Personnel Security Group
  - Assistant Director
  - Chief of Operations Security
  - Personnel Security Specialist, Information & Technical Security Group
  - Personnel Security Specialists, Policy Section
- Compliance Review Group
  - Senior Security Specialist
  - Policy Analyst

Office of the Inspector General

  - Two OIG Supervisory Investigative Agents, OIG Investigations Division
  - Office of Human Resources Specialist

Other Government Officials

  - OPM Training Officer
  - OPM Customer Service Group Chief
  - National Finance Center Data Analyst

Data and Sample File Reviews

The USMS Human Resources Division, the Judicial Security Division, SEPS, and the OIG Investigations Division provided us with data from five databases, described below. Because of the poor quality of data in the two USMS Human Resources Division databases for employees and contractors,

projections cannot be made from the statistics generated from these databases.

We used these databases for four purposes: 1) to evaluate the quality and completeness of data; 2) to generate random and judgmental sample files for review; 3) to determine the adjudications workload in recent years; and 4) to determine the databases' usefulness for case tracking and program management.

USMS Employees

The Human Resources Division provided us with a copy of its Microsoft Access employee database, as of March 2004, that the Human Resources Division uses to track background investigations and reinvestigations of current employees. The database contains 41 fields to record biographical data, position and clearance data, key event dates for processing investigations, the type of investigation requested, and its cost. We started with the full database of 7,309 entries and refined it to include only entries with an entered-on-duty date, or 4,424 entries.[25] We chose the entered-on-duty date because we were told that data field would identify active employees. Therefore, the database statistics on USMS employees provided in this review were derived from the universe of the 4,424 database entries with entered-on-duty dates on the date the database was obtained (March 2004).

In March 2004, SEPS provided us with specified fields for the 127 USMS employees it manages in its database, TRAQ. We used this database to generate a random sample of 26 files to review the timeliness and thoroughness of investigations and adjudications for USMS political appointees, attorneys, and other designated employees.

To conduct our sample file review, we generated a random sample of 66 cases from the universe of 4,424 employees.[26] We prepared a checklist for our review of each case file and used the information on the checklist to assess the thoroughness of OPM investigations and USMS adjudications and to determine compliance with USMS policy.

[25] The remaining 2,885 cases did not have entered-on-duty dates because they were in various stages of the investigation and hiring process.

[26] Over 75 percent of USMS employees occupy law enforcement positions. To ensure that we reviewed a sufficient number of employees who were not in law enforcement positions, including a range of positions and clearance levels, we separated the two caseloads and generated separate random samples of 33 cases each.

USMS Contractors (Excluding CSOs)

The Human Resources Division provided us with a copy of its Microsoft Access contractor database, as of March 2004, that the Human Resources Division used to track background investigations and reinvestigations of current contractors. The database fields are identical to those in the employee database. We started with the full database of 8,844 entries and refined it to include only entries with an entered-on-duty date, or 5,335 entries.[27] We used these 5,335 entries to select a random sample of 33 contract guards and a random sample of 25 other contractors, for a total of 58 review files.[28]

Of the 58 contractor files we requested for our sample review, the USMS was able to locate 25 of the files at headquarters. We used those files to evaluate compliance with federal and Department regulations and the thoroughness of investigations and adjudications. The remaining 33 contractors had been hired at the local level without adjudication at headquarters, so their files were stored in various districts or could not be located. We did not review the files stored at the districts.

Court Security Officers

The Judicial Security Division provided a list (and later a copy of the Judicial Security Division Oracle database) of the 4,323 contract CSOs as of May 2004. We used these cases to generate a random sample of 33 background investigation files to evaluate the thoroughness of CSO investigations and adjudications.[29]

[27] The remaining 3,509 cases did not have entered-on-duty dates and were not included in the random sample because there was insufficient information to determine their current status.

[28] There were 5,233 contract guards with entered-on-duty dates and only 102 other contractors. To ensure that we reviewed a sufficient number of contractors who were not contract guards, including some who had received national security clearances, we separated the two caseloads and generated separate random samples of 33 contract guards and 25 other contractors.

[29] Because all CSOs nationwide have the same responsibilities and are investigated and adjudicated to the same standard, we did not need to create a separate random sample within this caseload. Thirty-three files were necessary for a review of 4,323 cases at the 90 percent confidence rate.

