



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

**Review of the Protection of the Judiciary and
the United States Attorneys**

December 2009

I-2010-002-R

Redacted – For Public Release

EXECUTIVE DIGEST

Threats and inappropriate communications to federal judges, U.S. Attorneys, and Assistant U.S. Attorneys (AUSA) have increased dramatically during the past several years, growing from 592 in fiscal year (FY) 2003 to 1,278 in FY 2008.¹ Overall, during this 6-year period, there were 5,744 threats directed at these federal officials.

United States Marshals Service (USMS) district offices have primary responsibility for ensuring the safety and security of federal judicial proceedings and protecting the more than 2,000 federal judges and approximately 5,250 other federal court officials, including U.S. Attorneys and AUSAs.

Three other Department of Justice components – the Executive Office for United States Attorneys (EOUSA), United States Attorneys' Offices (USAO), and the Federal Bureau of Investigation (FBI) – are also involved in responding to these threats. EOUSA provides oversight, guidance, and support to USAOs on threats and related matters, and coordinates interactions between USAOs and other Department components. The USAOs are responsible for reporting threats against U.S. Attorneys, AUSAs, and their families to the USMS and EOUSA, and the USAOs also provide some protective measures in response to threats.² In addition, the FBI is responsible for conducting criminal investigations of threats against federal judges, U.S. Attorneys, and AUSAs.

The Office of the Inspector General (OIG) conducted this review to examine the USMS's response to threats made against federal judges and the USMS's, EOUSA's, and USAOs' handling of threats against U.S. Attorneys and AUSAs. This is the third OIG review to examine the

¹ According to USMS Directive 10.3.G.12, *Protective Investigations*, 2007, a threat is any action or communication, explicit or implied, of intent to assault, resist, oppose, impede, intimidate, or interfere with any member of the federal judiciary, or other USMS protectee, including members of their staffs or family. According to USMS Directive 10.3.G.5, *Protective Investigations*, 2007, an inappropriate communication is any communication directed to a USMS protectee or employee that warrants further investigation. In this report, we use the term "threat" to encompass both threats and inappropriate communications.

² The USAOs report threats against USAO personnel to EOUSA via Urgent Reports. The Urgent Report contains a brief synopsis of the facts and a concise summary of the event.

protection of federal court officials.³ In this review, we examined the role and responsibilities of USMS district offices, procedures that USMS district offices employ to assess and respond to threats, and the roles of EOUSA and the USAOs in the protection of the U.S. Attorneys and AUSAs. Our review examined the 1,587 threats reported during FY 2007 and FY 2008. In addition, we conducted a detailed examination of 26 threats in four judicial districts that we visited.

RESULTS IN BRIEF

Our review found deficiencies in the response to threats by the USMS and EOUSA. As a threshold matter, we found that threats against judges, U.S. Attorneys, and AUSAs are not consistently and promptly reported.

Moreover, when threats are reported the USMS does not consistently provide an appropriate response for the risk level posed by the threat. In addition, the USMS does not fully or effectively coordinate with other law enforcement agencies to respond to threats against federal judicial officials.

We also found that threatened USAO personnel may not receive sufficient protection because EOUSA and USAO staff providing protective measures lack threat response expertise and training similar to that of the USMS's judicial security staff, who are specifically trained in threat response procedures. EOUSA and USAO staff are also responsible for numerous security-related duties, which limits the time they have to devote to threat response. In addition, coordination on threat responses among EOUSA, the USAOs, and the USMS is inconsistent. Moreover, EOUSA is not consistently notified of threats against U.S. Attorneys and AUSAs and often lacks important information about threats and protective responses taken in response. These deficiencies prevent EOUSA from providing emergency support or tracking trends in threats against USAO personnel.

The following sections of this Executive Digest describe these findings in more detail.

Federal Judges, U.S. Attorneys, and AUSAs do not consistently and promptly report threats.

For the USMS to most effectively protect federal judges, U.S. Attorneys, AUSAs, and their families from harm, protectees must promptly notify the USMS when they receive threats. In our interviews and

³ The OIG's prior reports are described in Appendix I.

surveys most federal judges, U.S. Attorneys, and AUSAs told the OIG that they reported every threat made to them, but some said they did not. Although we could not determine the number of unreported threats, our interviews and surveys indicate that as many as 25 percent of all threats were not reported to the USMS. We also found that even when the judges and AUSAs reported threats, they often did not do so promptly. In about one-quarter of the reported threats made in FY 2007 and FY 2008, 2 or more days elapsed between receipt of the threat by the judge or AUSA and when they reported the threat to the USMS.

USMS district managers are required to ensure that protectees are aware of the importance of reporting threats. However, according to USMS directives, federal judges receive the USMS security handbook containing the guidance on reporting threats only after they receive a threat. Moreover, the handbook does not emphasize the consequences of delays or failures to report all threats immediately. The USMS told us that it instructs all Judicial Security Inspectors to provide the security handbook to all members of the judiciary as part of the USMS ongoing efforts to protect the judges.

U.S. Attorneys and AUSAs have other potential sources of guidance on threat reporting, such as the *U.S. Attorneys' Manual*. However, we found these sources do not require that all threats be reported to the USMS and do not include guidance that all threats should be reported promptly.

The USMS does not consistently provide an appropriate response for the risk level posed by the threat.

USMS district offices are required to conduct a risk assessment of each threat to identify whether the risk level qualifies as low, potential, or high. The USMS is then required to implement protective measures corresponding to the identified risk level.

In conducting our review of 26 threat cases involving 25 protectees at the 4 districts we visited, we found that the USMS did not record the risk level ratings for any of these threats in its threat database. Because the USMS had not recorded the ratings, we were unable to determine whether the protective measures implemented by the USMS were commensurate with the risk level rating.

Therefore, we sought to determine whether the 25 threatened judges and AUSAs we interviewed had received at least 4 of the

protective measures prescribed by the USMS for threats assessed as low risk. Under the USMS protocol, these protective measures should be provided in response to every threat. Through our interviews and a database review, however, we found that only one protectee received all four protective measures. In addition, five protectees were not provided any of the low risk level protective measures they should have received.

The USMS does not fully or effectively coordinate with other law enforcement agencies to respond to threats against federal judicial officials.

The USMS does not consistently track threat referrals to the FBI.

According to USMS policy, the USMS must notify the appropriate FBI field office when it learns of a threat against a protectee. We examined the threats against judges, U.S. Attorneys, and AUSAs in the USMS threat database that were reported during FY 2007 and FY 2008, and we found that 639 (40 percent) of the 1,587 threats in the database contained no information regarding FBI notification.⁴ We also examined the 26 threats we selected for review in the 4 districts to determine whether USMS records indicated that the FBI was notified of the threat. We found that 5 of the 26 threats (19 percent) contained no information regarding FBI notification.

Coordination between the USMS and the FBI is inconsistent among districts, and there are no formal protocols for coordination.

USMS and FBI policies state that the two agencies should work together closely to respond to threats against judicial officials. USMS and FBI personnel we interviewed at two of the four sites we visited said they coordinate with each other on the protective and criminal investigations in response to threats. However, at the other two sites we visited USMS personnel stated that the FBI does not communicate or share information concerning its criminal investigations, although FBI personnel said the components were coordinating.

No formal or informal agreement between the USMS and FBI defines their respective roles and responsibilities for threat response. As a result, personnel from both components told us that their working relationship and, more specifically, their communication on investigations depend on

⁴ Because the USMS threat database does not distinguish between threats and inappropriate communications, our analysis may include both.

personalities in each of the offices. They stated that a formal memorandum of understanding between the FBI and the USMS is needed.

The USMS districts fail to effectively coordinate with local law enforcement agencies for notification of emergency responses to judges' residences.

USMS policy requires district offices to send letters to the local law enforcement agencies in the jurisdictions where federal judges reside requesting that the USMS be notified whenever a police agency responds to any emergency call at a judge's residence. Three of the four sites we visited had sent such letters that included 24-hour/7-day-a-week USMS contact numbers. USMS officials at the fourth site told us they had not sent the letters because the judges in the district refused to allow the USMS to provide their home addresses to local law enforcement agencies.

We tested the USMS contact numbers provided in the three letters to the local law enforcement agencies. In two districts, when we called the contact numbers we received a recording that they were not working numbers. In the third district, our test call connected first to the courthouse communications office and then was re-directed to a USMS duty officer.

USAO staff who provide protective measures for threatened U.S. Attorneys and AUSAs lack sufficient expertise and training in threat response, and coordination among these entities is inconsistent.

USAO personnel lack expertise in threat response.

While EOUSA and the USAOs have implemented measures to protect USAO personnel against threats, we determined that EOUSA and USAOs lack threat response expertise and training similar to that of the USMS's judicial security staff. Deputy Marshals involved in ensuring the safety of protectees generally have extensive law enforcement training, along with specific training in determining and implementing threat response procedures. Although some USAO staff may have prior law enforcement experience, many do not, and the training available to EOUSA and USAO personnel in security and personal protection is limited. In particular, they do not receive formal training in determining the protective measures that are appropriate for each threat that is equivalent to the training that USMS staff receive.

The Assistant Director and the Threat Management Specialist of EOUSA's Security Programs Staff are responsible for providing guidance to

help the USAOs respond to a threat and for providing funding for the protective measures that are implemented. However, the two individuals in those positions during FY 2007 and FY 2008 did not have backgrounds comparable to that of USMS judicial security staff in responding to threats against individuals. The Assistant Director had prior physical security experience in other agencies, but is responsible for numerous security-related duties and therefore has limited time to devote to threat response or to develop more specialized expertise in the area.

EOUSA relies primarily on the USAOs' District Office Security Managers to provide a protective response in the field. However, at the four locations we visited none of the District Office Security Managers had law enforcement or other experience in threat response. Moreover, the District Office Security Managers told us that they were responsible for numerous other security-related functions in addition to responding to threats. Additionally, training opportunities for District Office Security Managers are limited, and this is problematic for staff with little or no experience in threat response.

Coordination between the USMS and USAOs is inconsistent and is not guided by formal protocols for coordination.

We found that USMS and USAO staff responsible for threat response did not share important information about threats and were not clear on each other's roles and responsibilities regarding protective response. For example, in one district we visited we found that USAO staff did not believe the USMS was required to provide USAO personnel with any protective measures other than [REDACTED] in response to the highest level threats. In that district – even though the courthouse and the USAO's building are adjacent and joined by a common hallway – the USMS district office did not provide USAO building security staff with threat information that had been distributed to courthouse security staff.

Similarly, we found that USMS staff did not regularly advise USAOs about or monitor protective measures implemented by EOUSA and the USAOs. During our site visits we found instances in which EOUSA and the USAOs implemented protective measures without the USMS's knowledge. There is no agreement or memorandum of understanding between the USMS and EOUSA, or between the USMS and any USAOs we visited, which addresses the sharing of information about threats against U.S. Attorneys and AUSAs and coordination of protective measures.

EOUSA is not consistently notified of threats against U.S. Attorneys and AUSAs and often lacks important information about threats and protective responses.

Some USAOs failed to submit required Urgent Reports to EOUSA on threats, and the submitted Urgent Reports frequently lack important information.

We found that threats against USAO personnel are generally not reported to EOUSA. When we compared the threats reported by the USAOs and the USMS districts in FY 2007 and FY 2008, we found that USAOs had reported fewer than half the number of threats reported by the USMS. In each of the four districts we visited, we found that the USAOs sent fewer Urgent Reports to EOUSA than the number of threats recorded in the USMS threat database.⁵ Additionally, when we reviewed the 165 Urgent Reports that District Office Security Managers submitted to EOUSA in FY 2007 and FY 2008 for threats against USAO personnel, we found that 75 percent of the reports were missing key information such as the date the threat occurred and whether the USMS and FBI were notified.

EOUSA is not kept informed of actions taken to protect threatened U.S. Attorneys and AUSAs.

At the time of our fieldwork, the USAOs did not routinely inform EOUSA of the USMS's protective responses to mitigate threats and protect threatened AUSAs. We analyzed the Security Programs Staff threat management database and Urgent Reports submitted by District Office Security Managers about threats and found the USAOs had submitted only 16 updates to the 165 initial Urgent Reports submitted to EOUSA. EOUSA personnel told us that they may receive updates via telephone, e-mails, or updated Urgent Reports. However, EOUSA was unaware of the protective measures provided by the USAO or the USMS, the initiation of an FBI investigation, or the progress of the FBI investigation.

EOUSA told us that it planned to improve the collection of information from USAOs by providing a web-based Urgent Report program in December 2009 or January 2010 so that District Office Security Managers can submit their reports directly to the threat management database, and these web-based forms will include the key information EOUSA needs.

⁵ The USAOs report threats against USAO personnel to EOUSA via Urgent Reports. The Urgent Report contains a brief synopsis of the facts and a concise summary of the event.

RECOMMENDATIONS

As a result of our review, we made 14 recommendations to:

- improve the understanding of federal judges, U.S. Attorneys, and AUSAs of the need for prompt reporting of threats and the consequences of delays or failure to report;
- ensure that the USMS provides protectees with protective measures that are commensurate with the risk level of the threat;
- ensure that the USMS collects information that will enable it to monitor the performance of its response to threats against protectees;
- ensure the USMS coordinates effectively with the FBI and local law enforcement agencies to keep the protectees safe;
- better prepare EOUSA and USAO personnel for responding to threats and to ensure better cooperation between the USMS and the USAOs; and
- ensure that EOUSA receives more complete and timely information to manage its threat response program and ensure the safety of the U.S. Attorneys and AUSAs.

