AUDIT OF THE UNITED STATES MARSHALS SERVICE'S OVERSIGHT OF ITS JUDICIAL FACILITIES SECURITY PROGRAM

U.S. Department of Justice
Office of the Inspector General
Audit Division

Audit Report 11-02
November 2010

This page intentionally left blank.

AUDIT OF THE UNITED STATES MARSHALS SERVICE'S OVERSIGHT OF ITS JUDICIAL FACILITIES SECURITY PROGRAM

EXECUTIVE SUMMARY

The United States Marshals Service (USMS) is the primary provider of court security services to the federal judiciary. The USMS's Judicial Facilities Security Program, which is administered by USMS headquarters and funded by the federal judiciary, provides 2 main services to more than 400 U.S. federal court facilities nationwide: (1) court security officers (CSO), and (2) security systems and equipment, including X-ray machines, surveillance cameras, duress alarms, and judicial chambers entry control devices. The CSOs deployed by the USMS to federal court facilities are contract workers procured through contracts with private security firms in each of the 12 federal judicial circuits. As of June 2010, over 5,000 CSOs were assigned to federal court facilities throughout the United States. As with CSOs, the security systems obtained by the USMS are also obtained through a contract with a private security provider. The USMS seeks to ensure the safety of federal court facilities and judicial proceedings through the use of the CSO program and the security systems it deploys. In fiscal year (FY) 2009, approximately $370 million were allocated by the federal judiciary for the USMS's court security services.

The USMS's Judicial Security Division is primarily responsible for administering the Judicial Facilities Security Program, including management and oversight of the CSO program, USMS security systems, and related contracts. According to the USMS, CSOs are experienced former law enforcement officers who receive limited deputations as special Deputy U.S. Marshals. Using USMS security screening systems CSOs are responsible for detecting and intercepting weapons and other prohibited items from individuals attempting to bring them into federal courthouses. Along with Deputy U.S. Marshals, CSOs also assist in providing security at facilities that house federal court operations.[1]

[1] Deputy U.S. Marshals are full-time USMS employees who carry out multiple missions including, apprehending federal fugitives, protecting the federal judiciary, operating the USMS's Witness Security Program, transporting federal prisoners, and seizing property acquired by criminals through illegal activities.

OIG Audit Approach

The objective of this audit was to assess the USMS's oversight of its Judicial Facilities Security Program. To accomplish our objective, we interviewed USMS headquarters officials, reviewed USMS policies and procedures, and obtained and analyzed data pertinent to the USMS's court security programs, including a review of CSO personnel files. We also reviewed the procurement process for a CSO contractor whose contract was later terminated. Additionally, we conducted field work at six USMS district offices. At each district office location, we interviewed the local Judicial Security Inspector, obtained documents pertinent to local court security operations, received a tour of the court facilities, and interviewed members of the federal judiciary. Finally, we disseminated a questionnaire to the Judicial Security Inspectors in each USMS district office concerning management of the CSO contracts and security equipment.

This report first provides an assessment of the USMS's efforts to secure federal court facilities. The sections that follow assess the USMS's oversight of its CSO program, security systems, and related contracts. This report provides 15 recommendations to the USMS to help improve its Judicial Facilities Security Program.

Results in Brief

We found weaknesses in the USMS's efforts to secure federal court facilities in the six USMS district offices we visited. In two districts we found non-functioning Court Security Committees and in three districts the Chief Judges expressed concerns related to the physical security of courthouses.

Additionally, we found that not all Judicial Security Inspectors and CSOs have been fully trained on the use of security screening equipment. Three of the six USMS district offices failed to conduct the quarterly testing required by USMS policy regarding security procedures to screen visitors, packages, and mail delivered to the courthouses. In February 2009, multiple USMS district offices failed to detect mock explosive devices sent by USMS headquarters to the district offices for local testing purposes.

Our review also found that the USMS's management of its CSO contracts needs improvement. We found that the USMS's Office of Security Contracts awarded a contract worth about $300 million to a CSO contractor with a history of fraudulent activities. This contract was awarded despite a fraud alert issued by the Department of Justice Office of the Inspector General (DOJ OIG) Investigations Division. Ultimately, the contractor went

bankrupt, leaving many CSOs temporarily without payment for their services.

We also identified issues with the USMS's maintenance of CSO personnel files. Through our review of a sample of 60 CSO personnel files we found that 2 percent lacked the required medical examination records and 63 percent contained out-of-date medical examination records. In addition, 18 percent lacked the required firearms qualification records and 47 percent of the firearms qualifications were out of date. Our limited file review presents serious concerns about the medical and firearms qualifications for CSOs.

This audit makes 15 recommendations to help the USMS improve the management of its Judicial Facilities Security Program. The remaining sections of this Executive Summary provide a further description of our audit findings.

USMS Efforts to Secure Federal Court Facilities

In this audit we conducted field work at six judicial districts throughout the United States. We visited multiple courthouse locations at five of these six judicial districts and interviewed key personnel, including Judicial Security Inspectors, Chief Deputy Marshals, Deputy U.S. Marshals, and members of the federal judiciary, including Chief Judges.

Physical Security

Our audit identified weaknesses in the USMS's efforts to protect the physical security of federal court facilities in some of the six judicial districts we visited. For example, in one district we were informed that the judicial security plan had not been updated since 1983.[2] In another district, we found that the Continuity of Operations Plan was not updated as required.[3]

[2] USMS policy directives require that each district office conduct an annual security survey of every judicial facility within the district to assess current conditions. Based upon results of this survey, the district must develop or update a judicial security plan for each facility, which should be designed to ensure that USMS employees respond quickly and effectively to judicial security needs at various risk levels when there are actual threats.

[3] Homeland Security Presidential Directive 20 requires that all executive departments and agencies maintain a Continuity of Operations Plan that ensures that primary mission essential functions continue to be performed during a wide range of emergencies, including localized acts of nature, accidents, and technological or attack-related emergencies.

In two other districts, we were unable to determine when the last update to the Continuity of Operations Plans occurred.[4]

Further, USMS policy directives state that each district office shall assign a principal coordinator to the local district Court Security Committee, which is responsible for assessing the adequacy of district-wide court security, ensuring the effective and efficient use of court security resources, and ensuring that there is an effective emergency preparedness program in place. In one district, the Court Security Committee was not functioning as required because it was not meeting regularly. The Chief Judge in that district stated that the Court Security Committee was generally not holding meetings due to poor communication between the USMS and the judiciary. In another district we visited, a Court Security Committee did not exist.

In addition, to assess the judiciary's level of satisfaction on general physical court security matters in each of the six judicial districts we visited, we interviewed members of the judiciary and judicial staff members in those districts. In one district, the Chief Judge was generally dissatisfied with the physical security of the building and expressed concerns over whether adequate security was being provided at entry checkpoints, including the public building entrance, parking garage, and judge's entrance. He stated that he did not believe that the CSOs provided adequate security for the building and that improved CSO training is necessary. In another district, the Chief Judge said that funding and manpower limitations have negatively affected the quality and level of court security provided by the USMS. In a third district, the Chief Judge and his assistant believed that inspections of trucks entering the courthouse are poorly conducted, which jeopardizes the safety of the facility.

Training on Security Screening Equipment

The USMS relies on the use of security screening equipment, such as Itemisers, metal detectors, and X-ray machines at courthouse facilities to prevent the introduction of weapons, explosives, and other contraband.[5] CSOs are responsible for operating this screening equipment and therefore must be trained adequately on its use.

The training curriculum for CSOs includes a basic orientation training course (Phase I), and a 3-day orientation course conducted at the Federal Law Enforcement Training Center (Phase II). A USMS official informed us

[4] Federal Continuity Directive 1 requires a minimum of an annual review of the Continuity of Operations Plan with updates throughout the year as necessary.

[5] Itemisers are explosives and narcotics detection devices.

that Phase II training is not always conducted before CSOs begin work, and this individual expressed concern that as a result, some CSOs lack the technical training needed to operate screening equipment deployed to courthouse facilities. Moreover, the USMS has no system to ensure that Judicial Security Inspectors and CSOs are adequately trained on newly deployed equipment. As a result, we found instances where security features of new equipment were not being used in districts, partly, because no one had received training on the features.

Testing of Security Procedures

USMS policy requires that Judicial Security Inspectors in each district office conduct quarterly unannounced tests to determine if CSOs are adequately screening visitors, packages, and mail that are delivered to the courthouse.[6] Our audit found that quarterly unannounced tests were not being regularly conducted at three of the six districts we visited. Without consistent application of this policy, the courthouses in these districts can become more vulnerable to security breaches.

In addition, in February 2009, the USMS Office of Security Systems scheduled the shipment of testing kits to each of the USMS district offices that contained mock explosive devices to be used in local testing exercises. Although the shipment of these testing kits was not intended to be a formal testing exercise, several of these mock devices were not detected when the packages were screened at the local district offices. We believe that the results of this unintended test emphasize the need for the USMS to ensure that CSOs are properly trained on security equipment and procedures.

Incidents and Arrests

The USMS maintains data on arrests and other incidents, such as attempts to bring illegal weapons or contraband into court facilities, bomb threats, and assaults. This data is collected at the district level and reported to the USMS Office of Court Security.

However, we found that not all district offices are regularly reporting their data on incidents and arrests and little analysis is conducted by the USMS on the data that is collected. We believe that the USMS should ensure that all USMS districts are reporting the data as required. Further, the USMS

[6] USMS Directives state that each district should conduct an unannounced examination of the security of each court facility at least four times a year. According to this directive, the tests should be conducted at random and by persons unknown to the court security officers at the facility, and each district should report its findings to the Judicial Security Division.

should periodically analyze incidents and arrests to identify trends, such as the use of certain weapons or increased incidences of suspicious vehicles identified at federal courthouse locations. This could allow for better planning in the deployment of screening equipment, building design, and staffing. We also believe that such information and analysis could be valuable to the federal judiciary and would help ensure that the judiciary is better aware of potential security threats.

Management of Security Contracts and the Court Security Officer Program

The USMS had a contract force of over 5,000 CSOs deployed at federal court facilities throughout the United States as of June 2010. The USMS currently has 12 primary security contracts that provide for CSO services in each of the 12 federal judicial circuits.[7] As discussed below, our review found that the USMS's management of its court security contracts needs improvement.

USMS Oversight of the CSO Contract Procurement Process

Our review found that the USMS's Office of Security Contracts did not follow USMS procurement policy. For example, in September 2006 the USMS awarded 3 of its 12 primary CSO contracts to 1 security guard company named USProtect Corporation (USProtect). The 3 CSO contracts awarded to USProtect totaled about $300 million, covered federal court operations in 3 of the 12 federal judicial circuits, and involved the hiring, training, and supervision of approximately 800 CSOs. Two months prior to the USMS's selection of USProtect, the DOJ OIG issued a fraud alert to the USMS regarding USProtect that included the information from a 2005 fraud alert issued by the Social Security Administration Office of the Inspector General (SSA OIG). The SSA OIG alert outlined a history of fraud related to USProtect covering a 12-year period. This history included multiple fraud convictions and civil judgments against its Chief Financial Officer, including criminal convictions for mail fraud, submitting false insurance claims, and bank fraud, as well as six fraud-related civil judgments totaling more than $1.4 million. Despite the fraud alert, the USMS awarded the contract to USProtect.[8] USProtect later filed for Chapter 7 bankruptcy protection

[7] In addition to the 12 primary contracts, the USMS has set aside contracts for the Northern District of Florida and the Central District of Illinois for 8(a) awards, which are contracts awarded to small businesses owned and controlled by socially and economically disadvantaged individuals.

[8] At the conclusion of this audit, the USMS informed us that the contracting officer responsible for this contract is no longer employed by the USMS.

after the USMS and other federal agencies decided not to renew their contracts amid allegations of fraud and mismanagement. This left many CSOs temporarily without compensation for their services.

On June 17, 2009, the DOJ OIG issued another advisory to the USMS related to deficiencies in the USMS contract award process as demonstrated by its selection of USProtect.[9] The USMS responded to this advisory on July 28, 2009, outlining procedures that it would adopt to address the issues discussed in the advisory. For instance, the USMS has agreed to provide additional training for members of its Technical Evaluation Board, as well as provide greater oversight of the solicitation review process by the contracting officer and the General Counsel's office.[10]

We also determined that the Office of Security Contracts lacks written policies that establish procedures for maintaining files on the selection of CSO contractors. According to an Office of Security Contracts official, the lack of organization of the security contract files makes it difficult for the USMS to defend against bid protests filed by vendors and claims filed by contractors. Although the USMS informed us of recent steps that it has taken to improve its file management system, we believe the USMS should continue to evaluate its current contract file maintenance practices and develop procedures to ensure that all necessary documentation is maintained in a consistent manner. Our audit also determined that the USMS lacks a streamlined system for tracking CSO work hours. We believe that a streamlined timekeeping system could decrease the risk of human error, overbilling by CSO contractors, and fraud.

USMS Management of the Court Security Officer Program

Our review found that the USMS has failed to conduct timely background investigations for newly hired CSOs. According to USMS policy, the USMS performs a background investigation for all CSO applicants prior to allowing them to work in a federal court facility.

Background investigations should be completed by the district and then sent to USMS headquarters for adjudication and approval. USMS policy

[9] Appendix III contains a copy of the advisory and the USMS's formal response.

[10] The Federal Acquisition Regulation requires that the "selection authority shall establish an evaluation team, tailored for the particular acquisition, that includes appropriate contracting, legal, logistics, technical, and other expertise to ensure a comprehensive evaluation of offers." In this case, the USMS contracting officer appointed a Technical Evaluation Board consisting of a U.S. Marshal, a Chief Deputy U.S. Marshal, two Deputy U.S. Marshals, and one employee from the Judicial Security Division.

requires that the district office submit background check information and recommendations to USMS headquarters within 21 days of the district office's receipt of the background investigation request. We tested a judgmental sample of 20 out of 213 CSOs hired between February and July 2009 and found that 17 of the sample background investigations were submitted to headquarters for adjudication more than 21 days after the district office's receipt of the request, contrary to USMS policy.

A performance violation includes conduct such as allowing restricted items to pass through security and leaving firearms unsecured. Although the USMS maintains data on CSO performance violations, we found that the USMS does not utilize this data effectively. For example, the USMS does not analyze performance violation data of CSOs to determine whether issues related to CSO performance in one circuit were occurring in another. Additionally, at the time of our field work, the USMS was not analyzing this data to assess and address potential CSO training needs, although we were told that the USMS is currently attempting to use this data in developing future CSO training.

We also found problems in the USMS's maintenance of its CSO personnel files. We reviewed 60 CSO personnel files to determine whether the files contained up-to-date medical examination records and firearms qualifications. According to USMS policy, each CSO must obtain an annual medical examination by a physician designated by the CSO contractor. A medical officer from the U.S. Public Health Service's Federal Law Enforcement Medical Program then reviews the results of the medical examination and determines whether the CSO is qualified to perform CSO job functions. In addition, each CSO must qualify annually to carry a firearm by taking a firearms proficiency test.

Our review found that 1 of the 60 files (2 percent) lacked a medical examination record and 38 (63 percent) of the medical examination records in these files were out of date.[11] In addition, we found that 11 of the 60 (18 percent) files lacked firearms qualification records and 28 (47 percent) of the files contained firearms qualification records that were

[11] The USMS provided us with the 60 CSO personnel files on December 4, 2009. Because USMS policy requires a CSO to receive an annual medical examination within 1 year of the previous examination, we considered a CSO personnel file to contain out-of-date medical examination records if the file did not contain evidence of a medical examination that occurred between December 3, 2008, and December 4, 2009.

out of date.[12] Our limited file review presents serious concerns about the medical and firearms qualifications for CSOs.

Management of Security Systems and Security System Contracts

The USMS's nationwide security systems contract covers the purchase, installation, and maintenance of security systems, including duress and intruder alarms, closed-circuit televisions, intercoms, and access-control systems for federal courthouses. The Contracting Officer's Technical Representatives (COTR) for the nationwide security systems contract are located at USMS headquarters, but the district Judicial Security Inspectors are generally responsible for managing the day-to-day oversight of the contract in the district offices.[13] For example, if a security camera needed to be installed at a court facility and the contractor sends someone to perform the work, the Judicial Security Inspector in that district typically certifies that the work was performed. However, despite USMS policy, we found that these certifications typically state only that the work was completed, not how much time was spent on the project. Because labor hours are not consistently monitored or tracked it is difficult for the USMS to ensure that labor hours claimed under the contract were actually worked by the contractor.

In addition to the security systems obtained through the nationwide security systems contract, the USMS also acquires security screening equipment, including X-ray machines, walkthrough metal detectors, and explosives detection units, through various procurement methods. This screening equipment is not purchased under a specific USMS contract and is maintained by the USMS. The USMS has no maintenance agreements for the millions of dollars worth of sophisticated screening equipment deployed at court facilities throughout the country. During our review, we found that when X-ray machines and metal detectors were in need of repair they were out of service anywhere from 1 day to several weeks. According to an Office of Security Systems official, the USMS previously conducted an analysis and determined that maintenance plans for this type of equipment were not cost effective. However, this official also told us that he was unsure whether the USMS was assessing the impact of downtime on court security. We recommend that the USMS track the cost of repairs for its screening

[12] The USMS provided us with the 60 CSO personnel files on December 4, 2009. Because USMS policy requires a CSO to qualify on their firearm once per calendar year, we considered a CSO personnel file to contain an outdated firearms qualification record if the file lacked a record for calendar years 2008 and 2009.