Misconduct Cases

The OIG Investigations Division provided a copy of the Investigations Data Management System (IDMS) database, which contained all USMS misconduct allegations made from fiscal year (FY) 2000 through April 2004, against USMS employees and contractors. We used the database to create a judgmental sample of 42 cases for the file review. These cases fell into three categories:

- Cases specifically mentioned during interviews with USMS staff;
- Cases that resulted in a criminal sentence, termination, or retirement, regardless of the nature of the misconduct; and
- All cases in which there was an allegation of violence, a threat of violence, or harassment involving domestic relationships, colleagues, the public, or prisoners.[30]

We requested from the USMS Office of Internal Affairs the case dispositions of the 42 cases that had met at least one of our criteria, and we determined that 29 (28 employees and 1 contractor) had misconduct allegations that were sustained. There were no political appointees, attorneys, or CSOs who met our criteria, so the sample did not include anyone from these categories. Statistics are based on these 29 cases or a subset of these cases.

These 29 sample misconduct files were used for three purposes: 1) to review the thoroughness of the background investigations and whether reinvestigations were initiated within five years; 2) to evaluate whether there was any relationship between the thoroughness of the background investigations and reinvestigations and subsequent sustained misconduct allegations; and 3) to determine whether reinvestigations of these individuals at the five-year deadline might have identified a problem before it led to a misconduct investigation.

Other Sources

We reviewed federal regulations, Central Intelligence Agency directives, OPM and SEPS guidance, OPM and USMS policy and procedures manuals, training materials, checklists, and the most recent USMS Office of Internal Affairs report (FY 2001). We also obtained relevant portions of a standard CSO contract from the Judicial Security Division.

[30] We chose these files based on the misconduct codes used by the OIG Investigations Division.

APPENDIX III: ACRONYMS

BI	Background investigation
CY	Calendar year (January 1 to December 31)
CDUSM	Chief Deputy Marshal
CFR	Code of Federal Regulations
CSO	Contract court security officers
DHS	Department of Homeland Security
DUSM	Deputy marshal
EOD	Enter on duty date
FBI	Federal Bureau of Investigation
FY	Fiscal year (October 1 to September 30)
HRD	Human Resources Division
IDMS	Investigations Data Management System
JSD	Judicial Security Division
NCIC	National Crime Information Center
NSI	National Security Information
OIG	Office of the Inspector General
OPM	Office of Personnel Management
RI	Reinvestigation
SCI	Sensitive Compartmented Information
SEPS	Security and Emergency Planning Staff
USC	United States Code
USMS	United States Marshals Service

APPENDIX IV: THE USMS'S RESPONSE

U.S. Department of Justice

United States Marshals Service

Office of the Director

Washington, DC 2O53O-1000

February 3, 2005

MEMORANDUM TO: Paul A.Price
Assistant lnspector General for
Evaluation and Inspections

(original signed)
FROM: Benigno G. Reyna
Director

SUBJECT: Response to Draft Evaluation Report - United States Marshals Service's Background Investigations
Assignment Number A-2004-007

Thank you for the opportunity to comment on the draft evaluation report entitled: United States Marshals Service's Background Investigations. We have reviewed the recommendations contained in the report, and our comments are attached.

Regarding any concerns relative to proprietary, confidential, or personal information that should not be released to the general public, our Office of General Counsel's sensitivity review of the draft report has revealed that the report does not contain any information within the definition of Limited Official Use (LOU) set out in DOJ Order No. 2620-7, September 1, 1982, or any information within the definitions of classified information set out in Executive Orders No. 12958 (April 17, 1995) and No. 13292 (March 25, 2003), and in the DOJ Security Programs Operating Manual, revised November 4, 2004.

Should you have any questions or concerns regarding this report, please contact Isabel Howell, Audit Liaison at 202-307-9744.

Attachment

cc: Suzanne Smith
Assistant Director
Human Resources Division

Richard P. Theis
Acting Director
DOJ Audit Liaison Office

United States Marshals Service Response to OIG Draft Report:
The United States Marshals Service's Background Investigations

Recommendation I:

Revise and formally adopt written policies and procedures that address all aspects of the background investigation process to reflect current federal regulations and Department policy.

USMS Response: ***(Agree)*** The USMS is currently revising the Personnel Security policy Ii is expected that the revised policy will be implemented no later than April 30. 2005.

Recommendation 2:

Develop an adequate database structure for the Human Resources Division to ensure that essential data are not overwritten and to enable both the Human Resources Division and Judicial Security Division to monitor compliance with regulations and Department policy.

USMS Response: ***(Agree)*** The Human Resources Division (HRD) has revised its database to consolidate all contractor and employee records (with the exception of Court Security Officer (CSO) records) into one database. By March 15, 2005, the database structure will be modified to include the additional data field recommended by the OIG in order to comply with applicable policy and regulations.

Recommendation 3:

Implement procedures to routinely review the accuracy of the databases that the Human Resources Division and Judicial Security Division use to manage the background investigation program.