TABLE OF CONTENTS

INTRODUCTION..... 1

BACKGROUND..... 4

RESULTS OF THE REVIEW14

CONCLUSION AND RECOMMENDATIONS40

**APPENDIX I: PREVIOUS OIG REPORTS ON THE JUDICIAL
SECURITY PROCESS43**

APPENDIX II: METHODOLOGY OF THE OIG REVIEW45

**APPENDIX III: RESULTS OF OIG SURVEY OF
U.S. ATTORNEYS AND ASSISTANT U.S. ATTORNEYS48**

**APPENDIX IV: THE UNITED STATES MARSHALS SERVICE'S
RESPONSE78**

**APPENDIX V: OIG'S ANALYSIS OF THE UNITED STATES
MARSHALS SERVICE'S RESPONSE83**

**APPENDIX VI: THE EXECUTIVE OFFICE FOR UNITED STATES
ATTORNEYS' RESPONSE89**

**APPENDIX VII: OIG'S ANALYSIS OF THE EXECUTIVE OFFICE
FOR UNITED STATES ATTORNEYS' RESPONSE93**

REDACTED - FOR PUBLIC RELEASE

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

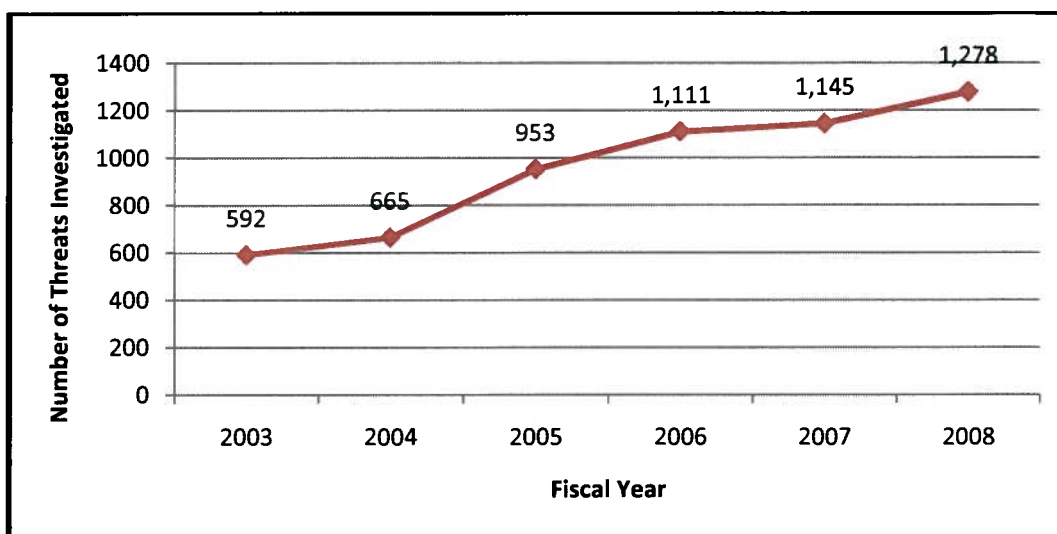
REDACTED - FOR PUBLIC RELEASE

INTRODUCTION

Introduction

Threats against federal judges, U.S. Attorneys, Assistant U.S. Attorneys (AUSA), and other court officials investigated by the U.S. Marshals Service (USMS) have more than doubled during the past several years, increasing from 592 in fiscal year (FY) 2003 to 1,278 in FY 2008.⁶ Overall, during this 6-year period, there were 5,744 threats directed at these federal court officials. Figure 1 presents the number of threats investigated each fiscal year.

Figure 1: Number of Threats Against Federal Court Officials Investigated by the USMS, FY 2003 Through FY 2008



Sources: USMS FY 2008 Budget and www.ExpectMore.gov.

⁶ According to USMS Directive 10.3.G.12, *Protective Investigations*, 2007, a threat is any action or communication, explicit or implied, of intent to assault, resist, oppose, impede, intimidate, or interfere with any member of the federal judiciary, or other USMS protectee, including members of their staffs or family. According to USMS Directive 10.3.G.5, *Protective Investigations*, 2007, an inappropriate communication is any communication directed to a USMS protectee or employee that warrants further investigation. In this report, we use the term “threat” to encompass both threatening and inappropriate communications.

Job-related threats to federal judges, U.S. Attorneys, and AUSAs include physical assaults, verbal assaults, and threatening letters posted on the Internet. In a 2008 Department of Justice (Department) Office of Inspector General (OIG) survey, 7 percent of threatened U.S. Attorneys and AUSAs reported incidents that went beyond written and verbal threats. In those incidents, the threats included attempts to physically intimidate the U.S. Attorneys and AUSAs. For example, two AUSAs reported being physically attacked, one reported that an alleged “contract hit” was put out on him, and another AUSA reported being followed by a family member of a defendant.

Media reports also highlight the nature of threats faced by federal judges and AUSAs. For example, in one incident, a speaker at a rally in Washington, D.C., urged the crowd to find the home of an AUSA who was prosecuting a domestic terrorist and locate where his children attended school. In another incident, a white supremacist wrote on an online blog that three named federal judges deserved to die. The blog post included the judges’ names, work addresses, and telephone numbers, as well as photos of the judges and a map showing the location of the courthouse in which they worked.

Examples of Threatening Letters and Telephone Messages

Example 1: “Go to Judge [REDACTED] court and get pictures of him and his staff. Look for ways to follow each of them after work. Get hang outs, and get phone numbers too – we want records – now this is all very illegal and against the law so be very careful...”

Example 2: “What the **** are you doing? Don't think we wont [sic] kill you and your ****ing wife.... smarten up.”

Example 3: “God wants me to do this. This is what he wants me to do. He wants me to destroy the judge – that judge is evil – he wants me to get rid of her.”

Source: USMS documents.

Purpose

This is the third OIG review to examine the protection of federal court officials. The first review examined the USMS’s protection of federal judges, focusing on measures applied during high-threat trials. The second review examined the USMS headquarters threat assessment process and the USMS’s progress in establishing a protective intelligence function.⁷

⁷ The previous OIG reviews were both titled *Review of the United States Marshals Service Judicial Security Process* and were issued in March 2004 (Evaluation and Inspections Report I-2004-004) and September 2007 (Evaluation and Inspections Report I-2007-010). The prior reports are described in Appendix I.

We conducted this review to examine the USMS's and the Executive Office for United States Attorneys' (EOUSA) response to threats made against federal judges, U.S. Attorneys, and AUSAs. Specifically, we examined the:

1. role and responsibilities of the USMS district offices in the protection of federal judges, U.S. Attorneys, and AUSAs;
2. procedures that USMS district offices employ to assess and respond to threats and incidents against federal judges, U.S. Attorneys, and AUSAs; and
3. role of EOUSA in the protection of the U.S. Attorneys and AUSAs.

Scope

The USMS's district offices are primarily responsible for protecting federal judges, U.S. Attorneys, and AUSAs. Accordingly, we examined how those offices fulfilled the USMS's mission to provide protection when federal judges, U.S. Attorneys, and AUSAs were threatened. Because EOUSA coordinates the relationships between United States Attorneys' Offices (USAO) and other Department components, we also examined its role in the protection of U.S. Attorneys and AUSAs.⁸ Our review encompassed threats that occurred during FY 2007 and FY 2008.

Additionally, although the USMS threat response consists of two functions that occur simultaneously – the protective response and the protective investigation – in this review we focused on the protective response portion of the process.

A detailed description of the methodology of the review is contained in Appendix II.

⁸ We did not review the USMS district offices' actions related to protecting other members of the judicial community, such as probation officers, court reporters, court clerks, or jurors.

BACKGROUND

In this section, we identify the primary organizations that have a role in responding to threats against federal court officials. These organizations include the USMS district offices, the Federal Bureau of Investigation (FBI), EOUSA, USAOs, and the Administrative Office of the U.S. Courts. We also describe the USMS and EOUSA threat response processes.

USMS

The USMS is responsible for ensuring the safe and secure conduct of federal judicial proceedings and for protecting more than 2,000 federal judges and approximately 5,250 U.S. Attorneys and AUSAs and other court officials at more than 400 court facilities in all 94 federal judicial districts. Protecting the judiciary is one of the primary missions of the USMS and a strategic objective of the Department.⁹ The USMS budget for judicial security was \$343 million in FY 2007 and \$344 million in FY 2008.¹⁰

USMS district offices identify potential threats or have threats reported to them and are responsible for determining the protective measures needed to ensure the safety of the protectee. The USMS refers to this as the “protective response.” USMS district office staff is also responsible for conducting a “protective investigation” into a threat.¹¹ The judicial security functions performed by USMS personnel are detailed below.

Judicial Security Inspectors

Judicial Security Inspectors are senior-level Deputy Marshals in the districts who oversee protective investigations conducted by District Threat Investigators. They also implement protective measures, such as conducting residential security surveys and security briefings for threatened

⁹ 28 U.S.C. 566(e)(I)(A).

¹⁰ Additionally, the *Court Security Improvement Act of 2007* authorized \$20 million for each fiscal year from 2007 through 2011 for the USMS to supplement its judicial security operations. However, according to USMS headquarters officials, none of the authorized funding has been appropriated to the USMS.

¹¹ According to USMS Directive 10.3.G.9, *Protective Investigations, 2007*, a protective investigation is the collection and assessment of information to determine a suspect’s true intent, motive, and ability to harm a USMS protectee. The objective of this type of investigation is to eliminate or mitigate any potential risk of harm to the protectee.

federal judges, U.S. Attorneys, and AUSAs.¹² As of February 2009, 113 Judicial Security Inspectors were assigned to the USMS's 94 districts.

District Threat Investigators

In consultation with the Judicial Security Inspectors, the District Threat Investigators conduct protective investigations into threats against USMS protectees. Their primary goal is to implement a threat management strategy to mitigate potential risks to threatened protectees. The District Threat Investigator duty is designated as a collateral duty for Deputy U.S. Marshals, although some District Threat Investigators performed those duties on a full-time basis, while others performed the duties on a part-time or as-needed basis.

Example of Threat Mitigation

An AUSA received several profanity-filled voicemails from an individual who was previously arrested for threatening the President of the United States. The USMS worked with USAO building security officers to prevent the caller from entering the USAO building. As a strategy to mitigate the threat, when the USMS District Threat Investigator interviewed the individual, the investigator warned him that he would be arrested if he attempted to harass or intimidate any court personnel.

Source: USMS documents.

Protective Intelligence Investigators

The Protective Intelligence Investigator is a recently created full-time position responsible for conducting complex protective investigations. Protective Intelligence Investigators report directly to the Chief Deputy U.S. Marshal or Assistant Chief Deputy U.S. Marshal. They are also responsible for proactively identifying, mitigating, and managing potential threats to USMS protectees. Protective Intelligence Investigators provide expertise to the District Threat Investigators during protective investigations and ensure they are adequately trained. As of August 3, 2009, there were 34 Protective Intelligence Investigators in USMS district offices.

¹² Residential security surveys identify areas of vulnerability and provide on-site safety and security recommendations. The residential security survey also provides information and guidance about emergency preparedness and general off-site safety and security. Security briefings provide the protectees with personal security awareness information such as keeping doors to their residences locked and being aware of their surroundings. Judges are given booklets containing this information.

Federal Bureau of Investigation

The FBI is responsible for conducting criminal investigations of threats against federal judges, U.S. Attorneys, and AUSAs. According to USMS policy, USMS District Threat Investigators must notify the appropriate FBI field office when they learn of a threat against a USMS protectee.¹³ Likewise, when the FBI learns of a threat against a USMS protectee the FBI has responsibility for informing the USMS of the threat. When a criminal investigation into a threat is initiated, the FBI case agent should work jointly with the District Threat Investigator.

Executive Office for U.S. Attorneys

EOUSA's primary mission is to provide general executive assistance and supervision to the 94 USAOs, including coordinating and directing the relationships of the USAOs with other components of the Department and providing overall management oversight and technical and direct support to the USAOs in the area of security programs. When U.S. Attorneys or AUSAs are threatened, EOUSA provides financial assistance and guidance to help the USAOs respond to the threat.

Within EOUSA, the Security Programs Staff of the Operations Branch is responsible for providing assistance and advice to the USAOs. According to EOUSA, the Security Programs Staff provides policy and procedural assistance to USAOs for the implementation and conduct of all aspects of security programs and ensures compliance with all national and Department security policies and regulations. The Security Programs Staff also provides general and specialized security training for personnel responsible for security and emergency management or preparedness related duties. The Security Programs Staff supports USAO security education and awareness efforts, including conferences, briefings, videos, brochures, and other materials. It provides budgetary and facilities management support to facilitate the design, procurement, and installation of all security-related equipment, services, and systems. Additionally, the Security Programs Staff oversees the Threat Management program to assist USAOs during threat situations, providing emergency and contingency planning and emergency security support in response to reported threats and natural disasters, as well as a structured methodology for analyzing the overall security practices of each USAO.

¹³ USMS Directive 10.3.E.1.c, *Protective Investigations*, 2007.

The Security Programs Staff is headed by an Assistant Director and includes a Chief of the Regional Security Program, who oversees 22 Regional Security Specialists located in some USAOs, and a Threat Management Specialist, who collects threat-related information to provide emergency support and security to the USAOs.

U.S. Attorneys' Offices

The USAOs are responsible for reporting threats against U.S. Attorneys, AUSAs, and their families to the USMS. According to the *District Office Security Manager's Handbook*, the District Office Security Manager is the principal security officer in each USAO and is responsible for relaying to EOUSA and the USMS all threats against AUSAs that are reported in the District. There are 93 District Office Security Managers in the 94 USAOs.¹⁴

According to the *District Office Security Manager's Handbook*, the District Office Security Manager advises the U.S. Attorney on all security matters and is assisted by other individuals as required. In addition to relaying threats reported by the attorneys to the USMS district office, the District Office Security Manager's duties include:

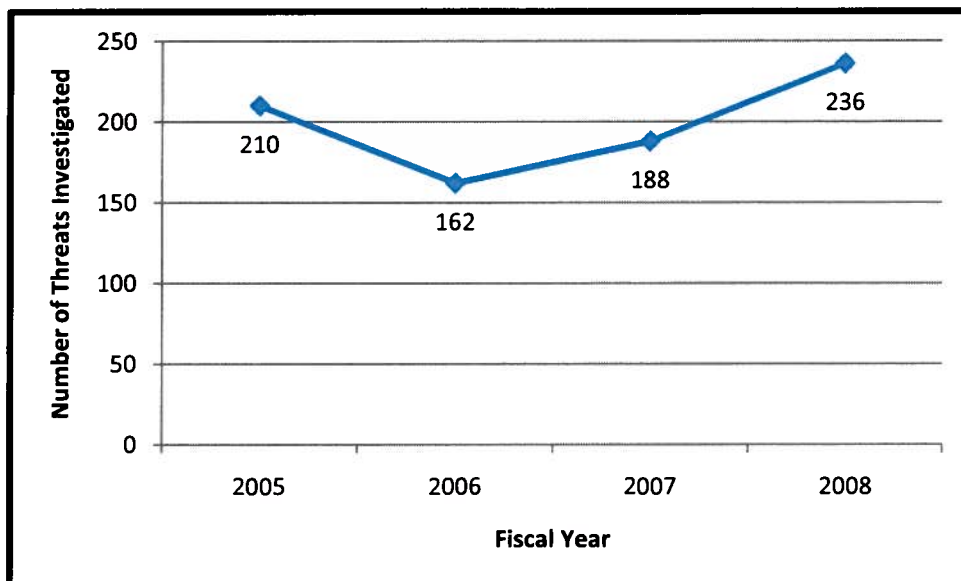
- coordinating the actions of personnel who are assigned security functions;
- analyzing the overall security needs of the USAO and recommending necessary security systems, equipment, and services to reduce vulnerabilities and risks;
- implementing and overseeing the Physical, Information, Personnel, Computer, and Communications Security programs, as well as the Security Education and Awareness, Loss Prevention, and Safety and Health programs;
- developing the District Office Security Plan and all contingency and emergency plans;
- preparing budget estimates for implementing office security programs and coordinating with the Security Programs Staff; and
- preparing and submitting Urgent Reports and Security Incident Reports.¹⁵

¹⁴ One District Office Security Manager oversees both the Guam and Northern Mariana Islands USAOs.

¹⁵ Urgent Reports are submitted on significant events of interest or concern to the Attorney General and Deputy Attorney General. Such events include threats against USAO
Cont'd.