[13] According to the USMS, all Judicial Security Inspectors receive COTR training and are required to be recertified every 2 years.

equipment and the impact of downtime on court security in order to periodically assess whether a maintenance plan for such screening equipment would be cost effective. By periodically reassessing the need for a maintenance plan, the USMS can ensure that the most cost-effective method is being used for maintenance of these items.

Recommendations

Based on our findings, this audit provides 15 recommendations to improve the USMS's oversight of its Judicial Facilities Security Program. Those recommendations are that the USMS:

1. Ensure that all USMS district offices regularly review and update their Continuity of Operations Plans and ensure that annual security surveys are performed at each district and that all judicial security plans are updated as required.

2. Ensure that all of its district offices assign a principal coordinator to the district Court Security Committee and encourage the local judiciary to lead regular meetings.

3. Ensure that all Judicial Security Inspectors and CSOs are appropriately trained before entering on duty. The USMS should also develop a process to ensure that all Judicial Security Inspectors and CSOs are adequately trained on newly deployed screening systems.

4. Ensure that its district offices perform the required quarterly unannounced tests to determine if CSOs are adequately screening visitors, packages, and mail that are delivered to the courthouse and maintain records of the results.

5. Ensure that all district offices report incidents and arrests at courthouse facilities as required and conduct a coordinated periodic analysis of the data each fiscal year.

6. Continue to evaluate its current contract file maintenance practices and develop procedures to ensure that all necessary documentation is maintained in a consistent manner.

7. Seek to streamline its current timekeeping practices for CSOs.

8. Perform a comprehensive review of its background investigation process for CSOs and seek to ensure that these investigations are completed in a timely manner.

9. Develop a method for analyzing its performance violation data to better understand violation trends and potential training needs among its CSO workforce.

10. Provide additional guidance to district Judicial Security Inspectors to ensure that all CSO performance violations are documented and reported to the Office of Court Security.

11. Evaluate its CSO personnel file maintenance practices and develop procedures to ensure that all necessary documentation, such as medical and firearms qualifications, is adequately maintained and up to date. In addition, the USMS should assess the feasibility of implementing an automated system for tracking important dates in the database to ensure that CSOs satisfy their qualification requirements in a timely manner.

12. Require district offices to supervise and verify labor hours claimed by contractors to help ensure that it is not being overbilled under the nationwide security systems contract.

13. Assess the feasibility of district offices maintaining their own security system equipment inventories of equipment maintained by the contractor so that comparisons can be made to the contractor's inventory to avoid unwarranted maintenance fees.

14. Track the cost of repairs for its screening equipment and the impact of downtime on court security in order to periodically assess whether a maintenance plan for its screening equipment would be cost effective.

15. Require the Office of Security Contracts to prepare past performance and interim evaluations in accordance with the Federal Acquisition Regulation.

This page intentionally left blank.

THE UNITED STATES MARSHALS SERVICE'S OVERSIGHT OF ITS JUDICIAL FACILITIES SECURITY PROGRAM

TABLE OF CONTENTS

THE UNITED STATES MARSHALS SERVICE'S OVERSIGHT OF ITS JUDICIAL FACILITIES SECURITY PROGRAM

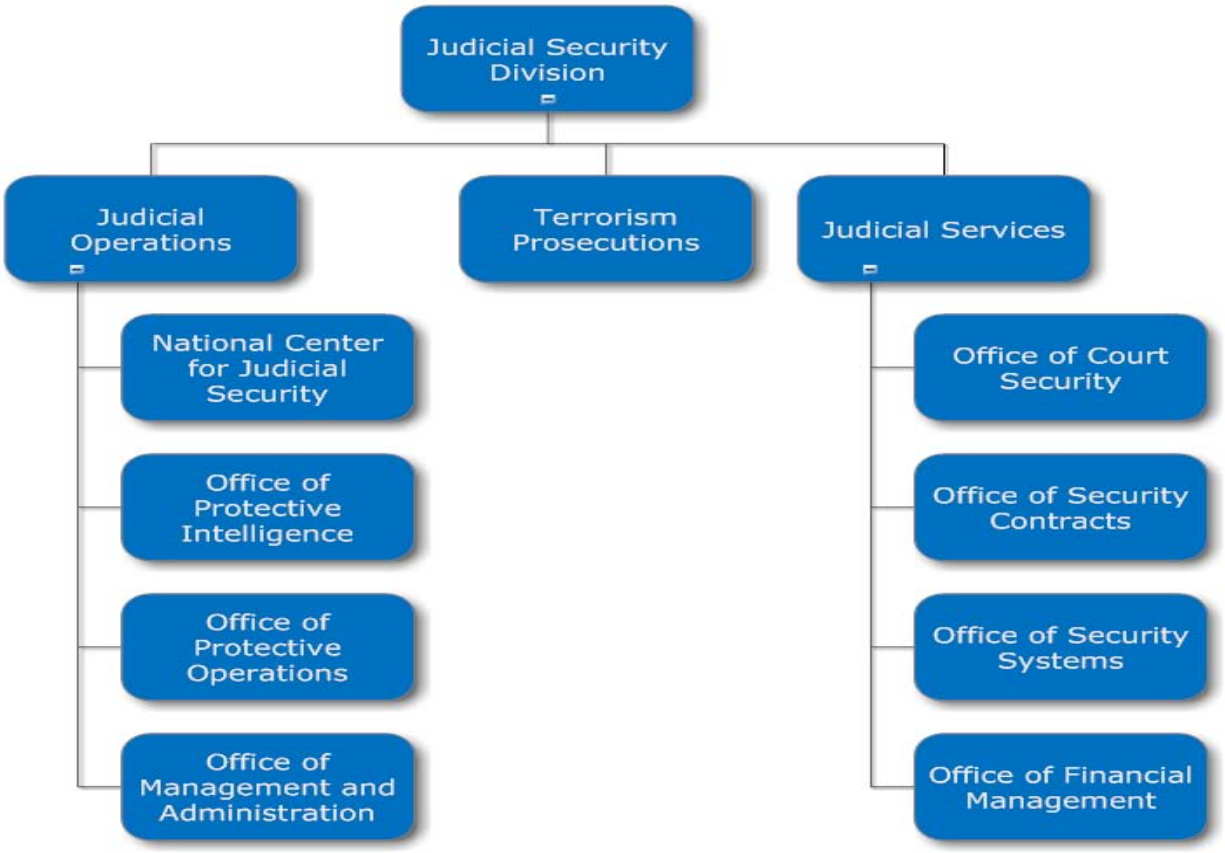
INTRODUCTION

The United States Marshals Service (USMS) provides court security services to federal court facilities. The USMS's Judicial Facilities Security Program, which is administered by USMS headquarters and funded by the federal judiciary, provides 2 main services to more than 400 federal court facilities nationwide: (1) court security officers (CSO), and (2) security systems and equipment, including X-ray machines, surveillance cameras, duress alarms, and judicial chambers entry control devices. The CSOs deployed by the USMS to federal court facilities are contract workers procured through contracts with private security firms in each of the 12 federal judicial circuits. As of June 2010, over 5,000 CSOs were assigned to federal court facilities throughout the United States. As with CSOs, the security systems obtained by the USMS are also obtained through a contract with a private security provider. The USMS seeks to ensure the safety of federal court facilities and judicial proceedings through the use of the CSO program and the security systems it deploys. In fiscal year (FY) 2009, approximately $370 million were allocated by the federal judiciary for these court security services.

The USMS's Judicial Services component of the Judicial Security Division is primarily responsible for administering the Judicial Facilities Security Program, including oversight of the CSO program and management of USMS security systems and contracts. According to the USMS, CSOs are experienced former law enforcement officers who receive limited deputations as special Deputy U.S. Marshals. Using USMS security screening systems, CSOs are responsible for detecting and intercepting weapons and other prohibited items from individuals attempting to bring them into federal courthouses. Along with Deputy U.S. Marshals, CSOs also assist in providing security at facilities that house federal court operations.[14] The organization chart for the Judicial Security Division follows.

[14] Deputy U.S. Marshals are full-time USMS employees who carry out multiple missions including, apprehending federal fugitives, protecting the federal judiciary, operating the USMS's Witness Security Program, transporting federal prisoners, and seizing property acquired by criminals through illegal activities.

Exhibit 1
USMS Judicial Security Division



Source: USMS

The Office of Court Security determines resource needs and provides operational guidance to USMS employees responsible for managing the CSO program in the USMS districts. This office is also responsible for developing and coordinating in-service training for CSOs, as well as developing and coordinating training for Judicial Security Inspectors. CSOs are supervised by Judicial Security Inspectors in each of the USMS district offices. There are 108 Judicial Security Inspectors, with at least 1 Judicial Security Inspector in each of the 94 USMS districts.[15]

The Office of Security Systems' responsibilities include the purchase, deployment, and installation of security systems at federal court facilities. These security systems include duress and intruder alarms, closed-circuit

[15] Judicial Security Inspectors manage CSO contract operations in their respective districts. These Judicial Security Inspectors are Deputy U.S. Marshals who have been delegated the responsibilities of a Contracting Officer's Technical Representative for the CSO contracts in their district.

televisions, intercoms, and access-control systems for federal courthouses. The Office of Security Systems also monitors contractor performance on the USMS's nationwide security systems contract. Currently, six of the Office of Security Systems security specialists serve as Contracting Officer's Technical Representatives (COTR), who coordinate with the 108 district Judicial Security Inspectors to manage the day-to-day use of security systems, including maintenance, installation, and inventory control. In August 2010, the USMS informed us that an additional three security specialists would soon be receiving COTR certificates, resulting in a total of nine security specialists managing the day-to-day activities on the nationwide security systems contract.

The Office of Security Contracts handles procurement activities for the Judicial Security Division and coordinates with both the Office of Court Security and the Office of Security Systems in the procurement of CSO contracts and security systems.

Prior OIG Reports

In recent years, the OIG has conducted reviews related to the USMS's efforts to protect court personnel and facilities. In 2000, the OIG issued an audit report on the USMS's Court Security Officer Program, which found that the training of CSOs was inadequate, unannounced testing of screening check points was not conducted as required, and security clearances and medical certifications were not consistently maintained at the district level. In 2005, the OIG examined background investigations conducted by the USMS and found that the USMS did not conduct routine re-investigations of CSOs unless it became aware of misconduct issues that required disciplinary action. Because CSOs carry firearms, protect the judiciary, and are granted unescorted access to court facilities, the OIG recommended that the USMS reinvestigate contractors who are assigned law enforcement duties every 5 years. In 2009, the OIG reviewed the USMS's response to threats against the members of the federal judiciary and United States Attorneys. That review concluded that the USMS did not consistently provide an appropriate response for the risk level posed by the threat. In addition, the report found that the USMS did not fully or effectively coordinate with other law enforcement agencies to respond to threats against federal judicial officials. Appendix II contains additional detailed information regarding the results of these OIG-led reviews.

OIG Audit Approach

The objective of this audit was to assess the USMS's oversight of its Judicial Facilities Security Program. To accomplish our objective we

interviewed USMS headquarters officials, reviewed USMS policies and procedures, and obtained and analyzed data pertinent to the USMS's court security programs, including a review of CSO personnel files. We also conducted an in-depth review of the procurement process for a CSO contractor whose contract was later terminated. Additionally, we conducted site work at six USMS district offices. At each district office location, we interviewed the local Judicial Security Inspector, obtained documents pertinent to local court security operations, received a tour of the court facilities, and interviewed members of the federal judiciary, including Chief Judges. Finally, we disseminated a questionnaire to the Judicial Security Inspectors in each district office concerning the management of the CSO contracts and security equipment.

This report first provides an assessment of the USMS's efforts to secure federal court facilities. The sections that follow assess the USMS's oversight of its CSO program, security systems, and related contracts. This report provides 15 recommendations to the USMS to help improve its Judicial Facilities Security Program.

USMS Efforts to Secure Federal Court Facilities

Our audit identified weaknesses in the USMS's efforts to protect federal court facilities that could compromise the USMS's ability to ensure the safety of these facilities. These weaknesses include the USMS's failure to: (1) maintain current security plans as required, (2) require CSOs to be fully trained on screening equipment and security procedures prior to assuming their duties, (3) consistently test security procedures, and (4) adequately analyze data on incidents and arrests.

To assess the USMS's efforts to protect federal court facilities, we conducted field work at six judicial districts throughout the United States. We visited multiple courthouse locations at five of these six judicial districts and interviewed key personnel including Judicial Security Inspectors, Chief Deputy Marshals, Deputy U.S. Marshals, and members of the federal judiciary, including Chief Judges.

Physical Security

During our visits to federal court facilities we sought to determine whether the local USMS district office was taking the actions necessary to protect the physical security of courthouse buildings. At each judicial district, we assessed the USMS's maintenance of security plans within the districts and sought feedback from the local federal judiciary on the USMS's handling of general physical court security matters.

Maintenance of Security Plans

All courthouse facilities must follow certain general security standards in various federal requirements. Homeland Security Presidential Directive 20 requires that all executive departments and agencies maintain a Continuity of Operations Plan that ensures that primary mission essential functions continue to be performed during a wide range of emergencies, including localized acts of nature, accidents, and technological or attack-related emergencies. A USMS policy directive requires that each district conduct an annual security survey of every judicial facility within the district to assess current security conditions.[16] Based upon results of this survey, the district must develop or update a judicial security plan for each facility that is designed to ensure that USMS employees respond quickly and effectively to judicial security needs at various risk levels when there are actual threats.

Overall, we found weaknesses in some of the judicial districts we visited in their handling of the requirements described above. In one of the districts, we found that the Continuity of Operations Plan was not updated as required.[17] In two other districts, we were unable to determine when the last update to the Continuity of Operations Plans occurred. In another district we were informed that the judicial security plan had not been updated since 1983. Because the judicial security plans should be tailored to the security challenges of each facility, the failure to maintain this document, along with the Continuity of Operations Plan, increases the vulnerability of court facilities.

Leadership of the District Court Security Committees

USMS policy directives state that the U.S. Marshal or designee in each judicial district will be the principal coordinator of a district Court Security Committee, which is chaired by the federal judiciary and will advise on the planning, implementation, and continuous review of the court security program for each federal judicial facility in the district. However, one district Chief Judge stated that the Court Security Committee was not functioning as required because it was not meeting regularly. According to the Chief Judge in that district, the Court Security Committee was generally not holding meetings due to poor communication between the USMS and the judiciary.

[16] USMS policy directives state that the U.S. Marshal, or designee, shall ensure that the district office conducts an annual judicial facility security survey of every judicial facility within the district to assess current security conditions.

[17] Federal Continuity Directive 1 requires a minimum of an annual review of the Continuity of Operations Plan with updates throughout the year as necessary.

Although the Chief Judge acknowledged that communication between the parties had begun to improve, at the time of our visit the Court Security Committee was not holding regular meetings. The Chief Judge expected that they would hold regular meetings in the near future. In another district, we were informed that a district Court Security Committee did not exist.

Judicial Satisfaction with Physical Security

To assess the judiciary's level of satisfaction on general physical court security matters, we interviewed members of the judiciary and judicial staff members at each of the six districts we visited. The judiciary and its staff who we interviewed generally indicated that they felt safe in USMS-protected buildings and that the USMS was responsive to security concerns. However, we were informed of specific concerns in three of these districts. For example, in one district, the Chief Judge noted security concerns at checkpoints, including the public building entrance, parking garage, and judge's entrance. In another district, the Chief Judge stated that the USMS has been responsive and helpful, but that funding and manpower limitations have negatively affected the quality and level of court security provided by the USMS. In yet another district, the Chief Judge described how a defendant gained access in an unknown way to an interior hallway that connects to the judicial offices. According to the Chief Judge, although no harm resulted from this incident, it made him and his staff very uncomfortable with the level of security provided. The Chief Judge and his assistant also believed that inspections of trucks entering the courthouse were poorly conducted and potentially jeopardized the safety of the facility.

We recommend that the USMS ensure that all district offices regularly review and update their Continuity of Operations Plans. The USMS should also ensure that annual security surveys are performed at each district and that all judicial security plans are updated as required. In addition, the USMS should ensure that each district office assigns a principal coordinator to the district Court Security Committee and encourage the local judiciary to lead regular meetings.

Training on Security Screening Equipment

The USMS relies on the use of security screening equipment, such as Itemisers, metal detectors, and X-ray machines, at courthouse facilities to prevent the introduction of weapons, explosives, and other contraband.[18] CSOs are responsible for operating this screening equipment and therefore,

[18] Itemisers are explosives and narcotics detection devices.

we believe that they must be trained adequately on its use. We also believe that Judicial Security Inspectors should be adequately trained in the use of this equipment.

The training curriculum for CSOs currently includes basic orientation training (Phase I) and a 3-day orientation course conducted at the Federal Law Enforcement Training Center (Phase II). CSO vendors are also responsible for providing annual training on security procedures, screening, and administrative matters.

CSO vendors are responsible for providing their CSOs with Phase I training prior to their entry on duty. Phase I training is offered through a series of videos and handouts and addresses topics such as security screening and searches. Phase II training, which is intended to be completed within 1 year of hire, covers multiple topics, including entry point screening, use of walk-through and hand-held metal detectors, the Department of Justice deadly force policy, and a review of a CSO's role in a weapons of mass destruction event. According to the Office of Court Security Assistant Chief of Training and Compliance, the USMS would like CSOs to complete Phase II training before they begin work. However, a USMS official told us that Phase II training is not always conducted before CSOs begin work, and this individual expressed concern that as a result, some CSOs lack the technical training needed to operate screening equipment deployed to courthouse facilities. At the conclusion of our audit, the USMS informed us that this CSO training program was recently redesigned and that implementation of the redesigned program will occur in FY 2011.