USMS Response: ***(Agree)*** The Judicial Security Division will develop and implement ***a*** monthly database report which will identify all CSO's with a background investigation or record check that is older than five years. The results of these reports will be forwarded to the districts with a request for a record check. We anticipate that the districts will complete the first set of identified record checks by April 1, 2005, and that the CSO database will be updated accordingly by *May* 1.2005.

The Human Resources Division has requested that USMS Information Technology Services (ITS) develop a program which will match against other databases, including the National Finance Center payroll system, to ensure that the most current data is available. Our goal is to implement this program by September 30. 2005.

Recommendation 4:

Require periodic written reviews on the efficiency and effectiveness of the background Investigations program to determine if process Improvements are needed.

USMS Response: ***(Agree)*** The USMS is currently requiring that all programs conduct a periodic self inspection to ensure that procedures arc adequate and that any deficiencies are corrected. The self-inspection criteria will be provided to OIG by March 15, 2005.

Recommendation 5:

Develop guidelines for adjudicators that include instructions on how to proceed when an OPM investigation is incomplete and criteria for recommending security approvals and disapprovals that are consistent with OPI and Department policy.

USMS Response: (*Agree)* By March IS, 2005, the Standard Operating Procedures (SOP) will be updated from the existing 2001 SOP to provide adjudicators additional guidance for completing personnel security determinations.

Recommendation 6:

Require that the Chief of Human Resources Services fully documents comments from field managers on an adjudicator's recommendation regarding a security approval for an applicant or employee.

USMS Response: (*Agree.)* The Chief of Human Resources Services has documented in the past and will continue to document any and all substantive information received from USMS managers regarding suitability issues of which the manager has first hand knowledge, or can provide lead information to facilitate the background investigation. Endorsements from field managers not having the benefit of direct knowledge of the issues involved in an investigation will continue to be viewed as having no beneficial impact upon the outcome of the suitability or security determination rendered by the Human Resources Division, and will not be incorporated into the file.

Recommendation 7:

Require reinvestigations every five years for contractors who are assigned law enforcement duties.

USMS Response: ***(Agree)*** It should be noted that the DOJ SEPS office guidance for contract employees does not require reinvestigation and leaves determinations for additional checks to the discretion of the program managers. In addition, the Courts do not currently require background investigations of their employees, other than those serving in probation and pre-trial services.

However, because CSOs perform armed facility security functions (such as screening attorneys, jurors, and visitors to court facilities). JSD will request district offices to conduct a criminal records check on each CSO hired before January 2000. The results will be forwarded to Headquarters and entered into a newly created data field. Positive results will be referred to the contractor for investigation and consideration of contract performance violations. JSD expects to complete these checks by April 2005.

APPENDIX V: THE OIG'S ANALYSIS OF THE UNITED STATES MARSHALS SERVICE RESPONSE

On January 10, 2005, the Office of the Inspector General (OIG) sent copies of the draft report to the Director of the United States Marshals Service (USMS) with a request for written comments. The Director provided the USMS's final written comments to us in a memorandum dated February 3, 2005.

The USMS concurred with all seven of the OIG recommendations; however, the actions that the USMS proposed to address three recommendations are not sufficient. The response to our recommendation to improve the accuracy of the databases the USMS uses to manage the background investigations program described actions that strengthen the databases, but will not correct the problems of inaccurate and missing data. Also, we recommended that all comments by managers regarding an adjudicator's recommendation be documented in the file so all information is available to decision-makers. However, the USMS indicated that the Chief of Human Resources Services would selectively document managers' input. In addition, we recommended that court security officers (CSOs) be reinvestigated every five years because they have security duties and they carry weapons. The OIG made this recommendation to ensure that contractors who have security duties are reinvestigated in a manner similar to Department employees whose duties include security. The USMS stated that it would conduct a criminal records check on CSOs every five years, but did not agree to conduct background reinvestigations on these CSOs. It remains the OIG's position that the reinvestigation should also include the checks and interviews that the Department requires for employees with similar responsibilities: law enforcement, credit, and national agency checks (e.g., National Crime Information Center, National Law Enforcement Telecommunications System); personal interviews; and interviews with references.

Following is an analysis of each USMS response to the report's seven recommendations.

RECOMMENDATIONS

Recommendation 1: Revise and formally adopt written policies and procedures that address all aspects of the background investigation process to reflect current federal regulations and Department policy.

Status: Resolved – Open

Summary of USMS's Response: The USMS is revising its Personnel Security policy and expects to implement it by April 30, 2005.

OIG's Analysis: The action described by the USMS is responsive to our recommendation. By May 2, 2005, provide a complete copy of the revised Personnel Security policy and procedures to guide policy implementation, that reflect current federal regulations and Department policy pertaining to the background investigation process.