Figure 2 presents the number of threats made against USAO personnel.¹⁶

Figure 2: Number of Threats Against USAO Personnel, FY 2005 Through FY 2008



Sources: Data from *DOJ Report on the Security of Federal Prosecutors* for FY 2005 and FY 2006, and data from USMS threat database for FY 2007 and FY 2008.

Administrative Office of the U.S. Courts

Under the supervision and direction of the Judicial Conference of the United States, the Administrative Office of the U.S. Courts monitors and provides some funding for the USMS’s implementation of the judicial facilities security program to provide security inside federal courthouses. Additionally, the Administrative Office of the U.S. Courts has worked with the USMS to obtain supplemental funding for the USMS to install intrusion detection systems in the residences of federal judges. To date, approximately 1,600 judges have had the systems installed in their residences.

personnel, bomb threats that directly involve a USAO, and any emergency that affects the continued operation of an office.

¹⁶ The USMS threat database does not distinguish between attorneys and other USAO personnel. For this analysis, we used Urgent Reports and USMS threat records for all USAO personnel during FY 2007 and FY 2008.

The Threat Response Process

The USMS district offices receive reports of threats from a variety of sources. Typical sources include judges and their staffs; defense attorneys reporting threats made by their clients; the Federal Bureau of Prisons reporting threats made by inmates; and confidential informants. Threats against U.S. Attorneys and AUSAs may be reported to the USMS by the USAO District Office Security Manager or the attorney being threatened. Figure 3 shows the threat reporting and response process according to policy.

Initial USMS District Response

When a threat is reported to the USMS, the District Threat Investigator or the Protective Intelligence Investigator initially determines whether the communication meets the standard of an “inappropriate communication,” that is, if it is a legitimate threat. If it does, the District Threat Investigator or the Protective Intelligence Investigator notifies the FBI to determine whether a criminal investigation is warranted.

The District Threat Investigator then completes a form, USM-550 Preliminary Threat Report, in the USMS’s threat database. The report contains information about the target of the threat, the type of threat, the delivery method, the suspect, other agencies that have been notified, and a brief synopsis of the threat. District Threat Investigators update the case using a form USM-11 Report of Investigation as more information becomes available.

Determining the Threat Risk Level

The District Threat Investigator and the Protective Intelligence Investigator, in consultation with the Judicial Security Inspector, assess the risk to the protectee. The risk assessment is an initial examination of the suspect’s intent, motive, and ability to carry out the threat. To determine the risk to the protectee, the District Threat Investigator and Protective Intelligence Investigator consider how, where, and to whom the threat was delivered, whether identities of the victim of the threat and any suspects are known, whether any suspect is incarcerated, whether additional victims were named, and how the suspect intends to carry out the threat. Based on this information, the District Threat Investigator and the Protective Intelligence Investigator categorize the threat as a low, potential, or high risk threat.

Figure 3: Threat Response Process

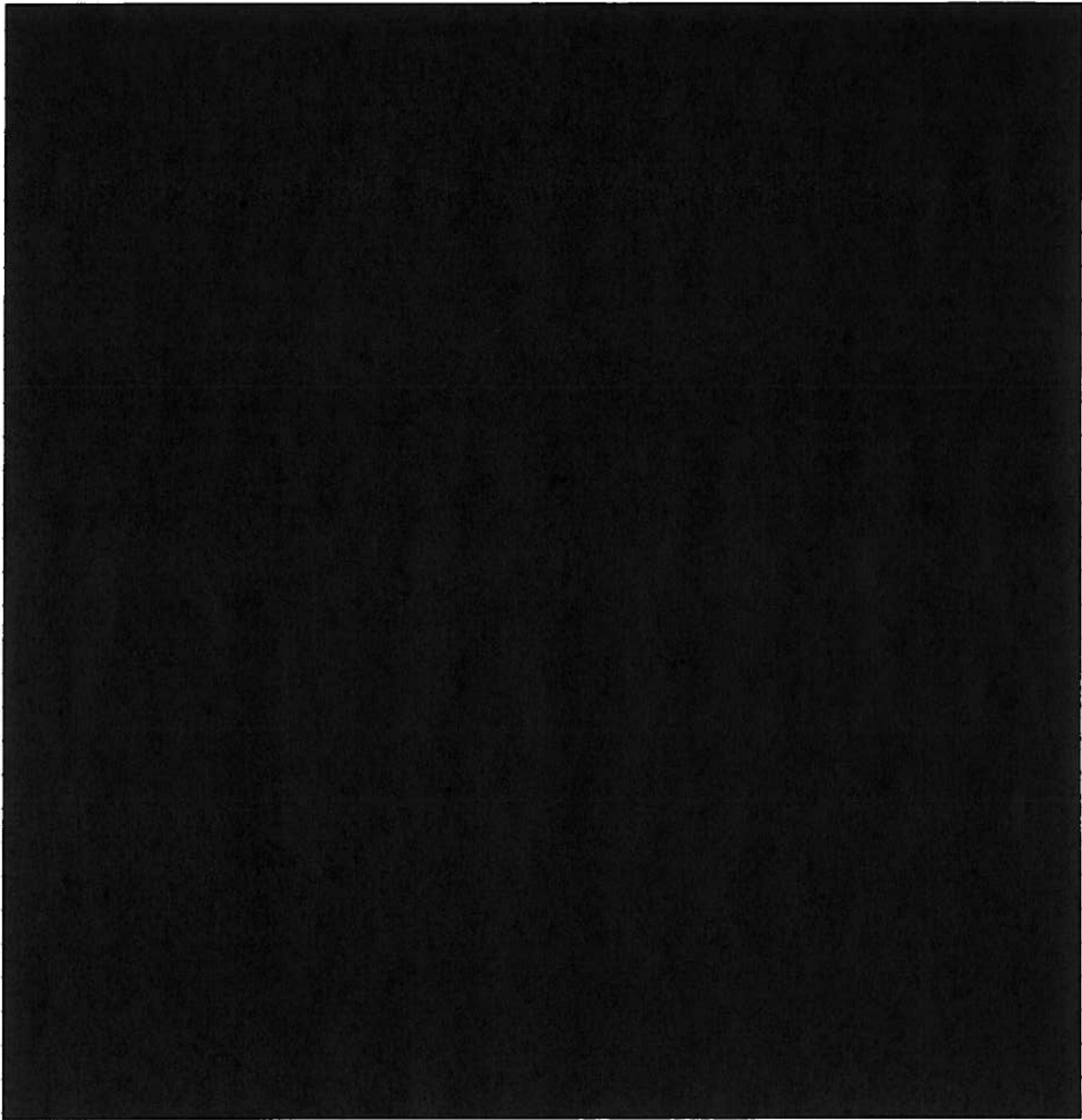
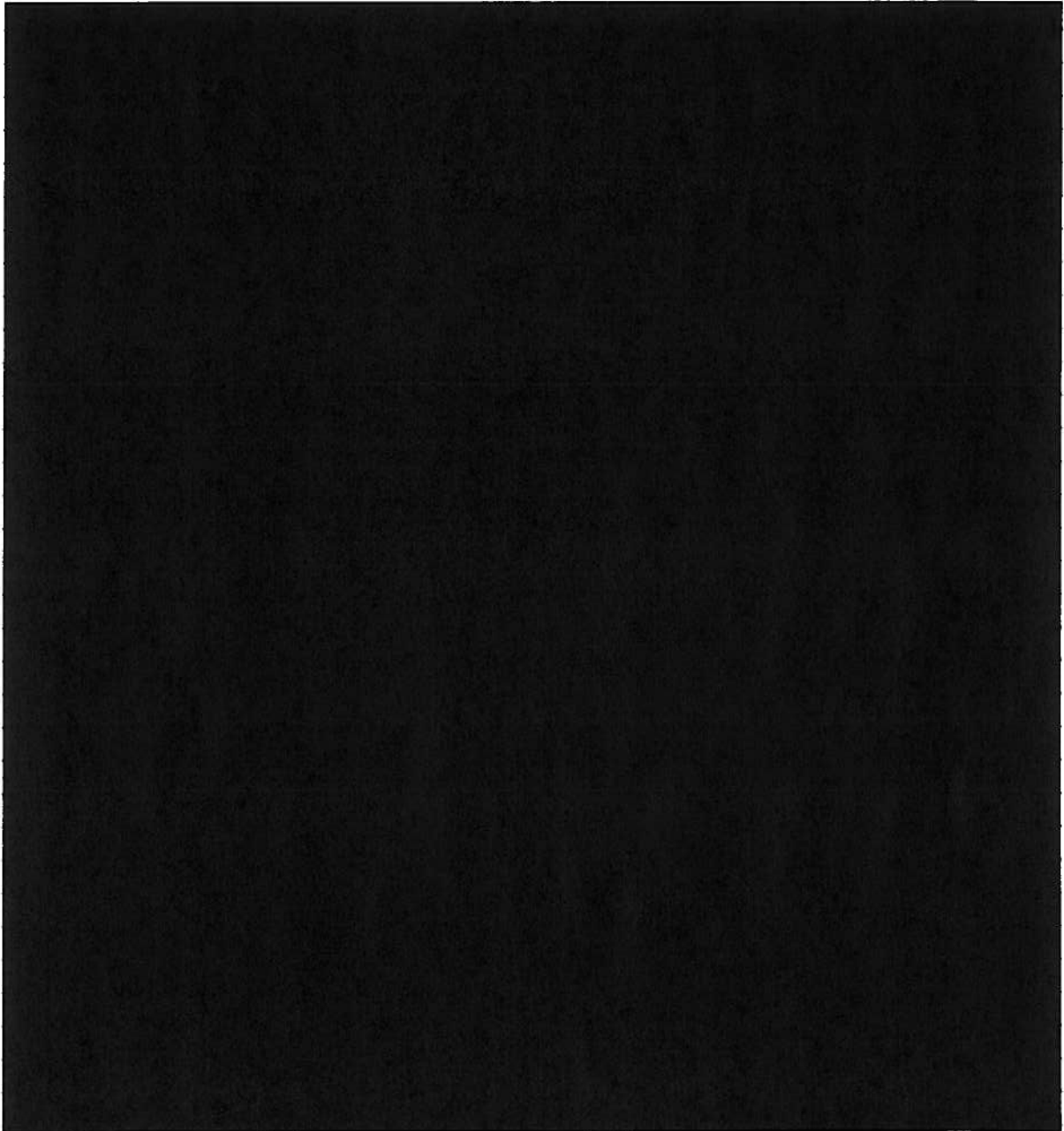


Figure 3: Threat Response Process (Continued)



Recommending the Appropriate Response

Based on the risk assessment, the District Threat Investigator and the Protective Intelligence Investigator recommend an appropriate protective response to the Judicial Security Inspector and the management of the USMS district office. USMS directives establish a progressive protective response based on each of the three risk levels. The protective measures corresponding to these risk levels are considered to be the minimum protective measures that should be implemented for the threat level rating. Risk levels and the associated protective measures are detailed on pages 18 and 19 of this report. Additional protective measures may be implemented if deemed necessary by the District Threat Investigator or Protective Intelligence Investigator.

Conducting the Protective Investigation

The District Threat Investigator or the Protective Intelligence Investigator also conducts a protective investigation to develop further information about the suspect's intent, motive, and likelihood of carrying out the threat, and to mitigate the risk of harm to the protectee.¹⁷ If the protective investigation indicates that a threat is likely to be carried out, the District Threat Investigator or the Protective Intelligence Investigator, in consultation with the Judicial Security Inspector, determines an appropriate investigative response to mitigate the threat.

USMS Headquarters Role

Entering the Preliminary Threat Report into the threat database notifies the Threat Management Center within the Office of Protective Intelligence at USMS headquarters of the threat.¹⁸ Using information from the report, the Office of Protective Intelligence conducts background checks of law enforcement databases, including the threat database, to determine whether any data exists on any suspect or previous threats. The Office of Protective Intelligence then makes investigative recommendations and provides its report to the USMS district office within 1 business day after the threat is reported. The Office of Protective Intelligence also conducts a

¹⁷ The protective measures and the protective investigation are initiated simultaneously.

¹⁸ The USMS opened the Threat Management Center (TMC) at USMS headquarters in September 2007. Duty inspectors are available to respond to the districts' questions and receive reports of threats 24 hours a day.

computer-based analysis, referred to as a comparative analysis, using the information from the district office and its own database queries.¹⁹

[REDACTED]

Threats Against U.S. Attorneys and AUSAs

The District Office Security Managers in the USAOs are responsible for reporting threats received by U.S. Attorneys and AUSAs. A District Office Security Manager may learn of a threat directly from the threatened attorney, a supervisor, or from any other source. When the District Office Security Manager learns of a threat, the Security Manager is required to notify the USMS, the local FBI office, and EOUSA. The District Office Security Manager notifies EOUSA of a threat by e-mailing an Urgent Report to the EOUSA Security Programs Staff. The Urgent Report contains a one-paragraph synopsis of the facts and a concise summary of the situation surrounding the event.

EOUSA Emergency Support

The Threat Management Specialist at EOUSA receives and reviews Urgent Reports to determine if details about the threat, the protective measures implemented by the USMS, or any other pertinent facts were omitted from the report. If information was omitted, the Threat Management Specialist contacts the USAO's District Office Security Manager to request additional information.

After reviewing an Urgent Report, EOUSA may provide emergency security support to the USAO, including a review of the district's security measures and advice and assistance to threatened individuals on dealing with the threat. EOUSA also compiles and coordinates threat-related information with the USMS, the FBI, and other sources to determine the nature of the emergency security support required by the USAO or individual to adequately address the risk posed by the threat. During the threat response process, the Threat Management Specialist maintains contact with the District Office Security Manager to monitor changes in the status of the threat. In addition, the Threat Management Specialist acts as a liaison with the USMS to obtain any further information that it may have about the threat against a U.S. Attorney or AUSA.

¹⁹ A comparative analysis compares the case's known characteristics with the characteristics of previous threat cases maintained in the USMS's threat database. The result of the comparative analysis is expressed as a score that indicates how closely the characteristics of the case being assessed match those of prior cases.

RESULTS OF THE REVIEW

We found deficiencies in several critical areas of the USMS threat response program. Federal judges, U.S. Attorneys, and AUSAs do not consistently and promptly report threats they receive. Moreover, we found that when threats are reported, the USMS protective response is not fully or effectively coordinating with other law enforcement agencies to respond to threats against federal court officials. In addition, we found that USAO personnel without sufficient expertise and training are providing some protective measures for threats against U.S. Attorneys and AUSAs. Moreover, when U.S. Attorneys and AUSAs are threatened, USAOs do not typically provide EOUSA with the information it needs to provide emergency security support to the USAOs and the threatened U.S. Attorneys and AUSAs.

Judges, U.S. Attorneys, and AUSAs do not consistently and promptly report threats.

Judges, U.S. Attorneys, and AUSAs do not report all threats.