We also found that there is not a reliable system to ensure that CSOs are adequately trained on newly deployed equipment. According to three Judicial Security Inspectors in the districts we visited, when new equipment is purchased and installed in court facilities, it is the responsibility of the lead CSO to train the other CSOs on how to operate the equipment. However, we were informed of an instance when training was not conducted on new X-ray machines purchased by the USMS. These machines, purchased beginning in 2003, came equipped with software designed to automatically detect explosives and weapons. However, the automated detection tool was not turned on by the vendor and went unused because neither the Judicial Security Inspectors nor the CSOs in the districts received training on how to use it. In 2009, we were told that an attorney at one court facility passed through a security check point with a gun in her bag because of CSO error and the failure to properly activate the automated detection setting on the X-ray machine, which could have detected the gun.

We were also informed of other instances where CSOs were not trained on the use of new equipment. For example, in FY 2002, the USMS spent $8 million to purchase hi-tech explosives detection units, known as Itemisers. We were told by some USMS officials that the USMS provided little training or guidance to the district offices on how to utilize the equipment, which resulted in many of the units not being used or properly maintained. According to one USMS official, this ultimately led to many Itemisers falling into a state of disrepair. At the conclusion of our audit, other USMS officials told us that training was provided to all of the districts and was not the sole reason for the Itemisers' state of disrepair. According to these officials, these machines were prone to failure, the software was difficult to use, and some districts chose not to use them in the absence of a policy or protocol for their use.

According to the USMS, basic training courses for new Judicial Security Inspectors were held in October and November 2007, August 2008, and January and March 2010. These sessions were intended to provide an introduction to the Judicial Security Inspector program, along with providing the basic fundamentals necessary to serve as a Judicial Security Inspector. In June 2009, the USMS held for the first time an advanced multi-day training course for approximately half of its Judicial Security Inspectors, which included training on screening equipment and other security systems. The USMS also informed us that online X-ray training was recently purchased and added as a mandatory requirement for all district Judicial Security Inspectors. The USMS currently estimates that this training should be completed by all Judicial Security Inspectors by October 2011.

We believe that inadequate training on security screening equipment for Judicial Security Inspectors and CSOs poses a significant risk to the safety of court personnel and facilities. Therefore, we recommend that USMS ensure that all Judicial Security Inspectors and CSOs are appropriately trained on security screening equipment before entering on duty. The USMS should also develop a process to ensure that all Judicial Security Inspectors and CSOs are adequately trained on newly deployed screening systems.

Testing of Security Procedures

USMS policy requires that Judicial Security Inspectors in each district office conduct quarterly unannounced tests to determine if CSOs are adequately screening visitors, packages, and mail that are delivered to the

courthouse.[19] However, our audit found that quarterly unannounced tests were not being regularly conducted at three of the six districts we visited.

In one of these offices, the Judicial Security Inspector stated that tests are performed every 6 months instead of quarterly due to problems obtaining a role player to conduct the test.[20] In another district, only two tests had been conducted since FY 2007, and in both tests the CSOs had failed to detect the unallowable weapons as they passed through screening. According to the Judicial Security Inspector for that district, he was relatively new to his position and did not understand these tests to be a requirement while learning his role. The Judicial Security Inspector in a third district stated that tests had not been performed prior to December 2009 because he did not have the time to conduct the tests. He also said that he had not been tasked to perform them. In response to our questions, this Judicial Security Inspector said that he would soon be considering how to begin performing the quarterly tests as required.

We believe that in the absence of the required testing, court facilities could become more vulnerable to security breaches. We recommend that USMS headquarters ensure that district offices perform the required quarterly unannounced tests and maintain records of the results.

Additional Identified Weakness

In February 2009, the USMS Office of Security Systems scheduled a shipment to each of the USMS district offices of testing kits containing mock explosive devices to be used in local testing exercises. Although the shipment of these testing kits was not intended to be a formal testing exercise, several of these mock devices were not detected when the packages were screened at the local district offices. Upon learning that several of these mock devices were not detected, USMS headquarters requested, but did not require, that all district offices report whether the mock devices went undetected when the package containing the device arrived in the district. Exhibit 2 reflects the information provided by the district offices that did report to USMS headquarters and the actions taken in response.

[19] USMS Directives state that each district should conduct an unannounced examination of the security of each court facility at least four times a year, and that these tests should be conducted at random by persons unknown to the court security officers at the facility. Each district must report its findings to the Judicial Security Division.

[20] In this context, a role player is an individual who plays the part of someone attempting to bring an unallowable item into the building.

Exhibit 2
Performance Violations Related to February 2009 Mock Explosives Shipment[21]

District	Date	Performance Violation	Action Taken
District A	2/4/2009	Two CSOs allowed an Improvised Explosive Device (IED) Test Kit of a simulated bomb to go through the X-ray machine without being detected.	Both CSOs received a 3-day suspension and warning
District B	2/4/2009	CSO allowed an IED Test Kit of a simulated bomb to go through the X-ray machine without being detected.	3-day suspension and warning
District C	2/5/2009	CSO allowed an IED Test Kit of a simulated bomb to go through the X-ray without being detected.	3-day suspension and warning
District D	2/5/2009	CSO allowed an IED Test Kit containing simulated explosives to pass through the X-ray machine undetected while operating the X-ray machine. The package did set off the X-ray explosive indicator and was clearly visible on the X-ray monitor.	CSO received a warning
District E	2/6/2009	Unknown CSO allowed an IED Test Kit of a simulated bomb to go through the X-ray machine without being detected.	No Action taken without CSO identified
District F	2/17/2009	CSO failed to detect dummy explosives when they arrived.	CSO received letter of reprimand

Source: USMS

We believe this unintended test emphasizes the need for the USMS to ensure that CSOs are properly trained on security equipment and procedures. We believe the failure of these district offices to identify these mock explosives devices, and the failure of USMS headquarters to identify whether other district offices similarly failed to identify these devices demonstrates that additional oversight from USMS headquarters is needed to ensure that district offices follow USMS policy related to the testing of security procedures.

[21] A performance violation is defined by the USMS as an infraction that violates the standards of competency, conduct, appearance, and integrity as outlined in the CSO contract.

Incidents and Arrests

Incidents such as arrests at federal court facilities and bomb threats must be reported to the Office of Court Security. However, we found that not all USMS district offices are reporting this data as required. For example, according to the data provided to us by the Office of Court Security, only 80 of the 94 USMS district offices (85 percent) reported incident and arrest data for March 2009 and October 2009. In addition, we were informed that although the data is collected and monitored by the USMS, the USMS engages in no coordinated effort to analyze this data. Exhibit 3 provides a breakdown of incidents and arrests that were reported by USMS districts in FYs 2009 and 2010.

Exhibit 3
Incidents and Arrests at U.S. Court Facilities
Fiscal Years 2009 and 2010[22]

Violation	FY 2009		FY 2010	
	Count	Percentage of Total	Count	Percentage of Total[23]
"Other" Incidents	2,585	79.0	3,578	91.1
Medical Emergency	301	9.2	167	4.3
Disruptive Person	201	6.1	98	2.5
Illegal Weapon	98	3.0	23	0.6
Contraband	42	1.3	41	1.0
Arrests	22	0.7	2	0.1
Bomb Threat	7	0.2	6	0.2
Forced Entry	7	0.2	3	0.1
Assault	6	0.2	8	0.2
Shooting	3	0.1	0	0.0
TOTALS	**3,272**	**100%**	**3,926**	**100%**

Source: USMS

As the table above shows, in FY 2009, 79 percent of the incidents were classified as "other" incidents. In FY 2010, this number rose to 91 percent of the total. When we asked the USMS how it defines this category, the

[22] Data reported for fiscal year 2010 does not cover the full fiscal year and is current through August 26, 2010.

[23] Throughout the report, total percentages may not equal 100 percent due to rounding.

USMS responded that this category reflects significant incidents such as damage to government property, protests and demonstrations, suspicious vehicles, and the photographing of U.S. courthouses. According to the USMS, there are no plans to address the high percentage of incidents categorized as "other" incidents because it believes there are too many other possible incidents to add additional categories to its data collection efforts. We disagree with the USMS. By including potentially significant incidents like suspicious vehicles and the photographing of U.S. courthouses in the "other" incidents category, the USMS may be missing the opportunity to identify trends that could demonstrate future threats to U.S. courthouses.

We believe that the USMS should ensure that all of its district offices report incident and arrest data as required and analyze the collected data on a routine, periodic basis, to identify trends such as the use of certain weapons or the increased incidence of suspicious vehicles found at federal courthouse locations. Such analyses could allow for better planning in the deployment of screening equipment, building design, and staffing. Furthermore, we believe such information and analyses could be valuable to the federal judiciary and would help ensure that the judiciary is better aware of potential security threats.

Conclusion and Recommendations

We believe that the USMS should take proactive steps to improve the physical security of the federal court facilities it protects. First, the USMS should require all of its district offices to regularly review and update their Continuity of Operations Plans and judicial security plans. Without updated security planning documents, the district offices are at risk of being unprepared should a security event occur. The USMS should also ensure that all CSOs and Judicial Security Inspectors are fully trained on the operation of screening equipment and screening procedures. The failure of the USMS to adequately train these personnel on screening equipment and procedures could result in greater vulnerability to federal court facilities and personnel. We also believe that the USMS should perform periodic analyses of incidents and arrests. Such analyses could assist the USMS in identifying trends; assist in the planning and deployment of screening equipment, building design, and staffing; and would help ensure that the judiciary is more aware of potential security threats.

We recommend that the United States Marshals Service:

1. Ensure that all USMS district offices regularly review and update their Continuity of Operations Plans and ensure that annual security

surveys are performed at each district and that all judicial security plans are updated as required.

2. Ensure that all of its district offices assign a principal coordinator to the district Court Security Committee and encourage the local judiciary to lead regular meetings.

3. Ensure that all Judicial Security Inspectors and CSOs are appropriately trained before entering on duty. The USMS should also develop a process to ensure that all Judicial Security Inspectors and CSOs are adequately trained on newly deployed screening systems.

4. Ensure that its district offices perform the required quarterly unannounced tests to determine if CSOs are adequately screening visitors, packages, and mail that are delivered to the courthouse and maintain records of the results.

5. Ensure that all district offices report incidents and arrests at courthouse facilities as required and conduct a coordinated periodic analysis of the data each fiscal year.

Management of Security Contracts and the Court Security Officer Program

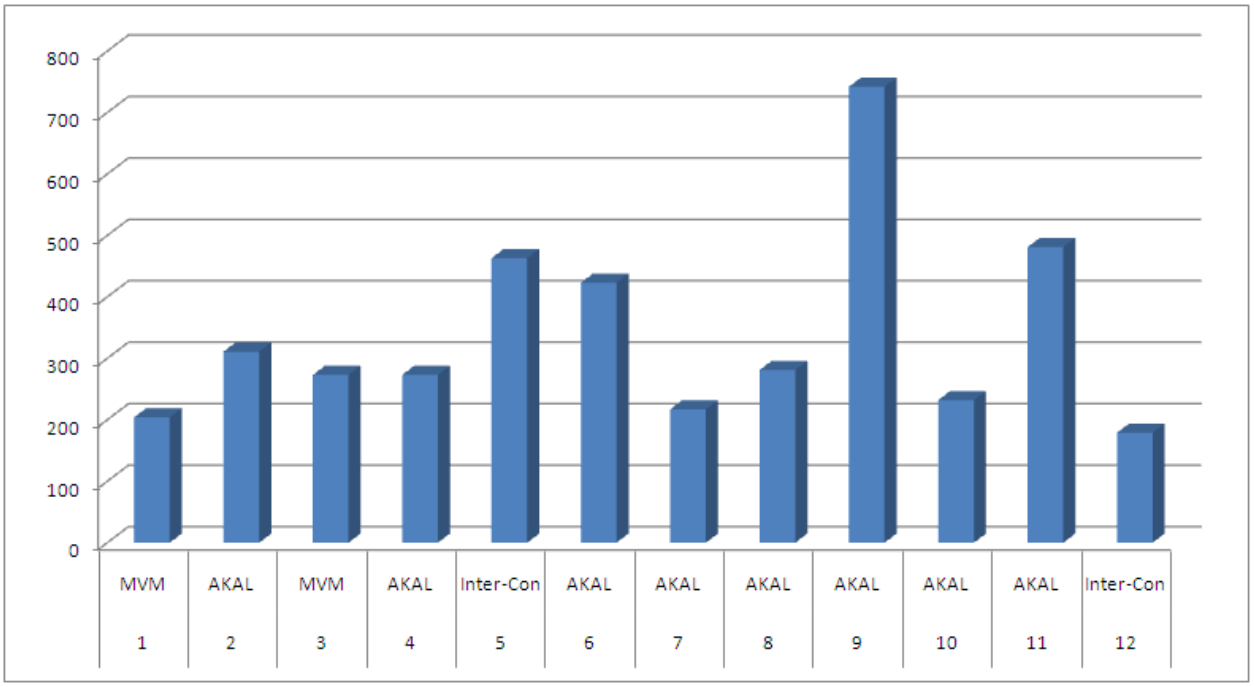
As noted above, as of June 2010, the USMS had a contract force of over 5,000 CSOs deployed at federal court facilities throughout the United States. These CSOs are supervised by Judicial Security Inspectors in each of the USMS district offices.

The USMS currently has 12 primary security contracts that provide for CSO services at federal court facilities nationwide.[24] The 12 contracts are organized geographically to align with each of the 12 federal judicial circuits. The CSO workforce varies in size from one judicial circuit to the next. For example, the CSO contract for the 9th Judicial Circuit, which is the largest of the 12 judicial circuits, provides over 700 CSOs to staff security operations at 67 court facilities. In contrast, the 1st Judicial Circuit provides approximately 200 CSOs to staff security operations at 11 court facilities.

[24] In addition to the 12 primary contracts, the USMS has set aside contracts for the Northern District of Florida and the Central District of Illinois for 8(a) awards, which are contracts awarded to small businesses owned and controlled by socially and economically disadvantaged individuals.

As of January 2009, the 12 primary CSO contracts were divided among 3 vendors. As reflected in Exhibit 4, the majority of the primary CSO contracts are with AKAL, who holds 8 of the 12 primary contracts. The remaining four primary contracts are divided evenly between MVM and Inter-Con.

Exhibit 4
U.S. Marshals Service
Court Security Officer Program
Distribution of Primary Contracts and CSOs by Judicial Circuit[25]



Source: USMS Office of Court Security

Our review found that the USMS's management of its court security contracts needs improvement. We believe a general lack of oversight by the Office of Security Contracts has resulted in inefficiencies and in some cases major breakdowns in the contract review and approval process.

USMS Oversight of the CSO Contract Procurement Process

Our review found that the USMS's Office of Security Contracts did not follow USMS procurement policy. For example, in September 2006, the USMS awarded 3 of its 12 primary CSO contracts to a security guard company, USProtect Corporation (USProtect). The 3 CSO contracts awarded to USProtect totaled about $300 million and covered federal court operations

[25] Data reflects distribution of CSO contracts as of January 15, 2009.

in 3 of the 12 federal judicial circuits, and involved the hiring, training, and supervision of approximately 800 contract guards. Two months prior to the USMS's selection of USProtect, the DOJ OIG issued a fraud alert to the USMS regarding USProtect that included the information from a 2005 fraud alert issued by the Social Security Administration Office of the Inspector General (SSA OIG). The SSA OIG alert outlined a history of fraud related to US Protect covering a 12-year period. This history included multiple fraud convictions and civil judgments against its Chief Financial Officer, including criminal convictions for mail fraud, submitting false insurance claims, and bank fraud, and six fraud-related civil judgments totaling more than $1.4 million. Despite its knowledge of this history, the Office of Security Contracts determined that USProtect offered the best value to USMS.[26]

In March 2008, USProtect filed for Chapter 7 bankruptcy protection after the USMS and other federal agencies decided not to renew their contracts with USProtect amid allegations of fraud and mismanagement. This left many CSOs temporarily without compensation for their services.

On June 17, 2009, the DOJ OIG issued another advisory to the USMS related to deficiencies in the USMS contract award process as demonstrated by its selection of USProtect.[27] The advisory highlighted that USProtect was awarded the contract in September 2006 despite: (1) the lack of due diligence in the USMS's background research, (2) USMS concerns that USProtect's proposed price was insufficient to cover program costs, and (3) USMS's failure to provide all relevant information to the USMS's Technical Evaluation Board.[28] Additionally, the advisory highlighted that the Technical Evaluation Board's bid review process was based on 3 criteria weighted on a 100-point scoring system but that in many instances, even though USProtect did not receive full points, the Technical Evaluation Board's forms contained no explanation of deficiencies or weaknesses that caused the lower-than-maximum score. In addition, the advisory noted that the

[26] At the conclusion of this audit, the USMS informed us that the contracting officer responsible for this contract is no longer employed by the USMS.

[27] Appendix III contains a copy of the advisory.