Recommendation 2: Develop an adequate database structure for the Human Resources Division to ensure that essential data are not overwritten and to enable both the Human Resources Division and Judicial Security Division to monitor compliance with regulations and Department policy.

Status: Resolved – Open

Summary of USMS's Response: The USMS Human Resource Division has consolidated all contractor and employee records (except those of court security officers) into a single database. Further modifications will be made by March 15, 2005, to comply with policy and regulations.

OIG's Analysis: The action described by the USMS is responsive to our recommendation. By May 2, 2005, provide a description of the changes that have been made to the database.

Recommendation 3: Implement procedures to routinely review the accuracy of the databases that the Human Resources Division and Judicial Security Division use to manage the background investigation program.

Status: Unresolved

Summary of USMS's Response: The Judicial Security Division will implement a monthly database report identifying all CSOs with background investigations or records checks that are more than five years old. Requests for record checks on these identified personnel will be sent to the districts. The initial record checks will be completed by April 1, 2005, and the database will be updated by May 1, 2005.

By September 30, 2005, the USMS Information Technology Services will develop a program to match the Human Resources database to other

databases, including the National Finance Center payroll system, to ensure that the most current information is available.

OIG's Analysis: The actions described by the USMS are partially responsive to our recommendation and will strengthen the USMS databases. However, these actions do not address the deficiency noted in our report concerning the databases unacceptably high level of inaccurate or missing data (see page 15). By May 2, 2005, provide a description of procedures that have been implemented requiring routine review of these databases to ensure that the data fields contain accurate and complete data.

Recommendation 4: Require periodic written reviews on the efficiency and effectiveness of the background investigations program to determine if process improvements are needed.

Status: Resolved – Open

Summary of USMS's Response: The USMS will require that all programs perform a periodic self-inspection to evaluate the adequacy of procedures, and will correct deficiencies. The self-inspection criteria will be provided to the OIG by March 15, 2005.

OIG's Analysis: The action described by the USMS is responsive to our recommendation. By May 2, 2005, provide a copy of the criteria, procedures and schedule for conducting the self-inspections.

Recommendation 5: Develop guidelines for adjudicators that include instructions on how to proceed when an Office of Personnel and Management (OPM) investigation is incomplete and criteria for recommending security approvals and disapprovals that are consistent with OPM and Department policy.

Status: Resolved – Open

Summary of USMS's Response: In the procedures required under Recommendation 1 due on May 2, 2005, the USMS will include guidance to adjudicators on the requisite steps to take when an incomplete investigation file is received from OPM.

OIG's Analysis: The action described by the USMS is responsive to our recommendation. Provide a copy of the updated procedures by May 2, 2005.

Recommendation 6: Require that the Chief of Human Resources Services fully document comments from field managers on an adjudicator's recommendation regarding a security approval for an applicant or employee.

Status: Unresolved

Summary of USMS's Response: The Chief of Human Resources Services will continue to document any and all substantive information based on direct knowledge received from managers that impact the background investigation process. Endorsements not based on direct knowledge of the issues will have no bearing on suitability determinations and will not be included in the file.

OIG's Analysis: The action described by the USMS is partially responsive to our recommendation. However, contrary to the USMS's response that it documents all substantive information that affects the background investigation process, our review found instances in which the Chief of Human Resources Services received verbal pressure from field managers regarding an adjudicator's recommendation that was not recorded in the background investigation file. Decision-makers should have a complete file available when making or reviewing security approval decisions. To ensure accountability, all comments and information, regardless of whether derived from direct or indirect knowledge, received from managers regarding an adjudicator's recommendation should be documented. The policy and procedures for the background investigation process required by Recommendation 1 should include a requirement that all input received from managers on an adjudicator's recommendations must be documented by the Chief of Human Resources Services.

Recommendation 7: Require reinvestigations every five years for contractors who are assigned law enforcement duties.

Status: Resolved – Open

Summary of USMS's Response: The Department's Security and Emergency Planning Staff guidance does not require reinvestigation for contract employees and courts do not require reinvestigations for employees, except for those in probation and pre-trial services. However, because CSOs perform facility security functions and carry weapons, a criminal records check will be performed on CSOs hired before January 2000. The result will be entered into a newly created database field.

Positive results will be considered for possible contract performance violations. These checks are expected to be completed by April 2005.

OIG's Analysis: The action described by the USMS is partially responsive to our recommendation. However, we believe that CSOs, because they are armed and have full access to federal court facilities, should be reinvestigated every five years, in a manner similar to the minimum checks for Department of Justice employees who are assigned security duties and carry weapons. These reinvestigation checks include: law enforcement, credit, and national agency checks (e.g., National Crime Information Center, National Law Enforcement Telecommunications System); personal interviews; and interviews with three references.