Although we could not determine the number of unreported threats, our interviews and surveys indicate that as many as a quarter of all threats were not reported to the USMS. Most federal judges, U.S. Attorneys, and AUSAs told us that they reported every threat made to them, but others said they did not report all threats they received. Table 1 summarizes the reporting and non-reporting of threats by judges, U.S. Attorneys, and AUSAs interviewed or surveyed by the OIG.

Table 1: Threat Reporting by Protectees

Protectee	Interviewees		Survey Respondents	
	Reported All Threats	Did Not Report All Threats	Reported All Threats	Did Not Report All Threats
Judges	8 (73%)	3 (27%)	174 (78%)	48 (22%)
U.S. Attorneys and AUSAs	11 (79%)	3 (21%)	47 (77%)	14 (23%)

Note: The OIG surveyed the federal judges in 2006 and the U.S. Attorneys and AUSAs in 2008.
Sources: OIG interviews and surveys.

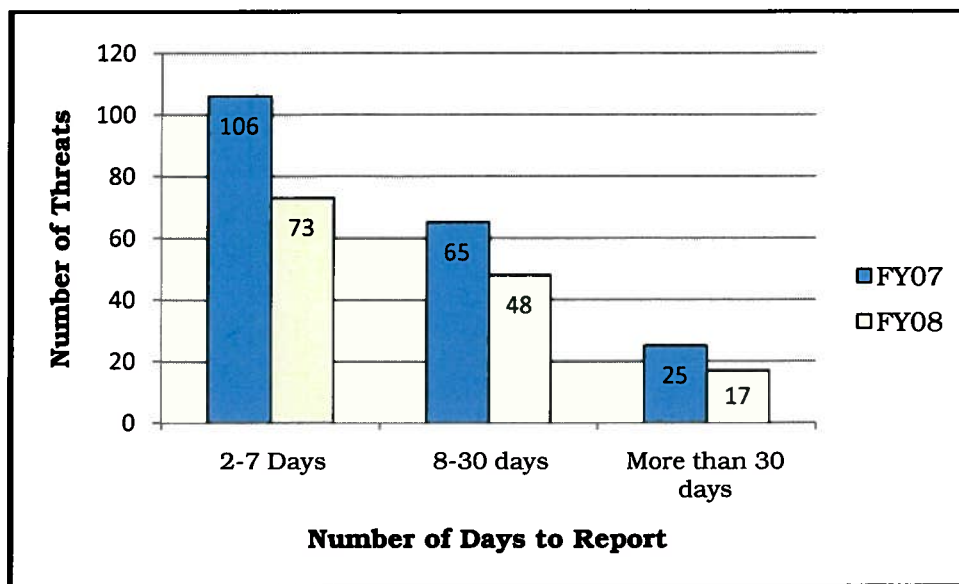
The federal judges, U.S. Attorneys, and AUSAs who did not report all threats to the USMS said they did not do so because they believed the threats were not serious. For example, one judge stated that he reported physical or anonymous threats to the USMS, but did not report threats he viewed as vague or indirect. Additionally, one AUSA stated that he did not immediately report a threat he received because he did not take it seriously. A day or two later, he casually mentioned it to a supervisor who then reported it.

Federal judges, U.S. Attorneys, and AUSAs delayed reporting threats to the USMS.

We found that even when judges, U.S. Attorneys, and AUSAs reported threats they did not always promptly notify the USMS of the threats. According to the USMS threat database, during FY 2007 and FY 2008 judges, U.S. Attorneys, and AUSAs reported 1,368 threats.²⁰ Of 766 threats reported by the protectees in FY 2007, 196 (26 percent) were reported to the USMS 2 or more days after the threats were received (Figure 4). Of 602 threats reported in FY 2008, 138 (23 percent) were similarly delayed. In fact, one threat was not reported until 363 days after it was received. Although the number of delayed threat reports decreased from FY 2007 to FY 2008, untimely reporting of threats remains a problem as it prevents the USMS from immediately ensuring the safety of the protectees.

²⁰ We excluded from this analysis threats that were brought to the attention of the protectee or the USMS by an informant because there may have been a delay between the date the threat was made and the date the informant reported the threat. We also counted threats that were made to multiple protectees by one threatener on a single date and were reported to the USMS on a single date as one threat.

Figure 4: Number of Threats Reported After 2 or More Days



Source: USMS database.

Federal judges, U.S. Attorneys, and AUSAs receive insufficient guidance on reporting threats.

We believe that the USMS must ensure that judges, U.S. Attorneys, AUSAs, and court personnel are aware of the importance of reporting threats to the USMS. For federal judges, guidance is contained in a security handbook that instructs judges to contact the USMS district office if they receive a threat. However, the USMS is only required to provide the handbook containing the guidance on reporting threats *after* the judge is threatened. Moreover, our review of the handbook found that it does not emphasize the consequences of delays or failures to report all threats immediately for the judicial security program to operate most effectively. The USMS told us that it instructs all Judicial Security Inspectors to provide the off-site security handbook to all members of the judiciary as part of its ongoing efforts to protect the judges.

U.S. Attorneys and AUSAs do not receive the USMS's security handbook. Instead, they refer to the *U.S. Attorneys' Manual*, which establishes requirements for what must be done only *after* a threat has been reported to the District Office Security Manager. The manual does not provide USAO staff with guidance on what to do when they receive a threat, and it does not require that all threats must be reported to the District Office Security Manager. The District Office Security Managers we interviewed stated that they only briefly discuss the need to report with the U.S. Attorneys and AUSAs in their offices. The importance of reporting threats is not being effectively communicated, as

demonstrated by our 2008 survey results showing that 6 of the 36 U.S. Attorneys and AUSAs who received training and were threatened did not report the threats.

When judges, U.S. Attorneys, and AUSAs do not promptly report to the USMS all threats they receive, the USMS cannot provide timely protection or take other actions to prevent suspects from harming the protectees. Additionally, failure to report all threats makes it more difficult for the USMS to detect patterns of behavior that might indicate a suspect may escalate a threat to a violent attack. Consequently, the ability of the USMS to protect federal judges, U.S. Attorneys, and AUSAs can be compromised.

Conclusion and Recommendations

To improve the understanding of federal judges, U.S. Attorneys, and AUSAs of the need for prompt reporting of threats and the consequences of delays or failure to report, we recommend that:

1. the USMS clearly explain to protectees the detrimental effect that delays or the failure to report has on the security provided.
2. the USMS update its security handbook to emphasize both the importance of immediately reporting threats to the USMS and the consequences of delays or failures to report.
3. EOUSA amend the *U.S. Attorneys' Manual* to clearly instruct the AUSAs that all threats must be reported promptly to the District Office Security Manager. Such instruction should include an explanation of the detrimental effect that delays or the failure to report has on the security provided.
4. the USMS review trends in reporting timeliness annually and provide the results of that analysis to the Administrative Office of the U.S. Courts and EOUSA for their use in judicial conferences and attorney training seminars.

The USMS does not consistently provide an appropriate response for the risk level posed by the threat.

The USMS did not consistently use its risk levels in assessing threats.

Determining whether the USMS implemented a protective response that was commensurate with the risk to the protectee requires a comparison of the implemented protective measures to the identified risk level of a threat.²¹ The minimum protective response is the response required by USMS directives, but the districts may implement other protective measures to ensure the safety of the protectee. The minimum protective response is dependent on the risk level determined by the District Threat Investigator. The following is a description of the risk levels and minimum protective measures for each level:

- **Low risk** - Risk of injury or death is assessed as unlikely and it is determined that the suspect does not appear to currently pose a credible, imminent risk to the protectee. Minimum protective measures to be taken are:

1. [REDACTED]
2. [REDACTED].²²
3. [REDACTED].²³
4. [REDACTED].²⁴

²¹ In this section, we use the term "threat" to encompass both threatening and inappropriate communications.

²² [REDACTED]

²³ [REDACTED]

²⁴ [REDACTED]

Cont'd.

5. [REDACTED].

- **Potential risk** – Risk of injury or death to the protectee is assessed as possible, but not imminent. These measures are implemented in addition to the protection provided for low level risks.

6. [REDACTED].

7. [REDACTED].

8. [REDACTED].

- **High risk** – Risk of injury or death to the protectee is assessed as likely. These measures are implemented in addition to the protection provided for low and potential level risks.

9. [REDACTED].

10. [REDACTED].

We examined the USMS threat database and interviewed USMS personnel to assess whether they determined the risk levels. However, we found no risk level ratings recorded in the threat database for any of the 26 threats we reviewed during our site visits.²⁵ Moreover, District Threat Investigators at the four sites we visited did not consistently use the risk levels as the minimum standard for determining the protective measures they provided to threatened judges, U.S. Attorneys, or AUSAs. Only one of four District Threat Investigators we interviewed said that he performed the risk assessments, although he said he did not document the levels in the threat database.²⁶ He said he did document “potential” and “high” risk level ratings in written threat assessments.²⁷ Although it was his responsibility to do so, a second District Threat Investigator said he does not perform risk assessments.

[REDACTED]

²⁵ One of the 25 protectees we interviewed during our site visits had 2 threats, which made the total number of threats we reviewed 26.

²⁶ According to USMS Directive 10.14.E.1, *Protection Details*, 2006, a risk assessment determines the appropriate level of protective response.

²⁷ According to USMS Directive 10.3.G.11, *Protective Investigations*, 2007, a threat assessment is a determination that a suspect either poses a threat or does not pose a threat to a USMS protectee.

Instead, he said that the Judicial Security Inspector performed them. The only time the third District Threat Investigator said that he performed a risk assessment was to determine whether a protectee needed a protective detail. The fourth District Threat Investigator said he depended upon his experience and knowledge and that he relied on the risk levels only for guidance. None of these three District Threat Investigators documented the risk levels in the threat database.

The USMS does not ensure that districts consistently provide the minimum protective measures that are required for each threat.

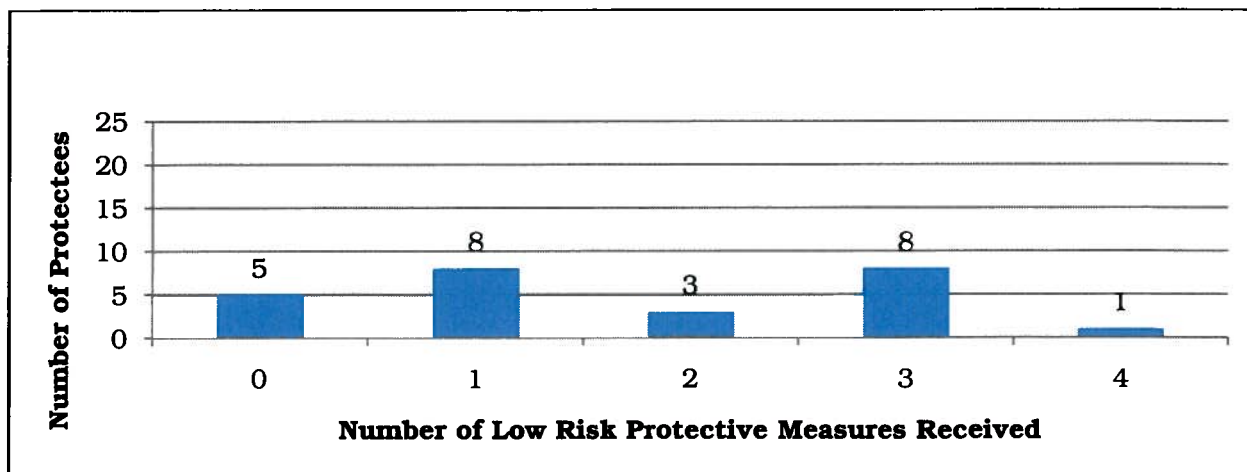
Although risk levels were not recorded for any of the threats we reviewed, for every threat received by its protectees, the USMS is required to provide *at least* the protective measures for the low risk level.²⁸ However, we found that the USMS threat database did not contain documentation to show that the minimum required protective measures had been provided to the protectees.

Therefore, we sought to determine through interviews whether the USMS had provided 25 judges and AUSAs at the sites we visited with at least four of the low risk level protective measures in response to the threats they received.²⁹ Only 1 of the 25 protectees we interviewed recalled receiving all four protective measures required for a low risk level threat. In addition, 5 of the 25 protectees (4 judges and 1 AUSA) did not recall receiving any of the required protective measures, and the USMS database did not indicate that they had received any. Figure 5 below presents the results of our analysis.

²⁸ According to USMS Directive 10.3.E.1.b, *Protective Investigations*, 2007, “when district management receives a report of a threat/inappropriate communication, involving a protectee, steps will be taken immediately to ensure the protectee’s safety.”

²⁹ As noted previously, we did not include in our analysis the office facility security survey protective measure.

Figure 5: Number of Protective Measures Provided to 25 Protectees Who Received Threats



Sources: OIG interviews and USMS database.

Conclusion and Recommendation

The USMS does not ensure that the protective measures provided to protectees are commensurate with the threat because the risk assessments are not consistently performed or documented. In addition, the evidence did not show that the USMS was consistently implementing even the minimum protective measures required for the lowest risk threats. We recommend that:

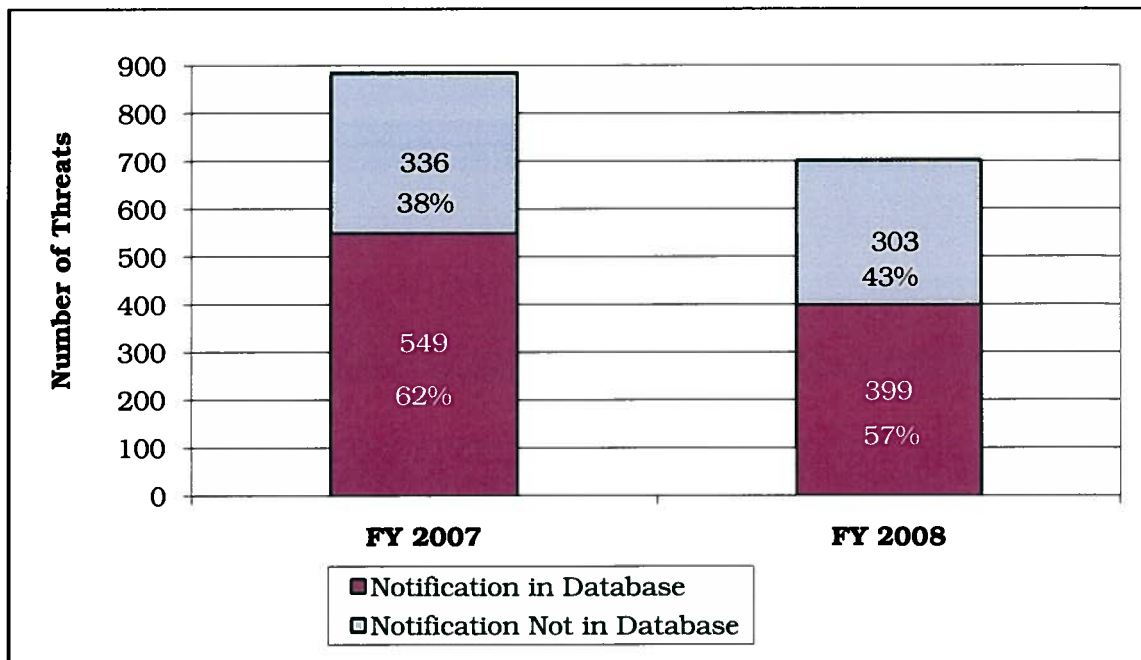
5. the USMS implement controls to ensure that required risk assessments are completed and documented in the USMS threat database, including the assignment of risk levels, and that the protective measures provided in response to each threat also be documented in the USMS threat database.