[28] The Federal Acquisition Regulation requires that the "selection authority shall establish an evaluation team, tailored for the particular acquisition, that includes appropriate contracting, legal, logistics, technical, and other expertise to ensure a comprehensive evaluation of offers." In this case, the USMS contracting officer appointed a Technical Evaluation Board consisting of a U.S. Marshal, a Chief Deputy U.S. Marshal, two Deputy U.S. Marshals, and one employee from the Judicial Security Division.

DOJ OIG's July 2006 fraud alert had not been provided to the Technical Evaluation Board.[29]

The USMS responded to the advisory on July 28, 2009, outlining procedures that it would adopt to address the issues discussed in the advisory. According to the USMS response, USMS procurement officials will diligently comply with all USMS procurement policies and procedures. The USMS response further stated that the contracting officer or source selection authority will share all relevant information and concerns with members of the Technical Evaluation Board and that counsel and advice will be sought from authorized program, procurement, and legal officials prior to an award. The response also said that, in retrospect, the USMS agreed that USProtect's price was insufficient to perform the requirements of the contract and that the contracting officer should have used better judgment in this area. According to the USMS, it has since hired a more experienced contracting officer to manage and administer the Office of Security Contracts. The response also stated that the USMS will provide additional training for members of the Technical Evaluation Board.

Security Contract File Management

We also determined that the Office of Security Contracts lacks written policies that establish procedures for maintaining files on the selection of CSO contractors. According to an Office of Security Contracts official, the lack of organization of the security contract files makes it difficult for the USMS to defend against bid protests filed by vendors and claims filed by contractors. For example, this official cited a claim that was filed by one of the CSO vendors in 2006. In this case the contractor alleged that the USMS failed to pay more than $700,000 in properly submitted invoices. According to this official, because of poor documentation and file management the USMS was unable to defend against the claim. Ultimately, the USMS had to pay the vendor on the claim. Although the USMS later informed us that it did not believe the lack of payment was a result of poor documentation, the USMS acknowledged that it had not paid the properly submitted invoices. In February 2008, a bid protest was filed by a CSO contract bidder related to the replacement of USProtect and the USMS was unable to defend its selection of another bidder. Because of concerns related to how the solicitation was set up, lack of documentation, and an insufficient review and evaluation by the Technical Evaluation Board, the USMS conceded in November 2008. As a result of this protest we were informed that all

[29] While the initial meeting of the Technical Evaluation Board took place prior to the DOJ OIG's issuance of the fraud alert in July 2006, the USMS was in possession of this information prior to the Technical Evaluation Board's follow-up meeting in August 2006.

12 judicial circuits' primary CSO contracts were open for rebidding. According to the USMS, proposals have been received and are currently being reviewed, and the anticipated award date is October 2010 for all 12 circuits.

In our judgment, the USMS needs to implement procedures to improve its file management system as soon as possible. At the conclusion of our audit the USMS informed us that at future training for USMS Contracting Officer's Technical Representatives they will receive a folder that will serve as a checklist for the filing of documents and the tracking of invoices. We believe this is a good first step toward improving the USMS's file management system and we recommend that the USMS continue to evaluate its current contract file maintenance practices and develop procedures to ensure that all necessary documentation is maintained in a consistent manner. By doing so, we believe that the USMS could avoid the expenses and disruption related to future bid protests and other types of contract challenges.

Oversight of CSO Contractor Invoicing

Our audit also determined that the USMS's management of invoices for CSO work hours needs improvement. CSOs currently manually record their time on a paper timesheet. In each of the six districts we visited, the Judicial Security Inspector received the hard copy of the CSO sign-in sheets on a daily or weekly basis and reviewed the timesheets for accuracy. At the end of the month the Judicial Security Inspector compared these timesheets to the invoices and monthly hourly reports received from the contractor. In response to a questionnaire we submitted to the Judicial Security Inspectors at each of the district offices, several Judicial Security Inspectors expressed concern that the billing process is too cumbersome.

The absence of a streamlined timekeeping system in the districts increases the risk of human error, overbilling by the contractors, and fraud. Our review revealed timekeeping inaccuracies in all six districts we visited. Therefore, we recommend that the USMS seek to streamline its timekeeping practices for CSOs.

USMS Management of the Court Security Officer Program

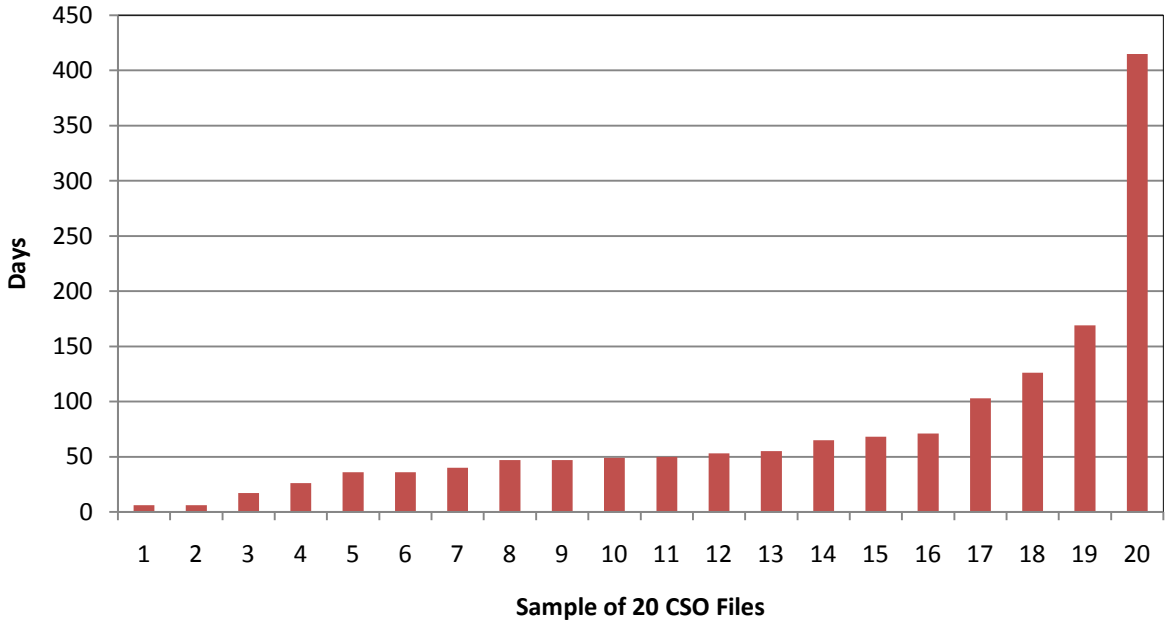
Our review of the Court Security Officer Program found that the USMS has failed to: (1) conduct timely background investigations for newly hired CSOs, (2) adequately utilize the data it collects on CSO performance violations, and (3) maintain adequate personnel records for its CSO workforce.

Background Investigations

Background investigations conducted by USMS district offices determine the suitability for the assignment of CSOs to the CSO contract. This investigation consists of individual interviews with CSO candidates, a review of past employment records, fingerprinting, criminal record checks, and a credit check. Background investigations are completed by the district and sent to USMS headquarters for adjudication and approval.

USMS policy requires that background check information and recommendations be submitted by the district office to its Office of Court Security within 21 days of the district office's receipt of the background investigation request. We tested a sample of 20 out of 213 CSOs hired between February and July of 2009. Overall, we found that 17 out of the 20 background investigations were submitted by the district office to the Office of Court Security after the 21-day requirement expired. These 17 untimely background investigations had an average processing time of 74 days. This included 1 investigation that took over 415 days for the district to complete.

Exhibit 5
USMS District Office Processing Times for
OIG Sample of CSO Background Investigations



Source: OIG Analysis of USMS records

According to one contractor, the delay in processing background investigations has caused a morale issue among the CSOs it employs.

This contractor stated that because of understaffing, it has had to restrict CSO leave requests and require overtime to cover shifts.

We recommend that the USMS perform a comprehensive review of its background investigation process for CSOs and seek to ensure that these investigations are consistently completed in a timely manner.

CSO Performance Violations

A performance violation is defined by the USMS as an infraction that violates the standards of competency, conduct, appearance, and integrity as outlined in the CSO contract. These infractions include allowing restricted items to pass through security and leaving firearms unsecured. Although the USMS maintains data on CSO performance violations, we concluded that the USMS does not utilize this data effectively.

According to the USMS it has a three-step process for reporting CSO performance violations: (1) the district office submits a request to the Office of Court Security that an alleged violation be investigated, (2) the Office of Security Contracts sends a letter to the CSO vendor and requests an investigation, and (3) the report of the vendor's investigation is sent to the Office of Security Contracts for USMS concurrence. Because CSOs are not USMS employees, the contractor must conduct the investigation and respond to the Office of Security Contracts with the results of its investigation. The contractor also must recommend and carry out appropriate disciplinary action for any performance violations. If Office of Security Contracts officials disagree with the contractor's findings, they can request the contractor to conduct further investigation or impose different disciplinary action. The USMS may also ask that the CSO be removed from the contract if the USMS does not agree with the contractor's course of action.

We were informed that CSO performance violations are tracked manually by both the Office of Court Security and the Office of Security Contracts. At our request, the USMS provided us with a breakdown of its CSO contract performance violations for FY 2008 through the first 10 months of FY 2010. The USMS expanded the number of categories it used to track these violations beginning in FY 2009. Exhibit 6 shows CSO contract performance violations by type for FY 2008 through the first half of FY 2010.

Exhibit 6 CSO Contract Performance Violations by Type Fiscal Years 2008, 2009, and 2010						
	FY 2008		FY 2009		FY 2010[30]	
Violation Type	**Violation Count**	**Percentage of Total**	**Violation Count**	**Percentage of Total**	**Violation Count**	**Percentage of Total**
Security Procedures	15	12.9	47	39.8	62	66.0
Misconduct	14	12.1	37	31.4	13	13.8
Abandonment of Post	N/A	N/A	8	6.8	2	2.1
Mishandled Firearm	3	2.6	8	6.8	3	3.2
Insubordination	N/A	N/A	4	3.4	N/A	N/A
Arrests	N/A	N/A	2	1.7	6	6.4
Sexual Harassment	N/A	N/A	2	1.7	5	5.3
Fraud	N/A	N/A	1	0.8	N/A	N/A
Solicitation	N/A	N/A	1	0.8	N/A	N/A
Threat	N/A	N/A	N/A	N/A	1	1.1
Other[31]	84	72.4	8	6.8	2	2.1
TOTALS	**116**	**100%**	**118**	**100%**	**94**	**100%**

Source: USMS

In addition, at our request, the USMS provided a breakdown of the actions taken to address performance violations. Exhibit 7 shows the action taken on CSO contract performance violations for FY 2008 through the first 10 months of FY 2010.

[30] Data is current through August 5, 2010.

[31] This category is used to track performance violations that do not fit the other established categories. For example, one of the cases categorized as "other" involved a CSO who was found to have several overdue and delinquent financial obligations during a routine background reinvestigation.

Exhibit 7 Action Taken on CSO Contract Performance Violations Fiscal Years 2008, 2009, and 2010						
	FY 2008		FY 2009		FY 2010[32]	
Action Taken	**Action Count**	**Percentage of Total**	**Action Count**	**Percentage of Total**	**Action Count**	**Percentage of Total**
Suspensions	35	30.2	34	28.8	18	19.1
Demotion & Warning	N/A	N/A	1	0.8	N/A	N/A
No Action	10	8.6	19	16.1	11	11.7
Pending[33]	23	19.8	29	24.6	38	40.4
Removal	21	18.1	13	11.0	9	9.6
Resignation	3	2.6	3	2.5	4	4.3
Warning	24	20.7	19	16.1	14	14.9
TOTALS	**116**	**100%**	**118**	**100%**	**94**	**100%**

Source: USMS

We believe that the USMS's expansion of performance violation categories is useful because the USMS can better determine the types of violations that are occurring. However, we believe that the USMS can utilize this data more effectively. For example, the USMS does not analyze its performance violation data to determine whether performance issues related to contractors in one circuit were occurring in another circuit. Additionally, at the time of our field work the USMS was not analyzing this data to assess potential CSO training needs, although we were told that the USMS is currently considering ways to utilize this data when developing future CSO training. We recommend that the USMS develop a method for analyzing its performance violation data to better understand violation trends and potential training needs among its CSO workforce.

One USMS official stated that Judicial Security Inspectors do not always report performance violations to USMS headquarters. This official indicated that on some occasions Judicial Security Inspectors handle the issues on a local level. Such an approach could lead to inconsistent

[32] Data is current through August 5, 2010.

[33] This category captures those violations that were pending at the close of the fiscal year.

reporting of performance violations and make it more difficult to gauge the extent of the problem and track resolution of corrective actions. In addition, it is difficult to seek the removal of a problem CSO if violations are not consistently reported to USMS headquarters. Therefore, we recommend that the USMS provide additional guidance to district Judicial Security Inspectors to ensure that all CSO performance violations are documented and reported to the Office of Security Contracts.

Maintenance of CSO Personnel Records

The USMS maintains an electronic database that contains information relating to CSOs' dates of hire, background investigations, medical records, firearms qualifications, and training certifications. The information contained in this database is based on personnel source documents maintained by USMS district offices. This electronic database is intended to provide an efficient method to track CSO personnel information. However, the USMS district offices are not able to update and access the database as needed. Instead, updates must be performed by USMS headquarters personnel. In addition, according to USMS officials, although the database stores this personnel information, it cannot be used to automatically alert the USMS of upcoming CSO requirements, such as needed training, firearms qualifications, and medical examinations.

We selected and reviewed a sample of 60 CSO personnel files for the requisite medical examination records and firearms qualifications. Generally, we found that the CSO personnel files were incomplete and poorly organized, which resulted in incomplete and inconsistent data in the CSO database.

According to the performance standards for all CSO contracts, the contractor must require the CSO to complete and pass an annual medical examination within 1 year of their last examination date. The medical examination is performed by a physician designated by the CSO contractor. A medical officer from the U.S. Public Health Service's Federal Law Enforcement Medical Program then reviews the results of the medical examination and determines whether the CSO is qualified to perform CSO job functions. If the CSO fails to complete and pass the examination, the CSO is disqualified and the contractor must prohibit the CSO from performing under the contract. However, we determined that 1 of the 60 selected files (2 percent) contained no medical examination records. In addition, 38 of the 60 files (63 percent) contained medical examination

records that were out of date because they indicated that the most recent examination occurred more than 1 year prior to our review of the files.[34]

In addition to the medical examination requirement, it is the responsibility of the contractor to ensure that all CSOs annually qualify on their firearm. However, our review of the same 60 CSO personnel files found that 11 of the 60 CSO files (18 percent) lacked firearm qualification records. In addition, 28 of the 60 files (47 percent) contained firearms qualifications that were out of date.[35]

Our limited file review presents serious concerns regarding the medical and firearms qualifications for CSOs. Without adequate personnel file maintenance it is difficult for USMS management to ensure that all CSOs are fit for duty. If a CSO is not fit for duty, this could lead to safety risks for other CSOs and those they are charged with protecting. We recommend that the USMS evaluate its personnel file maintenance practices and develop procedures to ensure that all necessary documentation, such as medical and firearms qualifications, is adequately maintained and up to date. In addition, we believe that the USMS should assess the feasibility of implementing an automated system for tracking important dates in the database to ensure that the CSOs satisfy their qualification requirements in a timely manner.

Conclusion and Recommendations

The workforce of more than 5,000 CSOs represent the first line of defense in the USMS's efforts to secure federal court facilities. However, we found that the USMS's management of its court security officer program and related contracts needs significant improvement. A general lack of oversight by the Office of Security Contracts has resulted in inefficiencies and in some cases major breakdowns in the contract review and approval process. In addition, the USMS is not completing background investigations for newly hired CSOs in a timely manner. Further, the USMS's failure to analyze performance violations has made it difficult for the USMS to understand CSO performance violation trends and to identify potential training needs. The

[34] The USMS provided us with the 60 CSO personnel files on December 4, 2009. Because USMS policy requires a CSO to receive an annual medical examination within 1 year of the previous examination, we considered a CSO personnel file to contain out-of-date medical examination records if the file did not contain evidence of a medical examination that occurred between December 3, 2008, and December 4, 2009.

[35] The USMS provided us with the 60 CSO personnel files on December 4, 2009. Because USMS policy requires a CSO to qualify on their firearm once per calendar year, we considered a CSO personnel file to contain an outdated firearms qualification record if the file lacked a record for calendar years 2008 and 2009.

USMS's failure to ensure that firearms qualifications and medical examinations are adequately documented could lead to safety risks for CSOs and those they are charged with protecting.

We recommend that the United States Marshals Service:

6. Continue to evaluate its current contract file maintenance practices and develop procedures to ensure that all necessary documentation is maintained in a consistent manner.

7. Seek to streamline its current time keeping practices for CSOs.

8. Perform a comprehensive review of its background investigation process for CSOs and seek to ensure that these investigations are completed in a timely manner.

9. Develop a method for analyzing its performance violation data to better understand violation trends and potential training needs among its CSO workforce.

10. Provide additional guidance to district Judicial Security Inspectors to ensure that all CSO performance violations are documented and reported to the Office of Court Security.

11. Evaluate its CSO personnel file maintenance practices and develop procedures to ensure that all necessary documentation, such as medical and firearms qualifications, is adequately maintained and up to date. In addition, the USMS should assess the feasibility of implementing an automated system for tracking important dates in the database to ensure that the CSOs satisfy their qualification requirements in a timely manner.