The USMS does not fully or effectively coordinate with other law enforcement agencies to respond to threats against federal judicial officials.

The USMS does not consistently track threat referrals to the FBI.

We examined the threats against judges, U.S. Attorneys, and AUSAs in the USMS threat database reported during FY 2007 and FY 2008 to determine whether the USMS reported them to the FBI.³⁰ Because the USMS threat management database does not distinguish between threats and inappropriate communications, our analysis may include both. We found that 639 (40 percent) of the 1,587 threats in the database contained no information regarding FBI notifications. Figure 6 displays the notification information for the threats by fiscal year.

Figure 6: FBI Threat Notifications in the USMS Threat Database for FY 2007 and FY 2008



Source: USMS threat database.

We also examined whether USMS records indicated that the FBI had been notified of the 26 threats we selected for review at the four sites we visited. We found that only 21 of the 26 threat entries in the database

³⁰ In this section, we use the term “threat” to encompass both threats and inappropriate communications.

(81 percent) showed that the FBI had been notified. The remaining 5 entries (19 percent) contained no information in the “Date Notified” field regarding FBI notification.

The USMS threat database is the only written record that informs USMS headquarters of whether or not the FBI has been informed of threats, and only the district offices can enter this information based on their actions. If the data fields are blank, the only way that USMS headquarters can verify that the FBI has been notified of threats is to call the districts and rely on the memory of district personnel.

Coordination between the USMS and the FBI is inconsistent among districts, and there are no formal protocols for coordination.

USMS and FBI policies state that the two agencies should work closely together to respond to threats against judicial officials.³¹ We interviewed District Threat Investigators and FBI Special Agents at each of the four sites we visited to determine the extent of coordination between the USMS and FBI. At two sites, we found that the USMS and FBI coordinate the protective and criminal investigations.

However, we received inconsistent statements from the USMS and the FBI about the level of coordination at the other two sites we visited. At both of those sites, the USMS District Threat Investigators stated that the FBI does not communicate

An Example of Inconsistent Statements about Coordination

A speaker at a rally exhorted the crowd to harass an AUSA who was prosecuting a domestic terrorist, berating him and telling the crowd to find where the AUSA lived and worked, where his children went to school.

When the AUSA learned of this rally, he informed the USMS, the USAO District Office Security Manager, and the FBI. The USMS and the FBI investigated and monitored the case, but according to the USMS, the FBI took 7 days to respond with its case information. Without the FBI's investigative results, the USMS was unable to determine whether an escalation of protective measures was necessary. However, the FBI stated that it was unaware of the USMS's dissatisfaction regarding information sharing.

Sources: News articles and interviews with the USMS and the FBI.

³¹ When the FBI opens a criminal investigation regarding a threat, the District Threat Investigator should work jointly with the FBI case agent. According to the *USMS Guide to Protective Investigations and Contemporary Threat Management*, joint investigations with the FBI must be full partnerships, with complete sharing of information and sources, but the district should not delay conducting a protective investigation in deference to the FBI's criminal investigation. The *FBI Manual of Investigative Operations and Guidelines* states that when the FBI institutes a criminal threat investigation, close liaison should be established with the USMS office responsible for the protectee.

or share information concerning its criminal investigations. In contrast, the FBI Special Agents said the components were coordinating. The FBI agent at one site stated that he considers himself and the District Threat Investigator to be partners in the investigation. The FBI agent at the other site told us that once the FBI is notified of a threat, the FBI provides all the information it has to the USMS.

We also found there is no formal or informal agreement between the USMS and FBI that defines the roles and responsibilities of USMS District Threat Investigators and FBI agents. District Threat Investigators and FBI agents we interviewed told us that communication between the USMS and the FBI regarding their respective investigations and their working relationships depend on personalities. They stated that a formal memorandum of understanding between the FBI and the USMS is needed.

The USMS districts fail to effectively coordinate with local law enforcement agencies for notification of emergency responses to judges' residences.

USMS policy requires district offices to send letters to local law enforcement agencies that provide coverage to an area in which a federal judge resides, requesting that the USMS be notified whenever an agency responds to any emergency call from a judge's residence.³² The letter must also provide the local law enforcement agency with a local USMS district office 24-hour number for the notification. Upon being notified of a local law enforcement agency response to a potential emergency at a judge's residence, the USMS district office can assess the incident in the context of any current threats and determine whether the incident may be related.

At the four sites we visited, we asked Judicial Security Inspectors whether the district offices had sent the letters to local law enforcement agencies and whether the Judicial Security Inspectors tracked their districts' responses to notifications of emergencies at federal judges' residences. Three of the four sites we visited had sent letters, but USMS officials at the fourth site told us they had not done so because the judges refused to allow information regarding where they resided to be provided to the local law enforcement agencies.

When we examined the letters, we found that those sent by two of the three sites provided the telephone number of a USMS duty officer to contact in the event of a response to an emergency. The letters sent by the third site

³² For ease of reference in this report, any call from a federal judge's residence that results in a local law enforcement agency response is considered an emergency call.

included no telephone number for the duty officer, but did provide a contact number for the letters' recipients to call if they had questions about the USMS's request to be notified.

We tested the 24-hour USMS contact numbers provided to the local law enforcement agencies.³³ In one district, the USMS contact number had been disconnected. In another district, our call was never answered and did not connect to voicemail or a message; a second number provided in this district's letter to local law enforcement agencies was "temporarily out of service." In a third district, our test call during business hours connected to the communications office at the federal courthouse, which was staffed not by Deputy U.S. Marshals but by Court Security Officers. We called again after normal business hours and our call connected to the Federal Protective Service instead of the USMS duty officer. In both instances (during business hours and after), we were re-directed to a USMS duty officer. In sum, none of the four districts we visited provided local law enforcement agencies with telephone numbers that would let the agencies notify the USMS directly in the event of a response to an emergency at a federal judge's residence.

Also, none of the districts we visited had a system for tracking the number of times local law enforcement agencies had notified them of emergency responses at judges' residences. At three of the districts, the Judicial Security Inspectors we interviewed were able to provide only anecdotal estimates, such as "less than a handful of times" and "at least six times." The fourth district we visited has one of the largest number of federal judges of any of the 94 districts. At the judges' request, this district did not ask local law enforcement agencies to notify the USMS of emergency responses at judges' residences. Not surprisingly, the Judicial Security Inspector in this district stated he had never been notified by a local law enforcement agency of an emergency response to a judge's residence.

The failure to ensure timely coordination with local law enforcement agencies can hinder the USMS in obtaining information that could enable it to swiftly determine whether USMS personnel should initiate a threat investigation and implement protective measures. Further, failing to gather this information prevents the USMS from identifying patterns of activity that could warn of would-be attackers' attempts to test or probe defenses.

³³ The OIG made these calls on July 20, 2009.

Conclusion and Recommendations

The USMS lacks the full range of information it needs to most effectively manage its threat response program. For approximately 40 percent of the threats reported in FY 2007 and FY 2008, the USMS's database does not show that the FBI was notified of the threats. Further, based on our site visits to four districts, the coordination and communication between the USMS and the FBI about threats to protectees are inconsistent and dependent upon personalities instead of a formal process or memorandum of understanding.

We also found that the USMS is not coordinating effectively with local law enforcement agencies. None of the four districts we visited had sent notification letters that would enable local law enforcement agencies to directly notify the USMS when they respond to an emergency at a federal judge's residence.

To ensure that the USMS collects information that will enable it to monitor the performance of its response to threats against protectees, and to ensure the USMS coordinates effectively with the FBI and local law enforcement agencies to keep the protectees safe, we recommend that the USMS:

6. establish internal controls at USMS headquarters to ensure that the USMS threat database contains full and accurate information, including ensuring that district offices regularly enter data in the "FBI Notified" and notification date fields.
7. coordinate with the FBI to establish a memorandum of understanding to formalize the coordination of protective and criminal investigations.
8. develop a mechanism to track the USMS district office responses to emergency notifications from local law enforcement agencies regarding emergency responses to federal judges' residences.
9. ensure that all districts send the required notification letters to local law enforcement agencies and that the letters contain a working contact number that connects directly to the local USMS duty officer.

USAO staff who provide protective measures for threatened U.S. Attorneys and AUSAs lack sufficient expertise and training in threat response, and coordination among these entities is inconsistent.

USAO personnel lack expertise in threat response.

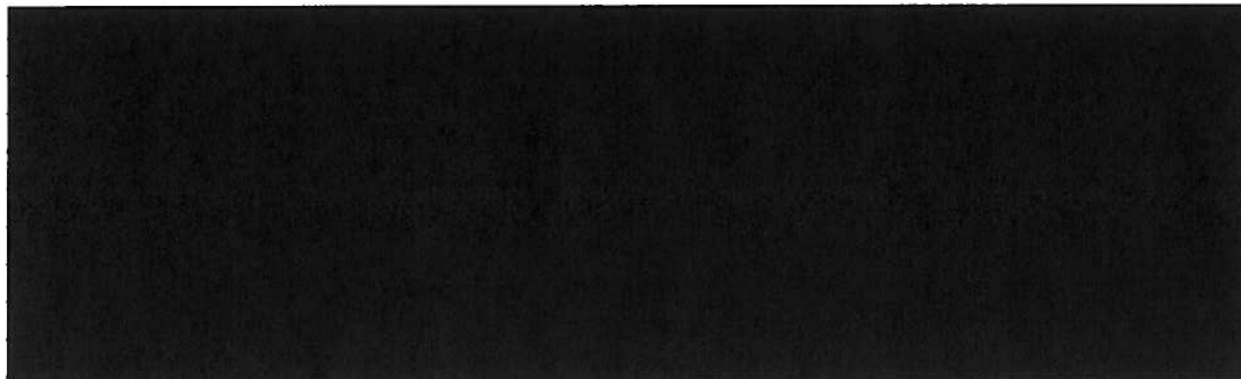
EOUSA and the USAOs have implemented measures to protect USAO personnel against threats, but we determined that EOUSA and the USAOs lack training and expertise in the threat response process similar to that of the USMS's judicial security staff. Deputy Marshals involved in ensuring the safety of protectees generally have extensive law enforcement training, along with specific training in determining and implementing threat response procedures. In contrast, while some USAO staff may have prior law enforcement experience, many do not, and the training available to EOUSA and USAO personnel to develop their expertise in security and personal protection is limited.

During our site visits, we interviewed 14 AUSAs who had been threatened. We determined that EOUSA or the USAOs provided many protective measures to the 14 threatened AUSAs.³⁴ In total, nine types of protective measures were provided to the AUSAs – three solely provided by EOUSA and the USAOs, and three provided by the USMS as well as EOUSA and the USAOs.³⁵ Figure 7 below presents the comparison of the protective measures provided by the USMS and EOUSA and the USAOs to the AUSAs.

³⁴ We asked the AUSAs and reviewed documentation from the USMS and EOUSA threat databases to determine the source of protective measures. In our interviews, we asked the attorneys about the protective measures associated with each of the risk levels (see pages 18 and 19 for a description) and whether EOUSA and the USAO, or the USMS had provided those measures. We also included other protective measures such as [REDACTED] when we were able to identify which component provided it.

³⁵ Two other protective measures ([REDACTED]) were only implemented by the USMS. The remaining protective measure, [REDACTED], requires the involvement of both the USMS and EOUSA. The USMS does [REDACTED], but only after EOUSA submits a request and verifies that [REDACTED].

**Figure 7: Protective Measures Provided by EOUSA/USAOs
and USMS Districts**



Sources: EOUSA Security Programs Staff database, USMS threat database, and AUSA interviews.

We next examined the expertise and duties of the staff providing these measures.

EOUSA. Two persons within EOUSA's Security Programs Staff are involved in threat response: the Assistant Director of the Security Programs Staff and the Threat Management Specialist. The Assistant Director is responsible for numerous security-related duties, including overseeing security training for USAO personnel responsible for security-related duties and budgetary and facilities management support for security-related equipment, services, and systems. The Assistant Director's background includes prior physical security experience in other agencies, but no direct training or experience equivalent to that of USMS judicial security personnel. Moreover, because of his other duties, we believe the Assistant Director has limited time to devote to threat response and to develop more specialized expertise in the area.

The Threat Management Specialist at the time of our review was more focused on the threat response. She was responsible for collecting, recording, and distributing threat information for 94 USAOs; developing contacts with the USAOs to update information regarding the threats; and maintaining contacts with the USMS to ensure that EOUSA is aware of every threat to the U.S. Attorneys and AUSAs. Finally, both the Assistant Director and the Threat Management Specialist had been on board at EOUSA only since 2007 and lacked institutional knowledge for dealing with the varying circumstances that each threat presents.

USAOs. EOUSA relies on the USAOs' District Office Security Managers in the field to provide protective responses. However, at the four locations we visited, none of the District Office Security Managers had law enforcement experience involving threat response. Moreover, the District Office Security Managers told us that they were responsible for numerous other security-related functions in addition to responding to threats.³⁶ The *U.S. Attorneys' Manual* recommends that District Office Security Manager responsibilities be assigned to Supervisory Assistant U.S. Attorneys as a collateral duty to their primary function as attorneys. As of September 2008 a large number of District Office Security Managers, 40 of 94 (43 percent), were AUSAs. At two of the USAOs we visited, the position was held by AUSAs, but in one of those districts a full-time security specialist performed the District Office Security Manager duties. The other two USAOs had full-time, non-AUSA District Office Security Managers.

Moreover, training opportunities are limited for District Office Security Managers, which is particularly problematic for those with little or no experience in threat response. EOUSA offers a training conference for District Office Security Managers at the Department's training center, the National Advocacy Center, every 18 months.³⁷

Example of a Delay in Protective Measures Provided by a USAO

In one district in which EOUSA funded two residential security systems for threatened attorneys, the installations were delayed. In both instances, the delays occurred when the USAO District Office Security Manager did not follow up with EOUSA to ensure that the paperwork was completed and that the security systems were installed in a timely fashion. As a result, there was a 2-month delay in the installation of each home security system. USAO staff told us that the lapse occurred because the District Office Security Manager was responsible for a large number of duties in addition to responding to threats.

Source: Interviews with USAO staff.

³⁶ The District Office Security Managers we spoke with told us they were responsible for physical security, personnel security (e.g., background investigations), Sensitive Compartmented Information Facility control, communications security, office safety (e.g., employee accidents and fire drills), managing the Special Security Officers contract, and building parking, along with the Critical Incident Response Plans and Teams, Continuity of Operations Plans, and Continuity of Government plans.