Management of Security Systems and Security System Contracts

Our audit found that the USMS does not maintain custody of the inventory records for the security systems equipment obtained through its nationwide security systems contract. The USMS also does not enter such equipment in its property management system. Instead, the USMS relies on the contractor to maintain and update its security systems equipment inventory. In addition, the USMS told us that it has no maintenance agreements for the millions of dollars worth of sophisticated screening equipment deployed at court facilities throughout the country that are obtained outside of the nationwide security systems contract.

Oversight of the Nationwide Security Systems Contract

A nationwide security systems contract covers the purchase, installation, and maintenance of duress and intruder alarms, closed-circuit televisions, intercoms, and access-control systems at federal courthouse facilities. The security systems contract is awarded for a 1-year term with 4 option years. The nationwide security systems contract is currently held by ADT, who according to one USMS official has held the contract with the USMS for the last 16 years.

The USMS Contracting Officer's Technical Representatives for the nationwide security systems contract are located at USMS headquarters. District Judicial Security Inspectors assist the Contracting Officer's Technical Representatives with the day-to-day oversight of the contract in the district offices.[36] For example, if a security camera needed to be installed at a courthouse and the contractor sends someone to perform the work, the Judicial Security Inspector in that district typically certifies that the work was performed.

According to USMS policy, the contractor documents the work performed on site and the U.S. Marshal or designee must sign a service call report verifying that the work was completed and the number of contractor hours listed is accurate. The U.S. Marshal or designee should also ensure that the equipment is operating properly or indicate otherwise on the service call report. However, we were told that in most circumstances the district offices do not supervise the work being performed by the contractor. Therefore, because labor hours are not always being monitored it is difficult for the USMS to consistently ensure that the labor hours claimed were actually worked by the contractor. We believe that this failure to supervise the work performed leaves the USMS vulnerable to fraud and potential overbilling. We recommend that the USMS require district offices to supervise and verify labor hours claimed by contractors to help ensure that it is not being overbilled under the nationwide security systems contract.

Oversight of Security System Inventory and Maintenance

The USMS's nationwide security systems contract covers the purchase, installation, and maintenance of surveillance cameras, duress alarms, monitors, and access control systems for courthouses. However, the USMS does not maintain recordkeeping custody over this equipment nor does it enter this equipment into the USMS property management system.

[36] According to the USMS, all Judicial Security Inspectors receive Contracting Officer's Technical Representative training and are required to be recertified every 2 years.

In accordance with the nationwide security systems contract the USMS relies on the private contractor, ADT, to maintain and update its inventory.

Maintenance fees charged on the ADT contract are assessed on a per item basis. Therefore, if the USMS does not ensure that items no longer in use are removed from ADT's inventory, it could result in significant overcharges. According to one USMS official, the USMS may have overpaid ADT between $10 million and $12 million for unnecessary annual maintenance fees over the past 5 years.[37]

At three of the six districts we visited, we found that the Judicial Security Inspectors maintained copies of inventory listings that they used to confirm whether inventory items were no longer in use. However, according to district officials in one of these three districts, despite informing ADT that certain items were no longer in use, ADT failed to remove them from the annual inventory and continued to charge the USMS for the maintenance of this equipment.

According to USMS headquarters officials, because the contractor's technicians add and remove equipment daily, they believe their involvement in the annual inventory process would introduce administrative burdens and costs. However, we believe that the USMS should be more proactive in the inventory process by maintaining local inventory records that should help avoid unwarranted maintenance fees.

Therefore, we recommend that the USMS assess the feasibility of district offices maintaining their own security system equipment inventories of equipment maintained by the contractor so that comparisons can be made to the contractor's inventory to avoid unwarranted maintenance fees. Without such practices, the USMS district offices cannot perform regular checks of the security system inventory to ensure that they are not being billed for maintenance fees for equipment no longer in use.

Maintenance of Screening Equipment

In addition to the security systems obtained through the nationwide security systems contract, the USMS also acquires security screening equipment, including X-ray machines, walkthrough metal detectors, and explosives detection units, through various procurement methods. This screening equipment is not purchased under a specific USMS contract and is maintained by the USMS.

[37] We did not audit the ADT contract. Therefore, we could not independently verify the estimated dollar amounts provided by this USMS official.

In contrast to the maintenance plan contained in the nationwide security systems contract, we found that the USMS has no maintenance agreements for the millions of dollars worth of sophisticated screening equipment deployed at court facilities throughout the country. During our review, we found that when X-ray machines and metal detectors were in need of repair they were out of service anywhere from 1 day to several weeks. According to an Office of Security Systems official, the USMS previously conducted an analysis and determined that maintenance plans for this equipment were not cost effective. However, this official also told us that he was unsure whether the USMS was assessing the impact of downtime on court security. Although we do not question the results of the USMS's analysis, we recommend that the USMS track the cost of repairs for its screening equipment and the impact of downtime on court security in order to periodically assess whether a maintenance plan for such screening equipment would be cost effective. By periodically reassessing the need for a maintenance plan, the USMS can ensure that the most cost-effective method is being used for the maintenance of these items.

Oversight of Contractor Performance

The Federal Acquisition Regulation (FAR) requires that performance evaluations be prepared at the time the work under the contract or order is completed. Past performance evaluations provide information about a potential contractor's ability to perform the contract successfully. The evaluation should contain current and relevant information, source of the information, context of the data, and general trends in a contractor's performance. In addition, for contracts or orders with a performance period exceeding 1 year, interim evaluations are prepared according to the government agency's specifications in order to provide current information for source selection purposes, contracts, or orders. The USMS and other agencies use this information as part of the analysis conducted during the solicitation award process to determine if a vendor can successfully perform on new contracts.

A USMS official that we interviewed acknowledged that the Office of Security Contracts was not reporting contractor performance as required by the FAR. According to this USMS official, the USMS no longer submits this information because the staff member formerly responsible for this task has retired and no one has been assigned to this duty.

This failure to report contractor performance hinders the USMS's ability to evaluate contractors who bid on new contracts. We therefore

recommend that the USMS require the Office of Security Contracts to prepare past performance and interim evaluations in accordance with the FAR.

Conclusion and Recommendations

We were told that in most circumstances that USMS district offices do not supervise the work being performed by the contractor under the nationwide security systems contract. Because this work is not always being monitored it is difficult for the USMS to consistently ensure that the claimed labor hours are actually worked by the contractor. We believe that a lack of supervision of the work performed under the nationwide security systems contract leaves the USMS vulnerable to fraud and potential overbilling. We therefore recommend that the USMS require district offices to supervise and verify labor hours claimed by contractors to help ensure that it is not being overbilled under the nationwide security systems contract. We also found that the USMS does not currently monitor the inventory records for the equipment obtained under the nationwide security systems contract, which may have led to the payment of unwarranted maintenance fees to the contractor. Accordingly, we recommend that the USMS assess the feasibility of district offices maintaining their own security system equipment inventories so that comparisons can be made to the contractor's inventory.

The USMS has no maintenance agreements for the screening equipment it deploys at court facilities throughout the country. We were informed that X-ray machines and metal detectors in need of repair were out of service for extended periods of time. We recommend that the USMS track the cost of repairs for screening equipment and assess the impact of downtime on court security in order to periodically assess whether a maintenance plan for its screening equipment would be cost effective. We also believe that the USMS should ensure that the Office of Security Contracts prepares past performance and interim evaluations for its contractors as required by the FAR.

We recommend that United States Marshals Service:

12. Require district offices to supervise and verify labor hours claimed by contractors to help ensure that it is not being overbilled under the nationwide security systems contract.

13. Assess the feasibility of district offices maintaining their own security system equipment inventories of equipment maintained by the contractor so that comparisons can be made to the contractor's inventory to avoid unwarranted maintenance fees.

14. Track the cost of repairs for its screening equipment and the impact of downtime on court security in order to periodically assess whether a maintenance plan for its screening equipment would be cost effective.

15. Require the Office of Security Contracts to prepare past performance and interim evaluations in accordance with the Federal Acquisition Regulation.

STATEMENT ON INTERNAL CONTROLS

As required by the *Government Auditing Standards*, we tested, as appropriate, internal controls significant within the context of our audit objective. A deficiency in an internal control exists when the design or operation of a control does not allow management or employees, in the normal course of performing their assigned functions, to timely prevent or detect: (1) impairments to the effectiveness and efficiency of operations, (2) misstatements in financial or performance information, or (3) violations of laws and regulations. Our evaluation of the United States Marshals Service's internal controls was *not* made for the purpose of providing assurance on its internal control structure as a whole. The United States Marshals Service's management is responsible for the establishment and maintenance of internal controls.

As noted in this report, we identified deficiencies in the United States Marshals Service's internal controls that are significant within the context of the audit objective and based upon the audit work performed that we believe adversely affect the United States Marshals Service's ability to effectively manage: (1) the CSO contract procurement process and (2) the daily oversight of its CSO contracts and nationwide security systems contract.

Because we are not expressing an opinion on the United States Marshals Service's internal control structure as a whole, this statement is intended solely for the information and use of the United States Marshals Service. This restriction is not intended to limit the distribution of this report, which is a matter of public record.

STATEMENT ON COMPLIANCE WITH LAWS AND REGULATIONS

As required by the *Government Auditing Standards* we tested, as appropriate given our audit scope and objective, selected transactions, records, procedures, and practices, to obtain reasonable assurance that the United States Marshals Service's management complied with federal laws and regulations, for which noncompliance, in our judgment, could have a material effect on the results of our audit. The United States Marshals Service's management is responsible for ensuring compliance with applicable federal laws and regulations. In planning our audit, we identified the following laws and regulations that concerned the operations of the auditee and that were significant within the context of the audit objective:

- Federal Acquisition Regulation (FAR)
- Homeland Security Presidential Directive 20 (HSPD-20)
- Federal Continuity Directive 1 (FCD 1)

Our audit included examining, on a test basis, the United States Marshals Service's compliance with the aforementioned laws and regulations that could have a material effect on United States Marshals Service's operations, through interviewing auditee personnel and examining procedural practices.

As noted in this report, we found that some of the United States Marshals Service's district offices that we visited did not comply with FCD 1, which requires a minimum of an annual review of Continuity of Operations Plans with updates throughout the year as necessary. In addition, we found that the United States Marshals Service did not comply with the FAR in its selection of a particular CSO contractor. The United States Marshals Service also failed to comply with the FAR by not reporting contractor performance.

APPENDIX I

OBJECTIVE, SCOPE, AND METHODOLOGY

Audit Objective

The objective of this audit was to assess the USMS's oversight of its Judicial Facilities Security Program.

Scope and Methodology

We conducted this performance audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objective. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objective. In general, our audit covered but was not limited to the period of fiscal years 2004 through 2009.

To accomplish our objective we interviewed USMS headquarters officials, reviewed USMS policies and procedures, and obtained and analyzed data pertinent to the USMS's court security programs, including a review of CSO personnel files. We also conducted an in-depth review of the procurement process for a CSO contractor whose contract was later terminated. Additionally, we conducted site work at six USMS district offices. At each district office location, we interviewed the local Judicial Security Inspector, obtained documents pertinent to local court security operations, received a tour of the court facilities, and interviewed members of the federal judiciary, including Chief Judges. Finally, we disseminated a questionnaire to the Judicial Security Inspectors in each district office concerning management of the CSO contracts and security equipment.

District Offices Visited

We identified the judicial circuits that were covered by each primary CSO contractor and judgmentally selected six USMS district offices that were geographically dispersed throughout the United States. Then, within each sample district, we selected specific federal court facilities to visit.

CSO Personnel Files

We selected a judgmental sample of 60 CSO personnel files from a universe of 7,312 records of CSO statuses that were active, new, pending, and shared between April 1, 1983, and September 17, 2009. We reviewed these 60 CSO personnel files to determine if they contained up-to-date medical examination records and firearms qualifications. Ultimately, we determined that 1 of the 60 files contained no medical examination record, while 38 of the personnel files contained medical examination records that were out of date.[38] Our review also determined that 28 of the 60 CSO files contained firearm qualifications that were out of date, while 11 of the files contained no firearms qualification records.[39]

We also selected a judgmental sample of 20 background investigation records for 213 CSOs hired between February and July of FY 2009 to determine whether these background investigations were completed in prescribed USMS timeframes. We determined that 17 of the 20 were untimely.

Our sample selection methodology was not designed with the intent of projecting our results to the total population of CSO personnel files or background investigation records.

[38] The USMS provided us with the 60 CSO personnel files on December 4, 2009. Because USMS policy requires a CSO to receive an annual medical examination within 1 year of the previous examination, we considered a CSO personnel file to contain out-of-date medical examination records if the file did not contain evidence of a medical examination that occurred between December 3, 2008, and December 4, 2009.

[39] The USMS provided us with the 60 CSO personnel files on December 4, 2009. Because USMS policy requires a CSO to qualify on their firearm once per calendar year, we considered a CSO personnel file to contain an outdated firearms qualification record if the file lacked a record for calendar years 2008 and 2009.

PRIOR OIG REPORTS

USMS – Court Security Officer Program (2000)

In 2000, the OIG issued a report on the USMS's Court Security Officer Program. The OIG found that the overwhelming majority of U.S. Marshals and Chief Judges surveyed indicated that they were satisfied with the CSO Program. At the same time, however, there was a strong undercurrent of concern among USMS employees and members of the judiciary regarding the management of the program, and the efficacy of using contract employees for judicial security. The report noted that the CSO Program at the time was a highly centralized operation. Procurement of the CSO contracts, as well as management of the program was largely a headquarters function. The districts dealt directly with contractors in some respects, such as bill-paying and timekeeping. But most decision-making matters, such as hiring, firing, and disciplinary actions were funneled through a handful of contracting officers and program managers at USMS headquarters, who managed the program for the districts. According to the report, as the program grew over the years, the centralized manner in which the program was run gave rise to a great deal of frustration on the part of those involved. These concerns brought into question whether the program of the size and breadth of the CSO program could be effectively managed in a highly centralized environment.

The OIG also noted (though not a serious problem at the time) that the potential for CSO strikes had become a concern among members of both the USMS and the judiciary. With unionization came the threat, already realized, of CSO strikes. And as the services provided by contract CSOs continued to expand, the report noted the greater potential impact on security operations should a future disruption in that service occur as a result of union or contract disputes.

The OIG also noted that the CSO contracts had become a lightning rod for legal challenges. Protests over the contracting process were on the rise, culminating in a barrage of protests related to a recent round of contract awards in early 1999. Some USMS officials believed these protests were a by-product of the growth in the program and the millions of dollars at stake in the large circuit-wide contracts. Although the USMS had successfully defended against most of the protests filed, it appeared that the trend was such that the legal challenges associated with these large circuit-wide contracts were becoming a cost of doing business.

Because of the conflicting nature of the evidence obtained, the OIG was reluctant to recommend a singular course of action. Instead, the report suggested several options available to the USMS: (1) continue utilizing the current CSO contracts, (2) eliminate the contract operation by converting contract guards to federal employees, or (3) effect a partial conversion by stratifying the current guard force into two separate units, one contract, and the other federal. The federal force would be used for courtroom security, while building security would remain a contract operation.

The OIG also noted several areas of concern regarding the CSO Program at the operational level. At the time, the Administrative Office of the United States Courts (AOUSC) reimbursed the USMS for program-related administrative costs incurred only at the headquarters level. However, the OIG estimated that the USMS incurred about $2.8 million annually in administrative costs at the district level, for which it was not reimbursed. Consequently, the USMS, in effect, subsidized the AOUSC-funded program in the amount of these unrecognized costs.

There was also a concern among a number of U.S. Marshals that CSOs did not receive adequate training for the duties required of them. U.S. Marshals identified needed subject areas of training ranging from bomb detection and anti-terrorist programs, to cardiopulmonary resuscitation (CPR) and people skills. The report found that there was no provision in the CSO contracts for in-service training.

The report also noted some internal control issues, which the OIG believed may have had an impact on security operations. For example, unannounced tests of security screening posts were being conducted on a quarterly basis, as required by USMS policy, at only 5 of the 16 district offices the OIG reviewed. Unannounced tests at the other 11 districts were conducted either infrequently, or in some cases not at all. Additionally, a number of CSOs' security clearances and medical certifications could not be verified because documentation was not consistently maintained at the district level.

Background Investigations Conducted by the USMS (2005)

This OIG 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, the report 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. The OIG analysis also showed that investigations were slow, and neither investigations nor adjudications were consistently thorough.

Specifically, the OIG found that the USMS placed or retained personnel in national security or public trust positions without complete investigative information. The OIG 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. The OIG 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. The report stated that by correcting these deficiencies, the USMS could better ensure that the individuals assigned to its national security and public trust positions have been thoroughly screened.

Review of the Protection of the Judiciary and the United States Attorneys (2009)

This OIG review found deficiencies in the response to threats by the USMS and the Executive Office for U.S. Attorneys (EOUSA). As a threshold matter, the OIG report found that threats against judges, U.S. Attorneys and Assistant U.S. Attorneys are not consistently and promptly reported. Moreover, the report stated that when threats were reported the USMS did not consistently provide an appropriate response for the risk level posed by the threat. In addition, the USMS did not fully or effectively coordinate with other law enforcement agencies to respond to threats against federal judicial officials. In addition, the report stated that coordination on threat responses among EOUSA, the United States Attorneys, and the USMS is inconsistent.