³⁷ According to the former Director of EOUSA, if a District Office Security Manager is appointed when a conference is not to be held for another 18 months, the departing District Office Security Manager might train the new recruit. Additionally, if the District Office Security Manager requests it, EOUSA will send someone from another USAO to train the individual.

However, in the past that training has included only a 1-hour session on threat response.³⁸ In addition, the guidance available to the District Office Security Managers is not sufficiently comprehensive to give them the tools to provide an effective threat response. Neither the *U.S. Attorneys' Manual* nor the *District Office Security Manager's Handbook* explains the role and duties of a District Office Security Manager. The *U.S. Attorneys' Manual* simply states that the District Office Security Manager notifies the USMS and the FBI of the threat, and serves as a coordinator for protective measures. It does not explain how the District Office Security Manager is to carry out these duties to provide an effective response. The *District Office Security Manager's Handbook* concentrates on the roles of the USMS and EOUSA, and only directs the District Office Security Manager to contact the Security Programs Staff when requesting a home alarm installation.

Coordination between the USMS and USAOs is inconsistent and is not guided by formal protocols for coordination.

In our interviews, we found that the USMS and USAO staff did not share key information regarding protective responses and were not clear on each other's roles and responsibilities regarding the response to a threat against a U.S. Attorney or AUSA. Regarding information sharing, we found that USMS staff did not regularly advise or monitor – and in some cases did not even know about – protective measures implemented by EOUSA and the USAOs. During our site visits we found instances in which EOUSA and the USAOs implemented protective measures without the USMS knowing about them. For example, in one district we found that two USAO employees performed residential security surveys without the assistance of the USMS, and one of these employees initiated the installation of residential security systems without giving the USMS the opportunity to advise on the need for, or the configuration of, the system.

We also found instances in which USMS and USAO staff expressed confusion over each other's roles and responsibilities in threat protection for USAO staff. For example, in one of the districts, we found that the USAO staff did not believe the USMS was required to provide any protective measures other than [REDACTED] in response to the highest level threats. A USAO official in that district told us the USMS's threat response program was focused exclusively on judges. In that same district, when the lives of an AUSA and her child were threatened, the AUSA reported the threats to the USAO, and

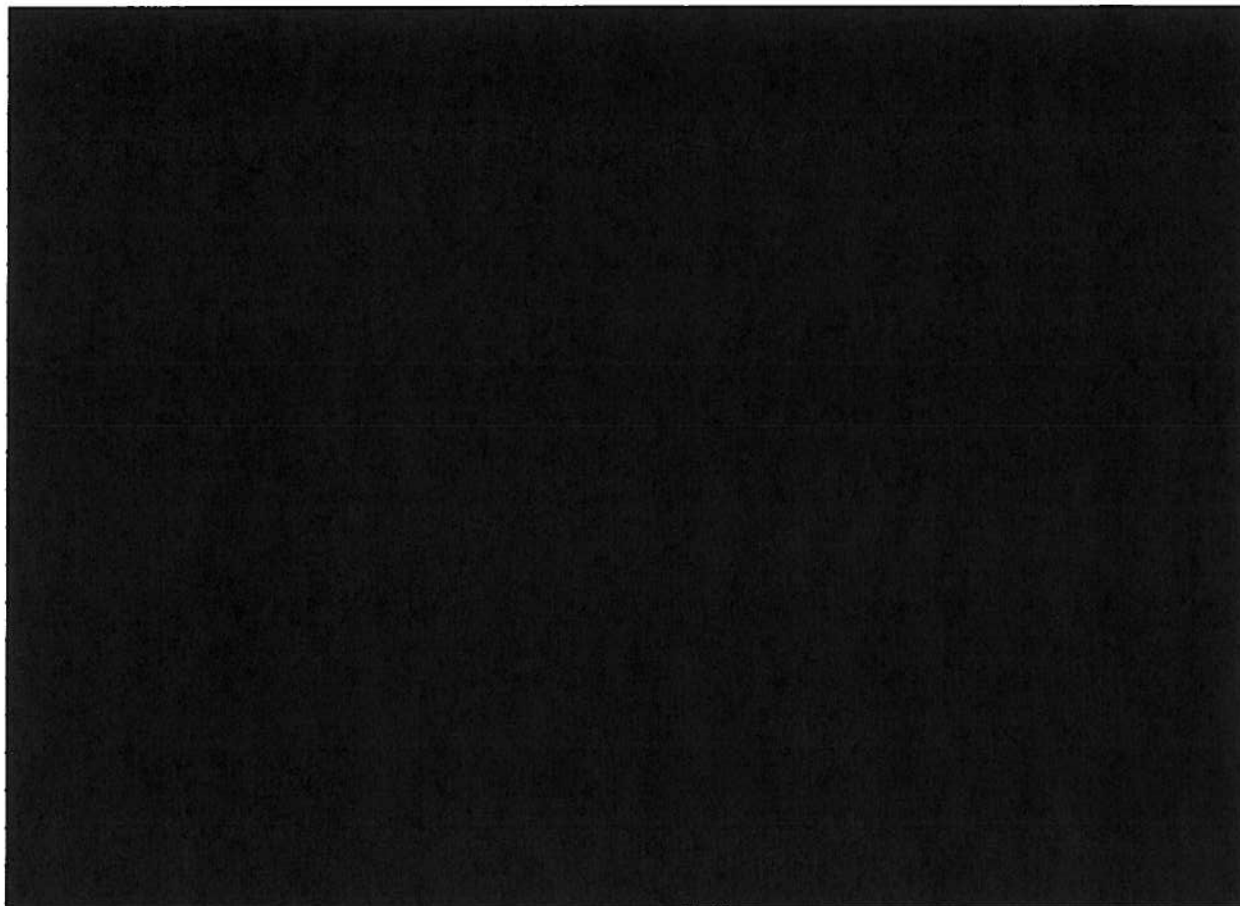
³⁸ At the March 2009 District Office Security Manager Conference, the 1-hour training in threat response was provided by an Assistant Chief and a Senior Inspector from the USMS Office of Protective Intelligence.

she said she was never contacted by the USMS. In fact, when a protective response was provided, it was provided by the Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF), where the AUSA's husband was employed as a Special Agent. Managers in the USMS district office said the USAO did not notify the USMS of the threat until 6 days after learning of it. A USMS manager said he felt "pretty okay" with ATF having provided a threat assessment and a residential security survey.

We also found in the same district that the USMS district office did not provide USAO building security staff with threat information that had been distributed to courthouse security staff, even though the courthouse and the USAO's building were adjacent and joined by a common hallway. At the time of our visit, the USMS district office was putting together points of contact for both the courthouse and the USAO building. USMS officials said they had no set policy for disseminating information to USAO building security staff about individuals who made threats. USAO staff told us the security personnel guarding that building had expressed frustration over not receiving notices about individuals who made threats.

There is no agreement or memorandum of understanding between the USMS and EOUSA, or between the USMS and any USAOs we visited, which addresses the sharing of information about threats against U.S. Attorneys and AUSAs or about protective responses. Figure 8 shows the lack of coordinated policy among the USMS, EOUSA, and the USAOs. While a USMS directive instructs district offices to provide information about protective investigations to the protectees involved, no policy directs USMS staff to provide information to the USAOs or EOUSA or to collect information about protective measures the USAOs or EOUSA implement.

**Figure 8: USMS and EOUSA Policy Regarding
the Protection of Threatened U.S. Attorneys and AUSAs**



Conclusion and Recommendations

EOUSA and USAOs have relatively few personnel performing personal security functions and, for the most part, they lack sufficient expertise in threat response and have limited training opportunities to prepare them to provide for the safety of U.S. Attorneys and AUSAs who have been threatened. In addition, USMS and USAO staff do not share key information and are not clear about their respective roles and responsibilities. Their efforts are not guided by formal protocols to help ensure there are no lapses in coverage and to avoid duplicative protective responses. To better prepare EOUSA and USAO personnel for responding to threats and to ensure better cooperation between the USMS and the USAOs, we recommend that:

10. EOUSA provide, in consultation with the USMS, sufficient training to EOUSA and USAO staff assigned threat response duties.
11. the USMS and EOUSA sign a memorandum of understanding that defines their roles and responsibilities in protecting U.S. Attorneys and AUSAs who receive threats.

EOUSA is not consistently notified of threats against U.S. Attorneys and AUSAs and often lacks important information about threats and protective responses.

Some USAOs failed to submit required Urgent Reports on threats to EOUSA.

We found that threats against USAO personnel are generally not reported to EOUSA. The USAOs' District Office Security Managers are required by the *U.S. Attorneys' Manual* to notify EOUSA by submitting an Urgent Report via e-mail of any threats made to USAO personnel.³⁹ However, we found that threats against USAO personnel are generally not reported to EOUSA. When we compared the threats reported by the USAOs and the USMS districts in FY 2007 and FY 2008, we found that USAOs had reported fewer than half the number of threats reported by the USMS (see Table 2).

Table 2: USMS District and USAO Reporting of Threats, FY 2007 and FY 2008

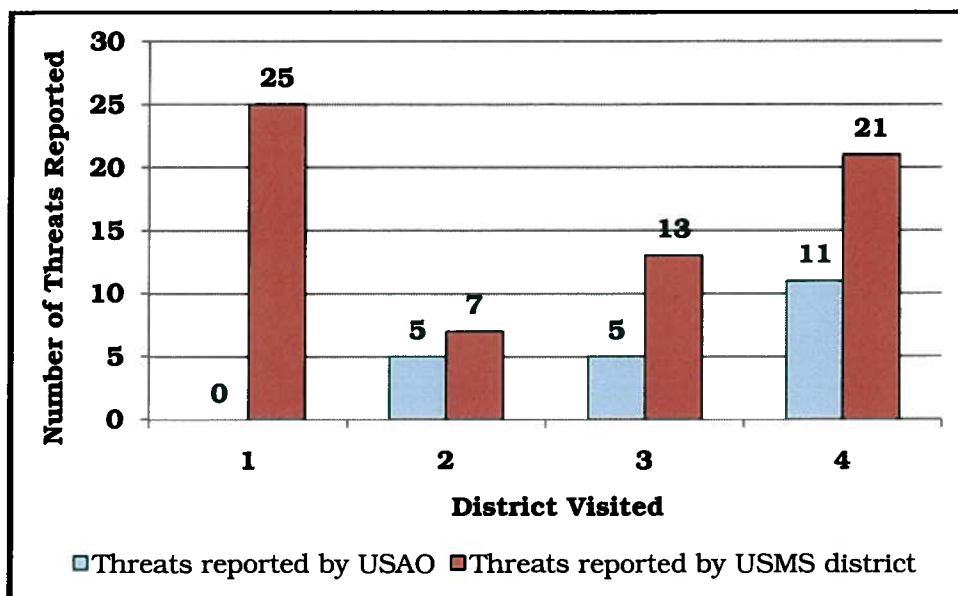
Component	In 67 districts, USMS reported more threats than USAOs	In 13 districts, USAOs reported more threats than USMS	In 14 districts, USMS and USAOs reported an equal number of threats	Total
	Number of threats reported			
USMS	402	14	8	424
USAO	129	28	8	165

Sources: USMS and EOUSA documents.

We also found that the USAOs in each of the four districts we visited sent fewer Urgent Reports to EOUSA than the number of threats recorded in the USMS threat database (Figure 9).

³⁹ *U.S. Attorneys' Manual*, Chapter 3-15.160.

Figure 9: Number of Threats Reported by USAO and the USMS in Visited Districts



Sources: USMS and EOUSA documents.

When we asked USAO employees in the four districts why they were not notifying EOUSA of threats, employees in three USAOs told us that they thought they had submitted all the required Urgent Reports. The District Office Security Manager for the fourth USAO (District 1 in Figure 9), which is one of the largest USAOs in the country, stated that EOUSA’s role in threat management was not clearly defined and that he did not rely on EOUSA for assistance in protecting threatened USAO employees. As a result, that USAO had not sent any Urgent Reports to EOUSA for the 25 threats against its personnel that we identified in the USMS threat database.

In addition, we found that EOUSA Security Programs Staff did not use the information in the threat management database to determine whether it was notified of all threats against USAO employees. In fact, the Security Programs Staff was unaware that some USAOs were not submitting Urgent Reports on all threats until we informed them of our findings.

EOUSA employees told us that they have taken steps to ensure that they are notified of threats reported to the USMS. In July 2008, EOUSA established a liaison with the USMS headquarters to share threat notifications. The EOUSA Threat Management Specialist told us she requests Urgent Reports from the USAOs when she learns from the USMS liaison of previously unreported threats. However, she stated that the

USAOs do not always respond to her requests. For example, we found that the USAOs had submitted only 5 Urgent Reports corresponding to the 50 threat notifications that the Threat Management Specialist had received from the USMS from July through September 2008.

Because the USAOs do not consistently notify EOUSA of threats made against USAO personnel, EOUSA does not have accurate information about the actual number or severity of all threats despite the notifications shared by the USMS liaison.⁴⁰ Unless EOUSA is aware of threats, it cannot fund protective measures, efficiently allocate resources, or assess the overall cost and performance of its security program.

Urgent Reports frequently lack relevant information needed for an effective response.

When we reviewed the 165 Urgent Reports that District Office Security Managers submitted to EOUSA in FY 2007 and FY 2008 for threats against USAO personnel, we found that 123 (75 percent) reports did not include key information, such as:

- the name and position of the targeted employee,
- the date the threat occurred,
- the date the Urgent Report was prepared, and⁴¹
- whether the USMS and FBI were notified.

All but 1 of the 165 reports included the targeted employee's name, but 73 (44 percent) failed to inform EOUSA whether the FBI had been notified of the threat, and 10 reports (6 percent) failed to indicate whether the USMS had been notified. Also, 46 reports (28 percent) failed to include the date the threat occurred, and 65 (39 percent) omitted the date the Urgent Report was prepared.

Because the Urgent Report template does not include these elements and the USAOs do not always include this information, EOUSA generally lacks initial threat information necessary to ensure the USMS and FBI have

⁴⁰ The USMS notification does not always include detailed information about the threat. Some notifications merely note that a threat has occurred against a specific attorney and provide no details.

⁴¹ The Urgent Report template does include a field for the date of the Urgent Report. That field is automatically updated with the current date each time the document is accessed rather than retaining the date the report was created.

been notified, to begin monitoring the response to the threat, and to determine the funding needed to provide protective measures to the threatened attorney.

EOUSA is not kept informed of actions taken to protect threatened U.S. Attorneys and AUSAs.