OIG MANAGEMENT ADVISORY MEMORANDUM AND USMS RESPONSE

U.S. Department of Justice
Office of the Inspector General

June 17, 2009

MANAGEMENT ADVISORY MEMORANDUM FOR:

JOHN F. CLARK
DIRECTOR
UNITED STATES MARSHALS SERVICE

FROM: RAYMOND J. BEAUDET
ASSISTANT INSPECTOR GENERAL
FOR AUDIT

SUBJECT: Immediate Improvements Necessary for the Judicial Security Division's Court Security Procurement Process

This memorandum is to advise you of significant issues identified during the course of our ongoing audit of the United States Marshals Service's (USMS) oversight of court security. We began our audit on January 15, 2009, and since that time have identified significant concerns relating to the USMS's procurement practices. We also learned that the USMS is in the process of developing solicitations for future court security contracts to be awarded later this year. Although our audit has not yet concluded, this memorandum provides early notification of significant issues that we have identified to date. We believe that these are serious concerns that require the USMS's immediate attention and corrective action. We plan to include in our audit report the information presented in this memorandum, along with any corrective actions that the USMS has implemented before our report is issued. Therefore, we request that within 30 days of this memorandum, the USMS provide us with a written response describing how the USMS plans to address the concerns described below.

Background

The USMS Judicial Security Division's Office of Court Security is responsible for ensuring the safety of the judiciary at federal court facilities throughout the country. The Court Security Officer (CSO) program is the primary mechanism used to accomplish this goal. Within the Office of Court Security, the Office of Security Contracts is responsible for procuring the

services of roughly 4,700 CSOs that are deployed at over 400 facilities nationwide.

The CSO contracts are structured as multi-million dollar contracts with security guard vendors that include providing protection through CSOs at court facilities in each of the 12 judicial circuits. For example, the CSO contract for the 9th Judicial Circuit includes federal court facilities in Alaska, Arizona, California, Guam, Hawaii, Idaho, Montana, Nevada, the Northern Mariana Islands, Oregon, and Washington. Therefore, problems associated with a particular vendor or contract may affect the safety of court operations in numerous court facilities throughout the country.

In September 2006, the USMS awarded 3 of its 12 CSO contracts to a security guard company, USProtect Corporation (USProtect). The three CSO contracts awarded to USProtect totaled $300 million to provide court security officers for the 3rd, 5th, and 12th Judicial Circuits.[1] Each contract was for 1 base year with four 1-year options. The contracts for the 3 judicial circuits encompassed federal court operations within 15 USMS districts and involved the hiring, training, and supervision of roughly 800 contract guards to be deployed to the numerous federal court facilities within the 3 judicial circuits.

On March 16, 2008, USProtect filed for Chapter 7 bankruptcy protection after the USMS Office of Security Contracts decided not to renew their contracts with USProtect and other federal agencies terminated their contracts with the company amid allegations of fraud and mismanagement. USProtect's financial collapse left many CSOs without compensation for their services. In the months leading up to the contract renewal award, the Office of Security Contracts began taking steps to re-bid the CSO contracts for the 3rd, 5th, and 12th Judicial Circuits, which succeeded in minimizing the disruption of security services when the USMS did not renew its contract with USProtect. However, our audit determined the USMS Office of Security Contracts was aware of USProtect's problems even before the initial contracts were awarded, yet ignored them.

Upon learning of the USProtect issue, we set out to determine how the USMS managed its procurement process with regard to USProtect, whether it complied with the Federal Acquisition Regulation (FAR) and its own procurement policies, and whether the situation described above could have been avoided. To accomplish this task, we interviewed USMS employees

---

[1] The 3rd Judicial Circuit includes federal court facilities in the states of Delaware, New Jersey, and Pennsylvania, as well as the U.S. Virgin Islands. The 5th Judicial Circuit includes federal court facilities in the states of Louisiana, Mississippi, and Texas. The 12th Judicial Circuit includes court facilities in the District of Columbia and the Northern Virginia Judicial District.

related to the CSO procurement process, including the Office of Security Contracts and Office of General Counsel.[2] In addition, we reviewed the documents that were available in the solicitation and contract files. Our focus was on actions, or the lack of actions taken, before the CSO contracts were awarded to USProtect.

We identified significant concerns relating to the USMS's procurement practices leading up to its selection of USProtect as a CSO vendor including its lack of compliance with the FAR and USMS procurement policies. Specifically, these concerns relate to the USMS's: lack of adequate background research on USProtect, an inadequate determination of responsibility of USProtect, selection of USProtect despite concerns with bids that were disproportionately low in comparison to other bids, and an inadequate technical review by the Technical Evaluation Board. Had the USMS complied with the FAR and its required procurement practices, we believe that it could have avoided the situation brought about by the collapse of USProtect. The following paragraphs discuss these issues in more detail.

Lack of Due Diligence in USMS's Background Research

We identified a lack of due diligence on the part of USMS employees within the Office of Security Contracts and Office of General Counsel in researching available information regarding USProtect. On July 17, 2006, the U.S. Department of Justice Office of the Inspector General (OIG) issued Fraud Alert 2006-02 to the USMS concerning USProtect, formerly known as Holiday International Security, Inc. (Holiday International), and its Chief Financial Officer, Richard Hudec. This fraud alert contained a prior fraud alert issued in May 2005 by the Social Security Administration Office of the Inspector General (SSA OIG) concerning Mr. Hudec. The SSA OIG memorandum detailed a string of criminal convictions and civil judgments against Mr. Hudec occurring over a 12-year period, all of which were related to fraud.[3] The final civil judgment

---

[2] The USMS Office of Security Contracts is responsible for awarding and managing the CSO contracts. The Office of General Counsel reviews vendor selections and other legal matters related to the CSO contracts in order to protect the USMS's interests.

[3] The SSA OIG fraud alert identified the following incidents of fraud committed by Mr. Hudec:

1. In 1990, Mr. Hudec pled guilty to mail fraud for submitting a false insurance claim. He was placed on 5 years probation and ordered to make restitution of $27,139.
2. In 1991, Mr. Hudec pled guilty to mail fraud for submitting another false insurance claim. He was sentenced to 6 months in prison and 5 years of probation.
3. In 1998, Mr. Hudec pled guilty to bank fraud for falsifying documents, forging signatures on a check, and depositing the check into an account from which he withdrew the money. He was sentenced to 28 months in prison, followed by 5 years of supervised release, and ordered to pay $168,000.

occurred in March 2002. According to the SSA OIG's fraud alert, Mr. Hudec held various executive positions in USProtect since 2001, including Chief Financial Officer. The alert ended with the following advisory statement: "The Purpose of this memo is to make you aware of this issue and recommend you review any contracts you may have with USProtect for potential fraud, such as false statements."

The FAR Subpart 15.305(a)(2)(iii) requires that the evaluation of prospective vendors "should take into account past performance information regarding predecessor companies, key personnel who have relevant experience . . . ." According to the fraud alert, Mr. Hudec had been a principle in Holiday International. The alert noted that Mr. Hudec's wife purchased 100 percent of that company's assets and renamed the company USProtect Corporation. Further, the fraud alert indicated that Mr. Hudec continued to hold various management positions in USProtect.

Despite these facts, we found no evidence in our review of USMS's contract files and interviews with USMS personnel of any research conducted on Holiday International or its key personnel, including Mr. Hudec. Instead, we found that the USMS officials responsible for awarding the contract accepted at face value USProtect's statement that Mr. Hudec was not involved in any way with the company owned by his spouse, even though USProtect's statement was contradicted by the fraud alert's statement that Mr. Hudec continued to hold various management positions in USProtect. We believe that the fraud alert forwarded by the DOJ OIG warranted a review of USProtect and its predecessor company, Holiday International. If such a review were performed, it would have become apparent to the USMS that the principal officers with Holiday International remained active with USProtect. This information would have provided justification to award the contract to another vendor, avoiding the situation that occurred in March 2008 when USProtect filed for bankruptcy protection after the USMS did not renew its contracts, leaving many CSOs without compensation for their services.

Determination of Responsibility

The FAR Subpart 9.105-1 requires that "before making a determination of responsibility, the Contracting Officer shall possess or obtain information sufficient to be satisfied that a prospective contractor currently meets the

---

4. In April 1999, Mr. Hudec had five civil judgments entered against him for receiving money, services, and credit based on false pretenses, false representations, and actual fraud. The five civil judgments amounted to a total of $1,282,016 in favor of five banks.
5. In March 2002, Mr. Hudec had a civil judgment entered against him for $191,437 in favor of a bank.

applicable standards in 9.104."[4] We found that the Office of Security Contracts lacked sufficient information to make a "determination of responsibility" for USProtect, and therefore lacked the proper justification for awarding the CSO contracts to USProtect. Given the severity of the charges contained in the OIG fraud alert and Mr. Hudec's suspected involvement in USProtect's operations, the USMS Contracting Officer should have obtained more information regarding Mr. Hudec's involvement with the company and its principles before making a determination of responsibility.

According to the USMS Contracting Officer, during contract negotiations she requested from USProtect an explanation as to whether Mr. Hudec was involved with the company. The Contracting Officer received in response a written statement from USProtect stating "Mr. Hudec is the Spouse of USProtect's 100% shareholder. Mr. Hudec is not a corporate officer or employee of USProtect Corporation." Based on this short disavowal of Mr. Hudec's involvement in USProtect, the Contracting Officer dismissed the information in the OIG's and SSA OIG's fraud alerts. No further documentation was requested by the Office of Security Contracts or the Office of General Counsel, nor was any provided by USProtect. Further, we determined through interviews with the USMS Contracting Officer and Associate General Counsel that neither the Office of General Counsel nor the Office of Security Contracts contacted the OIG or the SSA OIG regarding the information contained in the fraud alert. Given the serious nature of the information and the concerns regarding potential fraud including false statements, we believe that the USMS should have requested additional information in order to protect the USMS's interest and ensure that the company was responsible.

---

[4] The FAR Subpart 9.104 includes the following general standards: To be determined responsible, a prospective contractor must—

(a). Have adequate financial resources to perform the contract, or the ability to obtain them;
(b). Be able to comply with the required or proposed delivery or performance schedule, taking into consideration all existing commercial and governmental business commitments;
(c). Have a satisfactory performance record. A prospective contractor shall not be determined responsible or nonresponsible solely on the basis of a lack of relevant performance history, except as provided in 9.104-2;
(d). Have a satisfactory record of integrity and business ethics.
(e). Have the necessary organization, experience, accounting and operational controls, and technical skills, or the ability to obtain them (including, as appropriate, such elements as production control procedures, property control systems, quality assurance measures, and safety programs applicable to materials to be produced or services to be performed by the prospective contractor and subcontractors).
(f). Have the necessary production, construction, and technical equipment and facilities, or the ability to obtain them; and
(g). Be otherwise qualified and eligible to receive an award under applicable laws and regulations.

Further, the Office of Security Contracts disregarded internal concerns raised during a pre-solicitation review conducted by the USMS Procurement Policy Oversight Team (PPOT). USMS Procurement Policy 04-1 requires that all solicitations, invitation for bids, and request for quotations with a total life cost over $100,000 be reviewed by the PPOT prior to execution. In addition, the same USMS policy requires that all actions with a life cycle cost over $500,000 be reviewed first by PPOT and then by the USMS Office of General Counsel. The three CSO solicitations ranged in value from $94 million to $128 million, and thus each was valued at well over $500,000.[5] The purpose of the PPOT review is to ensure the USMS complies with the FAR and internal USMS policies before the USMS awards a contract. As part of the PPOT, the USMS Procurement Chief reviews contracts and solicitations for potential concerns and issues a memorandum to the Contracting Officer that includes, if necessary, findings and recommendations that need to be addressed in writing before the Contracting Officer awards the contract.[6]

The PPOT completed its review of the three solicitations and issued to the Office of Security Contracts its written findings in a memorandum, dated September 21, 2006, signed by the USMS Procurement Chief. This memorandum titled, "Pre-Solicitation Review for contract DJMS-07-D0001, 0002, and 0003 3rd, 5th & 12th Circuit Contracts for CSOs," detailed eight significant issues that should have precluded a "determination of responsibility" for USProtect. The memorandum referenced the FAR Subpart 9.103, which requires that, "in absence of information clearly indicating that the prospective contractor is responsible, the Contracting Officer shall make a determination of non-responsibility."

Specifically, the PPOT's memorandum questioned the lack of information used to make a determination of responsibility regarding USProtect. The memorandum stated that USProtect's "self-serving statement" was not sufficient to address the concerns raised in the OIG fraud alert. Our file review found no indication that the PPOT's concerns were addressed by the Office of Security Contracts or the Office of General Counsel or that these offices followed up on the fraud alert. The USMS's procurement policies require that, "Contracting officers/Contract Specialists must address all findings either by making the necessary changes or by preparing written justification for not accepting the findings. The written justifications will cite applicable policies, regulations, and/or status." Further the policy requires that, "[b]efore

---

[5] The solicitation for the 3rd Circuit had an Independent Government Cost Estimate (IGCE) totaling approximately $107 million for the 5-year life of the contract. Further, the IGCE for the 5th Circuit totaled over $128 million and the 12th Circuit totaled approximately $94 million. Therefore, all three solicitations required PPOT and Office of General Counsel review.

[6] USMS Procurement Policy 04-1 requires that PPOT findings need to be addressed in writing, but there is no requirement for the written response to be provided back to the PPOT.

proceeding with the action, the file must contain a copy of the findings, documentation of the changes made, and the written approval for the Contracting Officer's/Contract Specialist's supervisor for any decision not to accept a finding or findings." We reviewed all of the solicitation and award files and found no written response, justification, or approval by the Contracting Officer's supervisor to disregard PPOT findings as required by the USMS's procurement policies.

With regard to the Associate General Counsel's review, we were unable to verify whether it received a copy of the PPOT memorandum prior to its determination that there were "no legal impediments" to awarding the CSO contracts to USProtect. The Associate General Counsel stated that he normally would receive the PPOT review with the file, but could not recall whether he had reviewed the PPOT memorandum for the USProtect contracts. An e-mail confirms that the USMS Associate General Counsel provided approval of the contract on the morning of September 22, 2006, after asking if the PPOT review had been completed on September 21, 2006. However, there was no indication that the USMS Office of General Counsel received or reviewed the PPOT's review prior to communicating his approval to award the contracts. According to the USMS Procurement Chief, she indicated that she had not been contacted by the Office of General Counsel to discuss her findings.

The legal concerns raised in the PPOT memorandum should have alerted the Office of General Counsel and prompted the Associate General Counsel to look into this matter before giving his concurrence on USProtect's selection for the three CSO Contracts. The only documentation we found in our file review showing any involvement from the Office of General Counsel were: (1) a Memorandum For Record prepared by the Office of Security Contracts and edited by the Associate General Counsel before the PPOT conducted its review, which included instructions from the Associate General Counsel for the Office of Security Contracts to seek additional clarification on Mr. Hudec's involvement with USProtect; and (2) an email sent after the PPOT review from the Associate General Counsel to the Contracting Officer stating that the Associate General Counsel saw no legal impediment to awarding the contract to USProtect.

The failure to address and further research each of the issues detailed in the PPOT memorandum issued by the USMS Procurement Chief raises serious concerns about the USMS's court security procurement process. In this instance, there were incidents of fraud that were not taken into consideration by USMS staff before awarding the three contracts totaling approximately $300 million to USProtect. Based on the lack of documentation and the responses we received during our interviews, we believe that the USMS did not conduct a proper investigation or background research on USProtect. Also, the USMS Office of Security Contracts did not properly address the concerns raised in the PPOT memorandum. Had these actions been taken, there would have

been sufficient justification to select another vendor, thereby avoiding the financial and security risks associated with the collapse of USProtect.

As a result, we found that the USMS did not exercise due diligence in its awarding of CSO contracts for the 3rd, 5th, and 12th Judicial Circuits to USProtect. In our judgment, the Office of Security Contracts and the Office of General Counsel dismissed without sufficient research serious concerns raised by the OIG fraud alert and the USMS's PPOT regarding the USMS Contracting Officer's determination of responsibility. In not acting upon the concerns that were raised, the Office of Security Contracts chose to rely on USProtect's self-serving statement, which was insufficient justification for awarding the contracts.

USProtect's Price was Insufficient to Cover Program Costs

The FAR requires that contracting officers perform a cost estimate to ensure that the vendors' bids and proposed costs are sufficient to cover the cost of the program and perform the services they are contracting to perform. The FAR Subpart 15.305 states, in part, "[w]hen contracting on a cost-reimbursement basis, evaluations shall include a cost realism analysis to determine what the Government should realistically expect to pay for the proposed effort, the offeror's understanding of the work, and the offeror's ability to perform the contract." The CSO contracts are bid as cost reimbursement contracts.

We interviewed USMS officials who were involved with the evaluation and selection process for the three USProtect contracts. In addition, we reviewed the evaluation documents and pricing information that were contained in the solicitation files. As result of our preliminary review, we found that there was significant concern raised within the USMS over whether USProtect's bids were too low to cover their costs, based on USMS knowledge of and experience with the CSO program. However, we found no evidence that the Office of Security Contracts adequately addressed these issues prior to awarding the contracts to USProtect.