We also found that USAOs are not routinely informing EOUSA of the USMS's protective responses to mitigate threats and protect threatened AUSAs. We analyzed the Security Programs Staff threat management database and Urgent Reports submitted by District Office Security Managers and found few entries beyond the initial Urgent Reports about the threats. EOUSA personnel told us that they may receive updates via telephone, e-mails, or updated Urgent Reports. However, as of January 2009, the USAOs had submitted only 16 updates via Urgent Reports to the 165 initial Urgent Reports submitted to EOUSA during FY 2007 and FY 2008. We also found that EOUSA's Security Programs Staff did not always receive updated information from the USAOs on the progress of the protective measures provided by the USAO or the USMS, the initiation of an FBI investigation, or the progress of the FBI investigation. For example, in January 2008 an attorney who had been threatened by an inmate who was associated with the "Bloods" gang received protection from the USMS that included [REDACTED]. EOUSA's Security Programs Staff did not have a record of these protective measures.⁴²

Having complete information would enable EOUSA to better manage its security program by:

- coordinating the components' threat response actions,
- tracking trends in the types of threats against U.S. Attorneys and AUSAs,
- expanding USAO and District Office Security Manager training based on actual recent threats,
- better informing threatened U.S. Attorneys and AUSAs about the protective measures the USMS can provide to them,

⁴² EOUSA staff sometimes receives information on the response to threats through means other than Urgent Reports, such as e-mails, but in our review of the EOUSA database we saw only limited instances of this information being entered into the threat records of the database.

- guiding USAOs in improving proactive security and reacting more efficiently to threats, and
- basing procedures, such as residential security systems, deputations, and district security plans, on broad threat knowledge.

EOUSA's Security Programs Staff told us that they planned to improve the collection of information from USAOs. In June 2009, EOUSA informed us that it was designing a web-based Urgent Report program that would enable District Office Security Managers to submit their reports directly to the Security Programs Staff threat management database. The new web-based reporting system will be designed to provide a consistent method of communicating events to EOUSA. According to EOUSA, it will have the capability to track threats made against the AUSAs, identify the activities and protective measures provided, calculate the budget required for those protective measures, set automatic reminders that protective measures be reviewed to ensure they are still necessary, and develop aggregate reports about the number and type of events that have occurred. Also, according to the Assistant Director of the Security Programs Staff, the web-based forms will include names, dates, and protective measures provided and the automated database will track data from the reports of threats and other incidents. EOUSA expected to begin using the web-based Urgent Report program in December 2009 or January 2010. The OIG believes that specifying these data elements in the template will help EOUSA ensure receipt of consistent information from the USAOs.

Conclusion and Recommendations

The USAOs do not consistently notify EOUSA of threats made against USAO personnel or provide fundamental information EOUSA needs to monitor the District Office Security Managers' actions. Without knowing what protective measures the USMS and the USAOs intend to implement, EOUSA cannot assist in identifying additional security support. EOUSA also needs to be aware of USAO contact with the USMS and the FBI to fulfill its coordinating role. Without complete and current information on the response to threats, EOUSA is limited in its ability to track trends in threats against USAO personnel and the efforts to mitigate the threats.

We recommend that:

12. EOUSA provide guidance and periodic reminders to USAOs of the requirement to submit Urgent Reports immediately when a U.S. Attorney or AUSA is threatened.

13. EOUSA revise the Urgent Report template so that it includes a requirement to provide at least the following information:

- name and position of targeted employee;
- name and location of the person making the threat, if known;
- date the threat was made, or date the target was made aware of the threat;
- date the District Office Security Manager was informed of the threat;
- date the USMS and FBI were notified; and
- date the USAO submitted the Urgent Report to EOUSA.

14. EOUSA establish guidance to require the District Office Security Managers to send updated information via Urgent Reports at regular intervals to inform EOUSA of the status of USAO, USMS, and FBI actions to protect the threatened AUSA.

CONCLUSION AND RECOMMENDATIONS

The USMS threat response program has deficiencies in several critical areas that affect the USMS's ability to protect federal judges, U.S. Attorneys, and AUSAs from harm. Our review found that federal judges, U.S. Attorneys, and AUSAs are not consistently reporting threats on a timely basis, and in some instances are not reporting threats at all. When protectees do not report all threats, the USMS is unable to provide a comprehensive protective response.

However, once a threat has been reported, the USMS does not consistently use risk levels in assessing threats or provide at least the minimum required protective measures. Moreover, the USMS cannot verify that it has notified the FBI of all known threats against federal judicial officers.

The lack of coordination between the USMS and other law enforcement agencies also limits the USMS's ability to ensure the safety of its protectees. We found that coordination and communication between the USMS and the FBI regarding their respective investigations are inconsistent from district to district, and there are no formal or informal protocols for coordination. The USMS also is not coordinating effectively with local law enforcement agencies concerning notification of emergency responses to judges' residences, which prevents the USMS from obtaining information that might enable it to initiate a threat investigation and implement protective measures.

We also found that USAO personnel performing personal security functions did not have sufficient expertise and training to prepare them to provide for the safety of U.S. Attorneys and AUSAs who have been threatened. Moreover, USAO and USMS staff do not share key information and do not have clearly defined roles and responsibilities, which may result in lapses in, or duplicative, protective responses. Further, USAOs do not typically supply EOUSA with fundamental threat information, which prevents EOUSA from providing emergency security support or tracking trends in threats against USAO personnel.

As a result of our review, we make the following 14 recommendations.

To improve the understanding of federal judges, U.S. Attorneys, and AUSAs of the need for prompt reporting of threats and the consequences of delays or failure to report, we recommend that:

1. the USMS clearly explain to protectees the detrimental effect that delays or the failure to report has on the security provided.
2. the USMS update its security handbook to emphasize both the importance of immediately reporting threats to the USMS and the consequences of delays or failures to report.
3. EOUSA amend the *U.S. Attorneys' Manual* to clearly instruct the AUSAs that all threats must be reported promptly to the District Office Security Manager. Such instruction should include an explanation of the detrimental effect that delays or the failure to report has on the security provided.
4. the USMS review trends in reporting timeliness annually and provide the results of that analysis to the Administrative Office of the U.S. Courts and EOUSA for their use in judicial conferences and attorney training seminars.

To ensure that the USMS provides protectees with protective measures that are commensurate with the risk level of the threat, we recommend that:

5. the USMS implement controls to ensure that required risk assessments are completed and documented in the USMS threat database, including the assignment of risk levels, and that the protective measures provided in response to each threat also be documented in the USMS threat database.

To ensure that the USMS collects information that will enable it to monitor the performance of its judicial security program, and to ensure the USMS coordinates effectively with the FBI and local law enforcement agencies to keep the protectees safe, we recommend that the USMS:

6. establish internal controls at USMS headquarters to ensure that the USMS threat database contains full and accurate information, including ensuring that district offices regularly enter data in the "FBI Notified" and notification date fields.
7. coordinate with the FBI to establish a memorandum of understanding to formalize the coordination of protective and criminal investigations.
8. develop a mechanism to track the USMS district office responses to emergency notifications from local law enforcement agencies regarding emergency responses to federal judges' residences.
9. ensure that all districts send the required notification letters to local law enforcement agencies and that the letters contain a

working contact number that connects directly to the local USMS duty officer.

To better prepare EOUSA and USAO personnel for responding to threats and to ensure better cooperation between the USMS and the USAOs, we recommend that:

10. EOUSA provide, in consultation with the USMS, sufficient training to EOUSA and USAO staff assigned threat response duties.
11. the USMS and EOUSA sign a memorandum of understanding that defines their roles and responsibilities in protecting U.S. Attorneys and AUSAs who receive threats.

To ensure that EOUSA receives more complete and timely information to manage its threat response program and ensure the safety of the U.S. Attorneys and AUSAs, we recommend that:

12. EOUSA provide guidance and periodic reminders to USAOs of the requirement to submit Urgent Reports immediately when a U.S. Attorney or AUSA is threatened.
13. EOUSA revise the Urgent Report template so that it includes a requirement to provide at least the following information:
 - name and position of targeted employee;
 - name and location of the person making the threat, if known;
 - date the threat was made, or date the target was made aware of the threat;
 - date the District Office Security Manager was informed of the threat;
 - date the USMS and FBI were notified; and
 - date the USAO submitted the Urgent Report to EOUSA.
14. EOUSA establish guidance to require the District Office Security Managers to send updated information via Urgent Reports at regular intervals to inform EOUSA of the status of USAO, USMS, and FBI actions to protect the threatened AUSA.

APPENDIX I: PREVIOUS OIG REPORTS ON THE JUDICIAL SECURITY PROCESS

In March 2004, the Office of the Inspector General (OIG) reported on the USMS's efforts since September 11, 2001, to improve its protection of the federal judiciary.⁴³ We focused specifically on the USMS's ability to assess threats and determine appropriate measures to protect members of the federal judiciary during high-threat trials and while they are away from the courthouse.

We found that since September 11, 2001, the USMS had placed greater emphasis on judicial security by hiring 106 Court Security Inspectors and increasing courthouse security. However, the USMS's assessments of threats against members of the federal judiciary were often untimely and of questionable validity. Further, the USMS had limited capability to collect and share intelligence from USMS districts, the FBI's Joint Terrorism Task Forces (JTTF), and other sources on potential threats to the judiciary. In addition, the USMS lacked adequate standards for determining the appropriate protective measures that should be applied to protect the judiciary against identified potential risks (risk-based standards) during high-threat trials and when they are away from the courthouse.

The USMS concurred with all six of the recommendations in that report and during the next 2 years reported to the OIG the steps it had taken to implement them. The USMS stated that it had revised its established time frames for assessing threats; updated the historical threat database; increased the number of liaisons with other law enforcement and intelligence agencies and requested additional resources to increase representation on the JTTFs; established an Office of Protective Intelligence; increased the number of Top Secret security clearances and the amount of secure communications equipment in the districts; and issued revised judicial security directives that included risk-based standards and after action reports. The OIG has closed all of the recommendations.

In September 2007, the OIG released a follow-up to its March 2004 report examining the USMS's assessment of reported threats made against federal judges or other USMS protectees; the development of a protective intelligence capability to identify potential threats; and recent measures the

⁴³ Department of Justice, Office of the Inspector General, *Review of the United States Marshals Service Judicial Security Process*, Evaluation and Inspections Report I-2004-004, March 2004.

USMS had taken to improve judicial security and to enhance its capability to respond to judicial security incidents.⁴⁴

The OIG found that USMS efforts to improve its capabilities to assess reported threats and identify potential threats languished from the issuance of the March 2004 report to early 2007. We found that threat assessments took longer to complete, resulting in a backlog of 1,190 "pending" threat assessments as of October 1, 2006. Further, the USMS did not implement an effective program to develop protective intelligence that identified potential threats against the judiciary.

To improve the USMS's capacity to protect the federal judiciary, the OIG made six new recommendations. Since September 2007, the USMS has reported to the OIG the steps it has taken to implement them. For example, the USMS developed plans to improve its threat assessment process and for implementing a protective intelligence function to identify potential threats, including objectives, tasks, milestones, and resources. The USMS created a *Guide for Office of Protective Intelligence Personnel to Coordinate Protective Investigations*, which describes a comprehensive strategy for handling protective investigations and is in the process of modifying its inappropriate communication Threat Module of the Justice Detainee Information System (JDIS) to produce more user-friendly reports. Also, the USMS is finalizing policies for Technical Operations Group support concerning protective operations and investigations for Judicial Security Rapid Deployment Teams. The OIG has closed four of the six recommendations.

⁴⁴ Department of Justice, Office of the Inspector General, *Review of the United States Marshals Service Judicial Security Process*, Evaluation and Inspections Report I-2007-0104, September 2007.

APPENDIX II: METHODOLOGY OF THE OIG REVIEW

The methodology used in this review included interviews with USMS, EOUSA, and FBI personnel, as well as site visits to four federal judicial districts where we interviewed federal judges, USMS personnel, AUSAs, and other USAO personnel. In addition, we conducted a survey of a stratified random sample of AUSAs and performed document reviews and database analyses.

Interviews at USMS Headquarters and EOUSA

To determine the role and responsibilities of the USMS and the role of EOUSA in the protection of federal judges, U.S. Attorneys, and AUSAs, we interviewed 10 individuals: 4 from USMS headquarters at the Judicial Security Division and 6 from EOUSA. At USMS headquarters, we interviewed the Chiefs of the Office of Protective Operations, the Office of Protective Investigations, the Office of Court Security, and the Threat Management Center. At EOUSA, we interviewed the Director of EOUSA, the Chief of the Security Programs Staff, a Threat Management Specialist, a Physical Security Specialist, a Program Assistant for the Mission Assurance Team, and a Program Assistant for Physical Security.

Site Visits

We conducted site visits at four judicial districts. We chose the districts based on the number and severity of threats received by federal judges, U.S. Attorneys, and AUSAs in the districts, the number of prosecutors in the districts, and geographic location.

During these site visits, we conducted interviews and reviewed documents at four USAOs and four USMS district offices. At each USAO, we interviewed the U.S. Attorney, the Regional Security Specialist, the District Office Security Manager, and four AUSAs. At each USMS district office, we interviewed the U.S. Marshal, the Judicial Security Inspector, and at least one District Threat Investigator. We also interviewed at least two federal judges in each district to determine their experiences with protective measures provided after the judge received a threat. At three of the sites, we interviewed the judge who served as the Chair of the Court Security Committee for that district.

At each site, we also interviewed an FBI Special Agent who performed criminal investigations of threats against federal judges and AUSAs to

determine how the FBI and USMS coordinate their simultaneous investigations. In total, we interviewed 60 individuals in the field. When we report the percentage of site visit interviewees who held a particular opinion in our findings sections, we based the percentage on the number of people who answered a specific question on that topic instead of on the total number of interviewees.

Survey

We conducted a web-based survey of a stratified random sample of U.S. Attorneys and AUSAs to assess how they perceived the extent of the security provided to them in response to the threats they received. We also sought to determine what security measures were provided in response to threats received, as well as what security training was provided by the USMS and their respective USAOs. Using demographic data supplied by EOUSA about current AUSAs, we assigned the attorneys to different subsets and selected a random sample within each subset. The subsets were defined by three demographic factors: gender, length of service as a federal prosecutor, and the number of personnel working at the USAO.

We sent an invitation to participate in the web-based survey to the 688 U.S. Attorneys and AUSAs. We received 383 responses, a 56-percent response rate.

Some survey questions required respondents to select from pre-determined responses, while other questions allowed respondents to respond in their own words. In choosing the respondents' comments included in the body of this report, we selected those that were the most representative of the opinions expressed by the respondents.

Appendix III contains a copy of the survey and the results.

Document and Database Review

To determine the role and responsibilities of the USMS headquarters and the district offices in the protection of federal judges, U.S. Attorneys, and AUSAs and the response to threats received by those individuals, we reviewed the USMS's mission, directives, policies, and manuals; performance measures; budget documents; federal laws; and threat data from the Threat Management Center.

To determine the number and types of threats received by federal judges, U.S. Attorneys, and AUSAs in various districts, we reviewed USM-11

Report of Investigation forms and USM-550 Preliminary Threat Report forms from the USMS Threat Management Center database.⁴⁵ We also used the database to assist in determining:

- the sites to visit based on the number and severity of threats per district;
- the federal judges, U.S. Attorneys, and AUSAs to interview regarding their experiences in receiving threats;
- the average time for the USMS to respond to a threat;
- the risk levels assessed to each threat by the USMS; and
- the protective measures that were provided to threatened federal judges and AUSAs in response to various threats.