We reviewed the Technical and Price Negotiation Memorandum written by the Contracting Officer, dated September 14, 2006, in which the Contracting Officer stated repeatedly that USProtect's quoted start up costs were lower than the competing bids and were too low to cover actual start-up costs for all three Judicial Circuits. USProtect's bids on the three Judicial Circuits were well below both the Independent Government Cost Estimates (IGCE) and the bids submitted by competing vendors. USProtect's bid prices were approximately $4 million to $7 million less than the other bids received in each of the three circuits. The other two vendors were familiar with the costs of the program because they had prior experience with CSO contracts; USProtect had no previous experience with the CSO Program.

The Contracting Officer believed that USProtect's bid was insufficient to cover the costs of the program. In addition, the former Chief of the Office of Court Security indicated that the bids should be close to one another because the only variable costs associated with the contracts were administrative overhead and profit. He further stated that USProtect's resulting financial problems may have stemmed from providing overly low bids.

The Contracting Officer stated, after further negotiations with USProtect, that the company was confident that its start-up rates were sufficient, despite the concerns raised in her Technical and Price Negotiation Memorandum, dated September 14, 2006. The Contracting Officer accepted USProtect's claim that its prices were adequate and ultimately awarded the contract to USProtect. As with questions regarding Mr. Hudec's involvement with the company, the Office of Security Contracts again relied on self-serving statements from USProtect and dismissed legitimate concerns about USProtect's ability to provide contracted services at its overly low bid price.

We believe that the difference in amounts between USProtect's bids and competing bids was cause for serious concern regarding whether USProtect understood the requirements of the contract and if it had the financial means to cover the costs to run the CSO Program in each Judicial Circuit for which it bid. Yet, USProtect was awarded the CSO Contracts in all three circuits despite the Contracting Officer's concerns about the inadequate contract price, unanswered concerns by the PPOT, and an OIG fraud alert. The acceptance of the comparatively low bid prices despite these multiple indicators of problems raises concerns about the evaluation and award process conducted by the USMS Office of Security Contracts.

Technical Evaluation Board Lacked Evidence of a Thorough Review

The purpose of a Technical Evaluation Board (TEB) review is to provide the Contracting Officer with the information necessary to make the best selection possible. We examined the work performed by the TEB that led to the selection of USProtect. Specifically, we reviewed the individual rating sheets completed by each of the team members. We found that the review was not well-documented and that the TEB was not provided all relevant information. As a result, the TEB failed to point out significant weaknesses with USProtect that may have led to the selection of more qualified vendors.

The FAR Subpart 15.303(b)(1) states that "[t]he selection authority shall establish an evaluation team, tailored for the particular acquisition, that includes appropriate contracting, legal, logistics, technical, and other expertise to ensure a comprehensive evaluation of offers." In this instance the

Contracting Officer was the selection authority, and she appointed five USMS employees to serve on the TEB.[7] The TEB met from June 5, 2006, through June 16, 2006, at USMS Headquarters in Arlington, Virginia, to review the initial bid responses. The board reconvened via teleconference on August 29, 2006.

Each of the three vendors was evaluated based on three criteria weighted on a 100-point scoring system: (1) past performance weighted at 45 points, (2) contract management at 35 points, and (3) technical ability to meet the requirements in the statement of work at 20 points. The members of the TEB rated each vendor and gave them a score for each criterion. In addition, the evaluation forms provided space to document strengths, weaknesses, deficiencies, and clarifications. However, we found that in many instances, even though USProtect did not receive the full points allowed for a particular criteria, the evaluation form contained no explanation of any deficiencies or weaknesses that would cause a lower than maximum score for that criteria.

Further, the written evaluations contained no references to the OIG fraud alert. In addition, the Contracting Officer confirmed that the fraud alert was not given to members of the TEB at any time during their evaluation process. While the initial meeting of the TEB took place prior to the OIG's issuance of the fraud alert in July 2006, the USMS was in possession of this information prior to the TEB's follow-up meeting on August 29, 2006. This information should have been provided to the TEB since the Fraud Alert should have been taken into account in scoring the contractor for past performance and contract management.

Conclusion

We reviewed the USMS's awarding of CSO contracts to USProtect and identified significant concerns with its procurement process. We believe that these concerns stem from USMS's lack of adherence to the FAR and its own procurement policies. This lack of adherence to established policies and regulations resulted in the USMS' s selection of USProtect as being the "best value" to the government despite ample and persuasive evidence to the contrary.

Specifically, we found a significant failure on the part of the USMS's Office of Security Contract's and Office of General Counsel to exercise due diligence in following up on the OIG fraud alert issued 2 months prior to the awarding of the contracts. Further, we do not believe that the USMS conducted the necessary research on USProtect that was required by the FAR, nor did it gather the necessary information to be able to determine whether

[7] The board consisted of a U.S. Marshal, a Chief Deputy U.S. Marshal, two Deputy U.S. Marshals, and one employee from the USMS Judicial Security Division.

USProtect was a responsible vendor. Also, the USMS failed to address in writing, as it was required to do, concerns from the USMS Procurement Chief related to its selection of USProtect. In addition, despite the fact that the Contracting Officer identified USProtect's bids as being unrealistically low, the contract was awarded to USProtect. Lastly, the Technical Evaluation Board failed to adequately document its review of USProtect and the Contracting Officer failed to make the OIG fraud alert available to the Board for use in its evaluation of the contractor.

We believe that these failures on the part of the USMS led to three CSO contracts being awarded to USProtect, a less than responsible vendor that ultimately collapsed. USProtect's collapse placed the security of many court facilities at risk, something that could have been avoided had the USMS performed its due diligence and adhered to established policies and regulations. It also led to many CSOs not receiving timely payment for their services because the vendor filed bankruptcy. We recommend that the USMS implement immediate corrective action to address the concerns contained in this memorandum and ensure that the solicitation and award process to replace the soon-to-expire CSO contracts for the 12 judicial circuits are properly handled in accordance with the FAR and its procurement policies.

cc: Michael J. Prout
Assistant Director
Judicial Security Division
United States Marshals Service

Steven Conboy
Deputy Assistant Director
Judicial Security Division
United States Marshals Service

Gerald M. Auerbach
General Counsel
United States Marshals Service

Anita K. Maldon
Procurement Chief, Procurement Office
United States Marshals Service

Isabel Howell
Audit Liaison
United States Marshals Service

James W. Johnston
Director, Procurement Support Staff
Justice Management Division

Richard P. Theis
Assistant Director
Audit Liaison Group
Justice Management Division

U.S. Department of Justice

United States Marshals Service

Office of the Director

Washington, DC 20530-1000

July 28, 2009

MEMORANDUM TO: Raymond J. Beaudet
Assistant Inspector General
for Audit

FROM: John F. Clark
Director

SUBJECT: Immediate Improvements Necessary for the Judicial Security Division's Court Security Procurement Process

This memorandum is in response to your June 17, 2009, memorandum regarding issues identified during the course of the ongoing Office of the Inspector General (OIG) audit of the United States Marshals Service (USMS), Judicial Security Division, court security procurement process. The USMS has considered your concerns related to a contract award from 2006, and agrees that immediate improvement of the court security procurement process is imperative. In the past few months, the USMS has developed and implemented new measures to ensure that selections for future court security procurements are executed in a more judicious manner. Specific responses to each of the concerns outlined in your memorandum are described in the attached document.

These corrective actions will improve the USMS court security procurement process. Should you have any questions or concerns about this matter, please contact Assistant Director Michael Prout at 202-307-9500.

Attachment

cc: David J. Gaschke
Regional Audit Manager
San Francisco Regional Audit Office
Office of the Inspector General

Michael J. Prout
Assistant Director
Judicial Security Division

Isabel Howell
Audit Liaison

James W. Johnston
Director, Procurement Support Staff
Justice Management Division

Richard P. Theis
Assistant Director, Audit Liaison Group
Justice Management Group

Lack of Due Diligence in USMS Background Research

Procurement officials will diligently comply with all USMS procurement policies and procedures. The Contracting Officer (CO) or source selection authority will share all relevant information and concerns with members of the technical evaluation board. Counsel and advice will also be sought from authorized program, procurement, and legal officials prior to award. In the event the decision of the CO or source selection authority differs from the USMS Procurement Policy and Oversight Team's findings, the CO will address concerns or recommendations by making the necessary changes, or by preparing written justification to explain why the concerns or recommendations were not accepted. When feasible, all involved parties will meet to discuss and resolve any differences. Precautionary measures have also been set in place to ensure suitability of key contract officials. Effective immediately, all future court security solicitations will require key personnel, including corporate officials and shareholders in closely held corporations, to undergo and pass a limited background investigation prior to final award.

USProtect's Price was Insufficient to Cover Program Cost

In retrospect, the USMS agrees that USProtect's price was insufficient to perform the requirements of the contract, and that the CO should have used better judgment in this area. Since that time, the USMS has hired a more experienced CO to manage and administer the Office of Security Contracts. We are confident that the current CO will exercise extreme caution in rendering responsible determinations.

Technical Evaluation Board Lacked Evidence of a Thorough Review

Without revealing specifics of the procurement process, the source selection plan and new evaluation material have been developed to improve and streamline the evaluation process. Under the new plan, the technical evaluation board members will be involved in a more structured process and they will receive clearer guidance and support from the CO and legal advisors. In addition, all members assigned to the technical evaluation board will receive training from a qualified procurement instructor before the evaluation process occurs. The technical evaluation board will receive a comprehensive briefing to ensure that they understand their role and responsibility during the source selection process. Each member of the technical evaluation board will also be granted adequate time to review and familiarize themselves with the solicitation, the source selection plan, and the evaluation material. The CO and a legal advisor have also been directed to work closely with the members during the entire evaluation process.

USMS RESPONSE TO THE DRAFT REPORT

U.S. Department of Justice

United States Marshals Service

Office of the Associate Director

Alexandria, Virginia 22301-1025

October 29, 2010

MEMORANDUM TO: Raymond J. Beaudet
Assistant Inspector General
for Audit

FROM: Robert J. Finan II
Associate Director
for Operations

SUBJECT: Response to Draft Audit Report:
United States Marshals Service's Oversight of its
Judicial Facilities Security Program

The United States Marshals Service (USMS) is statutorily responsible for the security of the Judicial Branch. Based on a longstanding Memorandum of Understanding (MOU) with the Administrative Office of the United States Courts (AOUSC) and the Federal Protective Service (FPS), the USMS is also responsible for security at facilities housing components of the United States Courts. The security of over 800 facilities, including more than 400 where approximately 5,000 Court Security Officers (CSOs) are posted, is of the utmost importance to the USMS.

In reviewing your report, where you identify weaknesses related to concerns of the judiciary for the security of facilities, it is important to highlight a few points that were either not recognized, or were not included as part of this audit. I appreciate and will direct whatever action possible to address the concerns of the Chief Judges interviewed for the audit. It is noteworthy that the USMS is not the determining party as it relates to the budget for staffing or physical security. The USMS and the AOUSC work closely to address concerns and risk, and have seen progressive and positive increases in budgetary resources. While it is a concern that three of six Chief Judges interviewed expressed concern, I am heartened that in a recent audit of the USMS conducted by your agency (I-2207-010), over 85% of judges responding to your survey expressed they were either satisfied, or highly satisfied with their security and the USMS.

I note and appreciate your emphasis of the need for an active Court Security Committee in each district. It is likewise noteworthy that the Court Security Committee, which is a requirement of the Judicial Conference of the United States, is led by or responsible to the Chief District Judge; and while the USMS has a role, it is one of support to the Chief

District Judge. The Chief District Judge is responsible for maintaining an active Court Security Committee. The USMS will continue to encourage the same across all districts.

The USMS responses to the recommendations contained in the subject draft audit report are listed below:

Recommendation 1: Ensure that all USMS district offices regularly review and update their Continuity of Operations Plans and ensure that annual security surveys are performed at each district and that all judicial security plans are updated as required.

Response (Concur): The Assistant Directors for Judicial Security and Tactical Operations will emphasize this requirement to all United States Marshals and Chief Deputy United States Marshals, and will ensure it is a component of the District Audit Program and the annual District Self Assessment.

The below comments refer only to the Continuity of Operations Plan as referenced throughout the draft report:

1. p. iii, note 4: The note states that HSPD 20 requires that all federal departments and agencies maintain a Continuity of Operations Plan. The correct language from NSPD 51/HSPD 20 source document reads: all executive departments and agencies… http://www.dhs.gov/xabout/laws/gc_1219245380392.shtm#1. This does not change the intent of the comment or the impact upon the USMS.

2. p. iv, note 5: The draft report cites Federal Preparedness Circular (FPC) 65 as its reference. FPC 65 was superseded by Federal Continuity Directive (FCD) 1, in February 2008 (http://www.fema.gov/pdf/about/offices/fcd1.pdf). However, the updating requirements did not change with the adoption of FCD 1.

3. p. 5, first full paragraph: same as number 1, above.

4. p. 5, note 18: same as number 2, above.

5. p. 31: same as number 2, above.

The USMS District COOP Template, Annex A, Section 6.3 states that:

"The COOP Program Point of Contact (POC) develops district COOP plans in accordance with USMS policies and procedures. The POC performs an annual review of the COOP plan and makes updates and changes as necessary."

Additionally, the annual review is an FCD 1 requirement that is taught in the USMS COOP Managers Class, which is available annually to all districts. Since 2007, more than 182 district and headquarters personnel have completed this training class. Additionally, a template COOP plan is available for district personnel to utilize that covers all requirements of FCD 1.

The Tactical Operations Division, Office of Emergency Management, will continue to support any USMS district that requests assistance with the preparation, training, testing or exercising of a COOP plan.

Recommendation 2: Ensure that all of its district offices assign a principal coordinator to the district Court Security Committee and encourage the local judiciary to lead regular meetings.

Response (Concur): The Assistant Director for Judicial Security will emphasize this requirement to all United States Marshals.

The existing policy directs the United States Marshal to serve as the principal coordinator, and for Judicial Security Inspectors to attend and participate in Court Security Committee meetings. They are reminded during various training sessions to discuss with the judiciary the need for those meetings.

Recommendation 3: Ensure that all Judicial Security Inspectors and CSOs are appropriately trained before entering on duty. The USMS should also develop a process to ensure that all Judicial Security Inspectors and CSOs are adequately trained on newly deployed screening systems.

Response (Concur): The USMS selects personnel for the Judicial Security Inspector (JSI) position in accordance with a merit promotion selection process. Training on the role and duties of the position is conducted after the regulation required time-period for the promotion. Judicial Security Inspectors are required to obtain Contracting Officer's Technical Representative (COTR) certification immediately upon assuming the JSI position. They are also required to attend in-service training at the next scheduled session. JSIs were also required to complete an online x-ray operator training course this past fiscal year.

CSOs must currently complete Phase I and firearms qualification before assuming the duties of a CSO. The Office of Court Security (OCS) has revised the CSO Orientation Program and will implement the new program in Fiscal Year 2011. Under the revised program, the contractor must schedule and ensure that every CSO complete a 40 hour on-the-job standardized program as part of Phase I. Upon completion of Phase I requirements, a CSO may then be assigned to work alone. However, CSOs will not be permitted to operate any screening equipment until they have successfully completed the Phase II requirements and have completed a second 40 hour on-the-job training program specific to screening equipment. Once a CSO has completed all of the Phase II requirements, the CSO may be assigned to a post without any duty limitations. Training on newly deployed screening systems is performed by the vendor when installed.

Recommendation 4: Ensure that its district offices perform the required quarterly unannounced tests to determine if CSOs are adequately screening visitors, packages, and mail that are delivered to the courthouse and maintain records of the results.

Response: (Concur): The USMS regularly reminds and encourages its district offices of the requirements of conducting quarterly unannounced facility screening tests. This guidance is provided during training sessions, through internal communication, and is contained in USMS

Policy Directive 10.4, *Judicial Facility Security*. The USMS has developed an internal database to maintain and track these records and regularly reviews the results to identify security deficiencies.

Recommendation 5: Ensure that all district offices report incidents and arrests at courthouse facilities as required and conduct a coordinated periodic analysis of the data each fiscal year.

Response (Concur): The USMS regularly reminds and encourages its district offices of the requirements of ensuring the contractor reports and documents incidents and arrests at courthouse facilities. This guidance is provided during training sessions, through internal communication, and is contained in the post orders and CSO contract. The USMS maintains these reports in a database and regularly reviews these reports.

The USMS is currently developing an internal database which will be used to report, track, and analyze incidents and arrests that occur at its courthouse facilities.

Recommendation 6: Continue to evaluate its current contract file maintenance practices and develop procedures to ensure that all necessary documentation is maintained in a consistent manner.

Response (Concur): The USMS has developed procedures necessary to ensure contract file documentation is maintained in a consistent manner. A contract file checklist is required and included with every contract action. The checklist will standardize contract files and ensure that every file is consistent.

Recommendation 7: Seek to streamline its current timekeeping practices for CSOs.

Response (Concur): The USMS met with the vendors individually to modify the existing time and attendance form used and reported to the USMS. Additionally, the USMS will conduct training for all Judicial Security Inspectors in November 2010. During this training, Judicial Security Inspectors will be reminded of their responsibility for monitoring and approving CSO work hours.

Recommendation 8: Perform a comprehensive review of its background investigation process for CSOs and seek to ensure that these investigations are completed in a timely manner.

Response (Concur): The USMS will review the entire process of background investigations from the request that the investigation be conducted through the adjudication. The USMS already monitors the receipt of background investigations using a database and sends reminders when the investigations are overdue. Additionally, the processing of background investigations is a part of the district's Self-Assessment Guide (SAG), which holds them responsible for timely completion.

Recommendation 9: Develop a method for analyzing its performance violation data to better understand violation trends and potential training needs among its CSO workforce.

Response (Concur): The USMS has implemented a tracking database spreadsheet for all performance standard violations. The database allows for sorting of information to include contractor name, Circuit, District, performance standard numbers violated, proposed disciplinary action, et cetera. The database can generate reports that will allow for analysis of violation trends and potential training needs. The database will allow the USMS to identify potential training needs based on documented performance violation trends and other information.

Recommendation 10: Provide additional guidance to district Judicial Security Inspectors to ensure that all CSO performance violations are documented and reported to the Office of Court Security.

Response (Concur): The USMS regularly provides additional guidance to its districts on the requirements of reporting and documenting performance violations. This guidance is provided during training sessions, through internal communication, and is stated in the CSO contract.

It is the responsibility of the district Judicial Security Inspector, who serves as the Contracting Officer's Technical Representative (COTR) for the CSO contract, to ensure that the contractor remains in compliance with the terms and conditions of the contract and that the Government receives full measure of the goods and/or services required of the contract. Additionally, as required in the CSO contract, the contractor must immediately notify the Contracting Officer and the COTR in writing when a CSO engages in, or is suspected of, violating any of the performance standards stated in the contract.

Recommendation 11: Evaluate its CSO personnel file maintenance practices and develop procedures to ensure that all necessary documentation, such as medical and firearms qualifications, is adequately maintained and up to date. In addition, the USMS should assess the feasibility of implementing an automated system for tracking important dates in the database to ensure that CSOs satisfy their qualification requirements in a timely manner.

Response (Concur): The USMS will reevaluate the CSO personnel file maintenance to improve the processing, timeliness, and storage of personnel records. The USMS already monitors important dates in a database to ensure qualification requirements, but will seek to improve oversight of these requirements.

Recommendation 12: Require district offices to supervise and verify labor hours claimed by contractors to help ensure that it is not being over billed under the nationwide security systems contract.

Response (Concur): The USMS, with the required financial support of the AOUSC, will require district offices to verify labor hours if the nationwide security systems contract is labor hour based. The USMS recently switched from a Time and Materials type contract to a Firm Fixed Price type contract, negating the need to track contractor labor hours expended.

Recommendation 13: Assess the feasibility of district offices maintaining their own security system equipment inventories of equipment maintained by the contractor so that comparisons can be made to the contractor's inventory to avoid unwarranted maintenance fees.

Response (Concur): The USMS will evaluate options and logistics associated with districts having some inventory tracking capability. As a partial solution to the inventory issue, the USMS intends to reduce the number of security equipment items subject to maintenance fees in the new contract, the solicitation for which is now in development. This approach would also reduce the burden on district personnel, who are already working beyond available resources supporting the Judicial Facility Security Program.

Recommendation 14: Track the cost of repairs for its screening equipment and the impact of downtime on court security in order to periodically assess whether a maintenance plan for its screening equipment would be cost effective.

Response (Concur): The USMS has implemented a methodology for tracking screening equipment repair costs. The USMS will expand that methodology to also collect downtime data, and will continue to conduct market research on maintenance plan options.

Recommendation 15: Require the Office of Security Contracts to prepare past performance and interim evaluations in accordance with the Federal Acquisition Regulation.

Response (Concur): The USMS will prepare past performance and interim evaluations in accordance with FAR Subpart 42.15 - Contractor Performance Information.

OFFICE OF THE INSPECTOR GENERAL ANALYSIS AND SUMMARY OF ACTIONS NECESSARY TO CLOSE THE REPORT

The OIG provided a draft of this audit report to the United States Marshals Service (USMS). The USMS response is incorporated in Appendix IV of this final report. The following provides the OIG analysis of the response and summary of actions necessary to close the report.

Analysis of USMS Response

In response to our audit report, the USMS concurred with all of our recommendations and discussed the actions it will implement in response to our findings. However, the USMS added to its response specific points that it felt were not recognized or were not included as part of this audit. We provide the following reply to these statements, before discussing the USMS's specific responses to each of our recommendations and the actions necessary to close those recommendations.

In its response, the USMS notes that it is not the determining party as it relates to the budget for staffing or physical security. The USMS stated that "the USMS and the [Administrative Office of the United States Courts] work closely to address concerns and risk, and have seen progressive and positive increases in budgetary resources." Our report did note this issue, stating in the first paragraph that the USMS's Judicial Facilities Security Program is administered by the USMS and funded by the federal judiciary.

The USMS also stated in its response that it was concerned that three of the six Chief Judges interviewed expressed concern with the security provided by the USMS, and the USMS referred to another OIG report in September 2007 (I-2007-010) which reported that over 85 percent of judges responding to an OIG survey expressed that they were either satisfied or highly satisfied with their security and the USMS.[40] However, the prior report was an evaluation of the USMS efforts to improve its capabilities to assess and react to reported threats to the federal judiciary, not a review of the general security measures provided at courthouses. In that evaluation, we asked in a survey whether the judges were generally satisfied with the USMS performance in protecting federal judges. By contrast, in this audit we interviewed Chief Judges to determine whether they had specific

[40] The USMS's response incorrectly refers to this OIG report as (I-2207-010).

concerns related to the security provided by the USMS at their respective courthouses.

The USMS stated in its response that the Court Security Committee "is led by or responsible to the Chief District Judge; and while the USMS has a role, it is one of support to the Chief District Judge. The Chief District Judge is responsible for maintaining an active Court Security Committee." Our report acknowledges that the district Court Security Committee is chaired by the federal judiciary. However, our report also notes that USMS policy requires the United States Marshal or designee to be the principal coordinator of the local district Court Security Committee, which advises on the planning, implementation, and continuous review of the court security program for each federal judicial facility in the district. Recognizing that the USMS is not responsible for chairing these committees, our report recommends that the USMS ensure that it assigns a principal coordinator to each local committee and encourage the participation of the local judiciary. We believe that the USMS's response does not sufficiently recognize the important role the USMS should play on these Court Security Committees.

Summary of Actions Necessary to Close the Report

1. **Resolved.** The USMS concurred with our recommendation to ensure that all USMS district offices regularly review and update their Continuity of Operations Plans and ensure that annual security surveys are performed at each district and that all judicial security plans are updated as required.

   The USMS also stated in its response that the Assistant Directors for Judicial Security and Tactical Operations will emphasize these requirements to all United States Marshals and Chief Deputy United States Marshals, and will ensure it is a component of the District Audit Program and the annual District Self Assessment.

   This recommendation can be closed when we receive evidence that the requirement to: (1) regularly review and update Continuity of Operations Plans, (2) perform annual security surveys, and (3) update judicial security plans, are made part of the USMS District Audit Program and the annual District Self Assessment. Once updated, the USMS should provide us with a copy of its District Audit Program and annual District Self Assessment.

   In addition to providing its formal response to recommendation 1, the USMS provided technical comments regarding the report references to Homeland Security Presidential Directive (HSPD) 20 and Federal

Preparedness Circular (FPC) 65. Both of these report references related to the USMS's Continuity of Operations Plan obligations. As the USMS correctly notes, the OIG's use of the phrase "federal departments and agencies" in the draft report instead of the phrase "executive departments and agencies" does not affect the USMS's reported obligations under HSPD 20 or recommendation 1. Further, the USMS is correct that FPC 65 was superseded by Federal Continuity Directive (FCD) 1. Again, the USMS correctly notes that the updating requirement of FPC 65 did not change with the adoption of FCD 1. The OIG made these technical edits to the final version of this report.

2. Resolved. The USMS concurred with our recommendation to ensure that all of its district offices assign a principal coordinator to the district Court Security Committee and encourage the local judiciary to lead regular meetings. The USMS stated in its response that the Assistant Director for Judicial Security will emphasize this requirement to all United States Marshals and noted its existing policy that directs the United States Marshal to serve as the principal coordinator and Judicial Security Inspectors to attend and participate in Court Security Committee meetings. The USMS added that these individuals are reminded during various training sessions to discuss with the judiciary the need for those meetings.

This recommendation can be closed when we receive evidence that all USMS district offices have assigned a principal coordinator to the local district Court Security Committees and have encouraged the local judiciary to lead regular meetings.

3. **Resolved.** The USMS concurred with our recommendation to ensure that all Judicial Security Inspectors and CSOs are appropriately trained before entering on duty. The USMS also concurred that it should develop a process to ensure that all Judicial Security Inspectors and CSOs are adequately trained on newly deployed screening systems.

The USMS stated in its response that Judicial Security Inspectors are required to obtain Contracting Officer's Technical Representative (COTR) certification immediately upon assuming the Judicial Security Inspector position. The USMS also stated that they are required to attend in-service training at the next scheduled session. The Judicial Security Inspectors were also required to complete an online x-ray operator training course this past fiscal year.

The USMS also responded that the Office of Court Security (OCS) has revised the CSO Orientation Program and will implement the new

program in FY 2011. According to the USMS, training on newly deployed screening systems is performed by the vendor when the systems are installed.

This recommendation can be closed when we receive documentation supporting that all Judicial Security Inspectors and CSOs are adequately trained before entering on duty. Specifically, the USMS should provide evidence that all its Judicial Security Inspectors have completed the in-service training and the x-ray operator training course. The USMS should also provide documentation supporting the newly revised CSO Orientation Program, specifically as it pertains to training requirements for operating screening equipment. Further, the USMS should provide evidence of a process that ensures that all vendor-provided training for all newly deployed screening systems is conducted in a timely manner.

4. **Resolved.** The USMS concurred with our recommendation to ensure that its district offices perform the required quarterly unannounced tests to determine if CSOs are adequately screening visitors, packages, and mail that are delivered to the courthouse and maintain records of the results. The USMS stated in its response that it regularly reminds and encourages its district offices of these requirements and provides guidance through training sessions and internal communication. According to the USMS, it has developed an internal database to maintain and track these records and regularly reviews the results to identify security deficiencies.

   This recommendation can be closed when we receive evidence that the USMS provides regular reminders to its district offices, including training documentation and correspondence, of the requirement to conduct quarterly unannounced facility screening tests. In addition, the USMS should provide evidence of the internal database it uses to maintain, track, and analyze the results of its quarterly unannounced screening tests and provide a detailed description of the analysis it performs on these test results.

5. **Resolved.** The USMS concurred with our recommendation to ensure that all district offices report incidents and arrests at courthouse facilities as required and conduct a coordinated periodic analysis of the data each fiscal year. According to the USMS's response, the USMS is currently developing an internal database that will be used to report, track, and analyze incidents and arrests that occur at its courthouse facilities.

This recommendation can be closed when we receive evidence of the USMS's newly developed internal database that will be used to report, track, and analyze incidents and arrests that occur at its courthouse facilities. The USMS should also provide the methodology it will use in performing the recommended coordinated periodic analysis of the data each fiscal year.

6. **Resolved.** The USMS concurred with our recommendation to continue to evaluate its current contract file maintenance practices and develop procedures to ensure that all necessary documentation is maintained in a consistent manner. The USMS stated in its response that it has developed procedures necessary to ensure contract file documentation is maintained in a consistent manner, which includes a contract file checklist that will be required and included with every contract action. The USMS stated that the checklist will standardize contract files and ensure that every file is consistent. This recommendation can be closed when we receive a copy of the developed procedures for maintaining contract files, including any and all checklists.

7. **Resolved.** The USMS concurred with our recommendation to seek to streamline its current timekeeping practices for CSOs. The USMS stated in its response that it met with the vendors individually to modify the existing time and attendance form used and reported to the USMS. Additionally, the USMS will conduct training for all Judicial Security Inspectors in November 2010. During this training, Judicial Security Inspectors will be reminded of their responsibility for monitoring and approving CSO work hours.

   This recommendation can be closed when we receive documentation to support streamlined timekeeping procedures for CSOs, including a modified time and attendance form. In addition, the USMS should provide us with documentation of the November 2010 training that confirms that Judicial Security Inspectors were trained on their responsibility to monitor and approve CSO work hours.

8. **Resolved.** The USMS concurred with our recommendation to perform a comprehensive review of its background investigation process for CSOs and seek to ensure that these investigations are completed in a timely manner. The USMS stated in its response that it will review the entire process of background investigations from the request that the investigation be conducted through the adjudication.

This recommendation can be closed when we receive evidence of the USMS's completed review of the background investigation process and documentation supporting any changes that result from this review.

9. **Resolved.** The USMS concurred with our recommendation to develop a method for analyzing its performance violation data to better understand violation trends and potential training needs among its CSO workforce. The USMS stated in its response that it has implemented a tracking database spreadsheet for all performance standard violations. According to the USMS, the database can generate reports that will allow for analysis of violation trends and potential training needs.

   The USMS's response to our recommendation describes the capabilities of its database spreadsheet, but does not state the methodology that will be used to analyze performance violation data. We do not believe that simply logging performance violation data into a database is sufficient. This recommendation can be closed when we receive evidence that the USMS has developed a methodology for analyzing its performance violation data to better understand violation trends and potential training needs among its CSO workforce.

10. **Resolved.** The USMS concurred with our recommendation to provide additional guidance to district Judicial Security Inspectors to ensure that all CSO performance violations are documented and reported to the Office of Court Security. The USMS stated in its response that it regularly provides guidance to its districts on the requirements of reporting and documenting performance violations during training sessions and through internal communication. The USMS also highlighted that this requirement is stated in the CSO contract.

    Further, the USMS also stated in its response that the CSO contractor is responsible for reporting to the USMS when it learns that a CSO engages in or is suspected of violating any of the performance standards stated in the contract.

    We note that our recommendation is specific to instances where the USMS first learns of the performance violation. Therefore, this recommendation can be closed when the USMS provides additional guidance to its Judicial Security Inspectors to ensure that all CSO performance violations are documented and reported to the Office of Court Security. Further, the USMS should provide evidence that the Judicial Security Inspectors, as the COTRs on the CSO contracts, have

been provided with the relevant provisions of the CSO contract related to procedures for reporting CSO performance violations.

11. **Resolved.** The USMS concurred with our recommendation to evaluate its CSO personnel file maintenance practices and develop procedures to ensure that all necessary documentation, such as medical and firearms qualifications, is adequately maintained and up to date. The USMS also concurred that it should assess the feasibility of implementing an automated system for tracking important dates in the database to ensure that CSOs satisfy their qualification requirements in a timely manner. The USMS stated in its response that it will reevaluate its CSO personnel file maintenance to improve the processing, timeliness, and storage of personnel records.

    This recommendation can be closed when we receive evidence that the USMS has improved its CSO personnel file maintenance practices and developed procedures that ensure all necessary documents, such as medical and firearm qualifications, are being maintained and are up to date. Further, the USMS should provide evidence that it has assessed the feasibility of implementing an automated system for tracking important dates in its CSO database to ensure that CSOs satisfy their qualification requirements in a timely manner. If the USMS's tracking of dates has already been automated, then it should provide evidence of that change.

12. **Resolved.** The USMS concurred with our recommendation to require district offices to supervise and verify labor hours claimed by contractors to help ensure that it is not being over billed under the nationwide security systems contract. The USMS stated in its response that it recently switched from a time and materials type contract to a firm fixed price type contract, negating the need to track contractor labor hours expended.

    This recommendation can be closed when we receive documentation to support the USMS's switch from a time and materials type contract to a firm fixed price nationwide security systems contract. Further, the USMS should provide evidence that there is no labor hour component in its current nationwide security systems contract. If the nationwide security system contract has any elements that are based on labor hours, the USMS should provide evidence that it has required district offices to verify labor hours that are charged to the USMS and that district offices are complying with that requirement.

13. **Resolved.** The USMS concurred with our recommendation to assess the feasibility of district offices maintaining their own security system equipment inventories of equipment maintained by the contractor so that comparisons can be made to the contractor's inventory to avoid unwarranted maintenance fees. The USMS stated in its response that it will evaluate options and logistics associated with districts having some inventory tracking capability. As a partial solution to the inventory issue, the USMS intends to reduce the number of security equipment items subject to maintenance fees in the new contract, the solicitation for which is in development. According to the USMS, a reduction in the number of security equipment items that are subject to maintenance fees would reduce the burden on district personnel.

    This recommendation can be closed when we receive the detailed results of the USMS's evaluation of its district offices' inventory tracking capability. Additionally, the USMS should provide a copy of the new contract when finalized showing any reduction in the number of security equipment items subject to maintenance fees compared to the previous contract and identify the resulting savings.

14. **Resolved.** The USMS concurred with our recommendation to track the cost of repairs for its screening equipment and the impact of downtime on court security in order to periodically assess whether a maintenance plan for its screening equipment would be cost effective. The USMS stated in its response that it has implemented a methodology for tracking screening equipment repair costs. The USMS will expand this methodology to also collect downtime data, and will continue to conduct market research on maintenance plan options. This recommendation can be closed when we receive documentation that supports the USMS's tracking of screening equipment repair costs and downtime data. Further, the USMS should provide us with evidence that it has been evaluating maintenance plan options.

15. **Resolved.** The USMS concurred with our recommendation to require the Office of Security Contracts to prepare past performance and interim evaluations in accordance with the Federal Acquisition Regulation. The USMS stated in its response that it will prepare past performance and interim evaluations in accordance with Federal Acquisition Regulation Subpart 42.15 – Contractor Performance Information. This recommendation can be closed when we receive evidence that the USMS's Office of Security Contracts has prepared past performance and interim evaluations on its contractors in accordance with the Federal Acquisition Regulation.