To examine the role and responsibilities of EOUSA in the protection of U.S. Attorneys and AUSAs, we reviewed EOUSA's mission, policies, procedures and manuals; training materials; budgets for protective measures; Urgent Reports submitted by the USAOs when a threat was received; and the EOUSA threat database.

To determine the role of the USAOs in the protection of U.S. Attorneys and AUSAs, we reviewed office security plans; Urgent Reports generated when a threat was received by an attorney; security training materials; position descriptions for security-related positions; and budget requests pertaining to security for each of the four districts we visited.

⁴⁵ USM-11s and USM-550s contain a summary of the threat event, information on the suspect, and a report of investigation containing a synopsis of the protective investigation.

APPENDIX III: RESULTS OF OIG SURVEY OF U.S. ATTORNEYS AND ASSISTANT U.S. ATTORNEYS

We conducted a web-based survey of a stratified random sample of U.S. Attorneys and Assistant U.S. Attorneys (AUSA) to assess how they perceived the extent of the security provided to them in response to the threats they received. We sent invitations to participate in the web-based survey to the 688 members of the chosen sample. Three hundred eighty-three attorneys in 30 districts responded to the survey.

Note: When percentages do not add to 100, it is because of rounding.

Background Questions

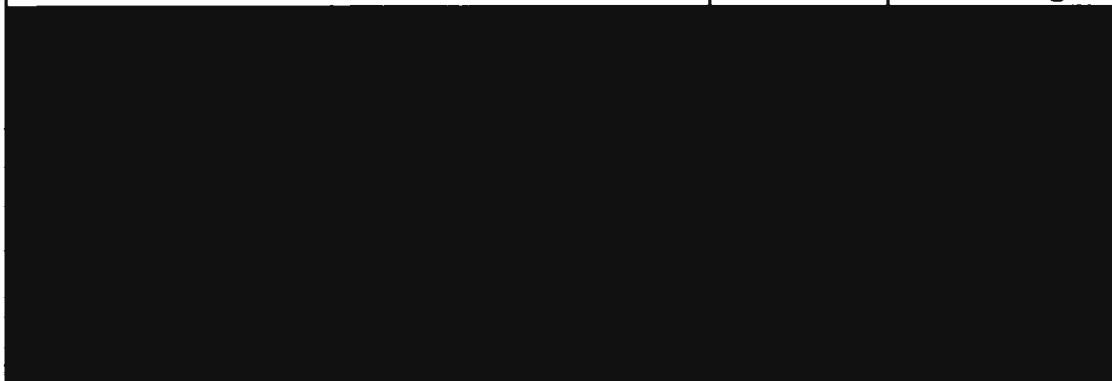
- 1) Are you a U.S. Attorney or an AUSA?

Attorney Type	Number	Percentage
U.S. Attorney	8	2%
AUSA	375	98%
Total	383	100%

- 2) Are you male or female?

Gender	Number	Percentage
Female	139	36%
Male	244	64%
Total	383	100%

- 3) What district do you work in?

District	Number	Percentage
		

District	Number	Percentage
Total	383	100%

4) How many attorneys are in your district office?

Attorneys Per Office	Number	Percentage
1-29	79	21%
30-99	132	35%
100+	172	45%
Total	383	100%

5) Since January 1, 2006, what type of matters do you primarily handle?

Matter Type	Number	Percentage
Civil	75	20%
Criminal	308	80%
Total	383	100%

- 6) How many years' experience do you have as an AUSA or U.S. Attorney?
(Include all the years you worked at any USAO as an attorney.)

Years' Experience	Number	Percentage
Less than 1 year	45	12%
1 to 3 years	49	13%
4 to 9 years	73	19%
10 to 14 years	83	22%
15+ years	133	35%
Total	383	100%

- 7) What type of case do you believe poses the greatest risk of receiving threats?

Case Type	Number	Percentage
Drugs	100	26%
Gangs	171	45%
Pro se (criminal defendant)	24	6%
Pro se (civil party)	33	9%
Public corruption	2	1%
Terrorism	13	3%
Tax (civil)	5	1%
Tax (criminal)	10	3%
Other	25	7%
Total	383	100%

Twenty-five respondents chose "Other" and provided answers in their own words. The OIG categorized information within their answers as follows:

Category	Number of Responses
All criminal cases	1
Any type of case	1
Civil rights	1
Depends on defendant	2
Firearms	3
Foreclosures/collections	1
Forfeiture	2
Fraud	2
Gangs & drugs	1

Category	Number of Responses
Irate family members	1
Judgment debtors	1
Liberty & property	1
Organized crime	3
Violent crime	1
White collar	2
Don't know	2
Total	25

N=25

N represents the number of respondents.

- 8) If you answered "Other" to the previous question, please specify whether the case was civil or criminal.

Civil or Criminal Case	Number of Responses
Criminal	19
Civil	2
Civil & criminal	1
Respondent answered forfeiture but did not classify the cases as civil or criminal	1
Respondent answered risk was not case-related but rather was dependent on the defendant's tendency toward violence and mental history	1
Respondent answered that he did not know what type of case posed the greatest risk, but then also answered criminal when asked to specify a civil or criminal case	1
Total	25

N=25

- 9) Do you know what procedures to follow in the event you, or a family member, receive a work-related threat?

Yes/No	Number	Percentage
Yes	308	80.4%
No	74	19.3%
No answer	1	0.3%
Total	383	100%

- 10) Have you, or an immediate family member, personally received a threat since January 2006 related to your employment at the USAO? (Please answer “yes” to this question only if you believe the threat was related to your employment at the USAO.)

Yes/No	Number	Percentage
Yes	61	16%
No	322	84%
Total	383	100%

- 11) If you answered “Yes” to the previous question, please specify how many threats you received since January 2006.

Number of threats	Number of responses
One threat	37
Two threats	11
Three threats	6
More than three threats	1
Total	55

N=55

Only 55 of 61 respondents who reported receiving threats in Question 10 answered this question.

One of the 55 respondents to this question reported receiving over 1,000 threats.

- 12) What types of work-related threats have you received? (Check all that apply.)

Threat Type	Number Of Responses
E-mail	3
Face-to-face	15
Letter	12
Telephone call	12
Other	29
Total	71

Respondents could select more than one response.

Twenty-nine respondents chose “Other” and provided answers in their own words. The OIG categorized information within their answers as follows:

Origin of Threat	Number of Responses
Third party (e.g., informant)	18
Person followed family member	1
Written threat	4
Discovered by investigators	1
Physical attack	2
Reported	1
Inappropriate contact with defendant's significant other	1
Alleged contract hit	1
Total	29

N=29

- 13) For any threats that you or an immediate family member received since January 2006, was the threat related to a specific case to which you were assigned?

Yes/No	Number	Percentage
Yes	51	84%
No	8	13%
Don't know	2	3%
Total	61	100%

- 14) Please specify the type of case to which you were assigned. (Check all that apply.)

Case Type	Number of Responses
Drugs	15
Gangs	9
Pro se (criminal defendant)	2
Pro se (civil defendant)	3
Public corruption	2
Terrorism	1
Tax (civil)	1
Tax (criminal)	1
Other	25
Total	59

N=51

Respondents could select more than one response.

Twenty-five respondents chose "Other" and provided answers in their own words. The OIG categorized information within their answers as follows:

Case Type	Number of Responses
Armed bank robbery	1
Assault/civil rights	1
Child exploitation	1
Civil rights violation	2
Collection	1
Drugs & gangs	1
Espionage & violent crime	1
Extortion	1
Felon in possession	2
Firearms	1
Firearms & child pornography	1
Foreign request for assistance	1
Fraud	1
Identity theft	1
Immigration	1
Postal	1
Project safe neighborhoods	1
Stalking	1
Violent crime	2
White collar	2
Total	24

N=25

One respondent answered with a number, not a case type.

- 15) If you answered “Other” to the previous question, please specify whether the case was civil or criminal.

Civil/Criminal	Number of Responses
Civil	1
Criminal	20
Total	21

N=21

Only 21 of 25 respondents who reported handling an “Other” case type in Question 14 answered this question.

- 16) Have you reported any threat(s) made against you personally or against a member of your family during your time as a U.S. Attorney or AUSA since January 2006?

Yes/No	Number	Percentage
Yes	51	84%
No	10	16%
Total	61	100%

- 17) Of the times that you, or a member of your family, were threatened since January 2006, how often did you report those threats? (Select one.)

Threat Reported	Number	Percentage
Every time	47	92%
Most of the time - half or more than half of the times you were threatened	4	8%
Some of the time - less than half of the times you were threatened	0	0%
Never	0	0%
Total	51	100%

- 18) If you only reported the threats most of the time or some of the time, what was/were your reason(s) for not reporting a threat? (Check all that apply.)

Reason Not Reported	Number	Percentage
I did not think the threat posed a real danger	3	75%
I was not familiar with the reporting procedures	0	0%
Threat reporting procedures were too cumbersome or inconvenient	0	0%
I did not want additional protection	0	0%
I did not feel that the protection provided would be adequate based on previous experience with the protection that was provided	1	25%
Other (please specify)	0	0%
Total	4	100%

19) If you never reported any threat(s) you received, why not? (Check all that apply.)

See Question 17. All of the survey respondents stated that they reported threats they received all or most of the time.

20) Since January 2006, when you reported your threat(s), to whom, and how often, did you report them? (Check all that apply.)

Entity Reporting To	Frequency of Reporting Threats to Entity			
	All of the Time	Most of the Time	Some of the Time	Never
District Office Security Manager	32	4	-	15
Other USAO managers	42	2	-	7
USMS	31	-	3	17
FBI	19	2	2	28
State or local law enforcement	8	1	3	39
Other	-	-	1	-

Missing column values indicate that no respondents chose that answer. One respondent reported the threat to ATF.

21) Please explain why you reported your threat(s) to the entity(s) you checked.

Reason Reported to Entity	Number of Responses
Regulation	15
Supervisor/chain of command	7
Protection/safety of self and family	4
Third party government employee informed threatene	4
Reported to case agent	1
Described how the threats occurred	5
No answer	4
Miscellaneous	11
Total	51

N=51

22) Once your threat was reported, was a threat assessment done?

Yes/No	Number	Percentage
Yes	34	67%
No	4	8%
Don't know	13	25%
Total	51	100%

23) Were you given the results of the threat assessment?

Yes/No	Number	Percentage
Yes	24	71%
No	9	26%
Don't recall	1	3%
Total	34	100%

24) Please explain below why you believe that the threat assessment was or was not accurate or useful.

Category	Number of Responses
Threat was not serious	2
Threat was serious	4
Threateners were interviewed	2
Improved security	4
Useful	2
Accurate	3
USMS mitigated threat	2
Home alarm provided	1
Not useful	2
Appropriate feedback	1
Total	23

N=22

Only 22 of 24 respondents who reported receiving the results of the threat assessment in Question 23 answered this question.

One respondent provided more than one response.

25) After you reported the threat(s), what was the longest response time for each of the following entities? (Check all that apply.)

Responding Entity	0-3 hours	3-12 hours	12-24 hours	1-3 days	Don't know
District Office Security Manager	22	5	0	2	22
Other USAO managers	33	5	0	2	11
USMS	22	3	4	5	17
FBI	9	2	1	3	36
State or local law enforcement	6	1	1	1	42
Other	2	0	0	1	0

N=51

Three respondents chose “Other” and provided answers in their own words. The OIG categorized information within their answers as follows:

Other Responding Entities	Number of Responses
ATF	2
Customs and Border Patrol	1
Federal authorities not involved	1
Total	4

N=4

One respondent did not answer “Other” in Question 25, but responded to this question.

26) If other entities who are not listed in Question 25 responded to your threat, please specify which entities responded and their longest response time.

Of the three respondents who indicated an entity, two reported that the ATF responded within zero to three hours and the other respondent reported that Customs and Border Patrol responded within one to three days.

27) Since January 2006, when you reported the threat(s) that you or your family received, were you afforded any protective measures?

Response	Number	Percentage
Never	29	57%
Some of the time	5	10%
Most of the time	2	4%
All of the time	15	30%
Total	51	100%

28) Since January 2006, when you reported the threat that you or your family received, what [REDACTED] were you or your family offered? (Check all that apply.)

Protective Measure	Not Offered	Offered But Declined	Offered And Accepted
[REDACTED]			
N=	[REDACTED]		

29) If you were offered [REDACTED] other than those listed above, please specify what those measures were and whether you accepted or declined them.

Other Protective Measures Offered	Number of Responses
[REDACTED]	[REDACTED]
Total	[REDACTED]

N= [REDACTED]

30) Please indicate whether the investigation(s) and the protective measures provided by the U.S. Marshals Service in response to the threat(s) were appropriate.

USMS Measures Appropriate	Number	Percentage
[REDACTED]	[REDACTED]	[REDACTED]
Total	[REDACTED]	[REDACTED]

31) Please explain why you believe that the investigation and protective measures provided by the U.S. Marshal Service were or were not appropriate.

Appropriateness of USMS Response	Number of Responses
[REDACTED]	[REDACTED]
Total	[REDACTED]

N= [REDACTED]

32) Please indicate whether the investigation(s) and the protective measures provided by the EOUSA in response to the threat(s) were appropriate.

EOUSA Measures Were Appropriate	Number	Percentage
Total		

33) Please explain why you believe that the investigation and protective measures provided by the EOUSA were or were not appropriate.

Reasons Why EOUSA Response Was or Was Not Appropriate	Number of Responses
Total	
N=	

34) If you believe any of the [REDACTED] in Question 28 or Question 29 needed improvement, please explain below.

Protective Measures That Need Improvement	Number of Responses
[REDACTED]	[REDACTED]
Total	[REDACTED]

N=[REDACTED]

35) If you did not receive protective measures in response to a threat and you believe that you should have, please explain below.

Reason Respondent Should Have Received Protective Measures	Number of Responses
[REDACTED]	[REDACTED]
Total	[REDACTED]

N=[REDACTED]

Daily Security Measures Provided

36) Where is your office located?

Location	Number	Percentage
[REDACTED]	[REDACTED]	[REDACTED]
Total	[REDACTED]	[REDACTED]

37) If your office is NOT in a federal courthouse or federal building, which of the following [REDACTED] are used for building security? (Check all that apply or check "don't know" if you are not familiar with the security measures used in your building.)

Non-Federal Facility

Building Security Feature	Number	Percentage (of 129)
[REDACTED]		

[REDACTED]

Non-Federal Facility

Additional Security Measures	Number of Responses
[REDACTED]	
Total	[REDACTED]

N= [REDACTED]

38) How useful do you find the following building security measures?
(Check N/A if you are not aware that your building has a particular measure)

Non-Federal Facility

Security Measures	Not Useful	Somewhat Useful	Neutral	Useful	Very Useful	N/A

N=

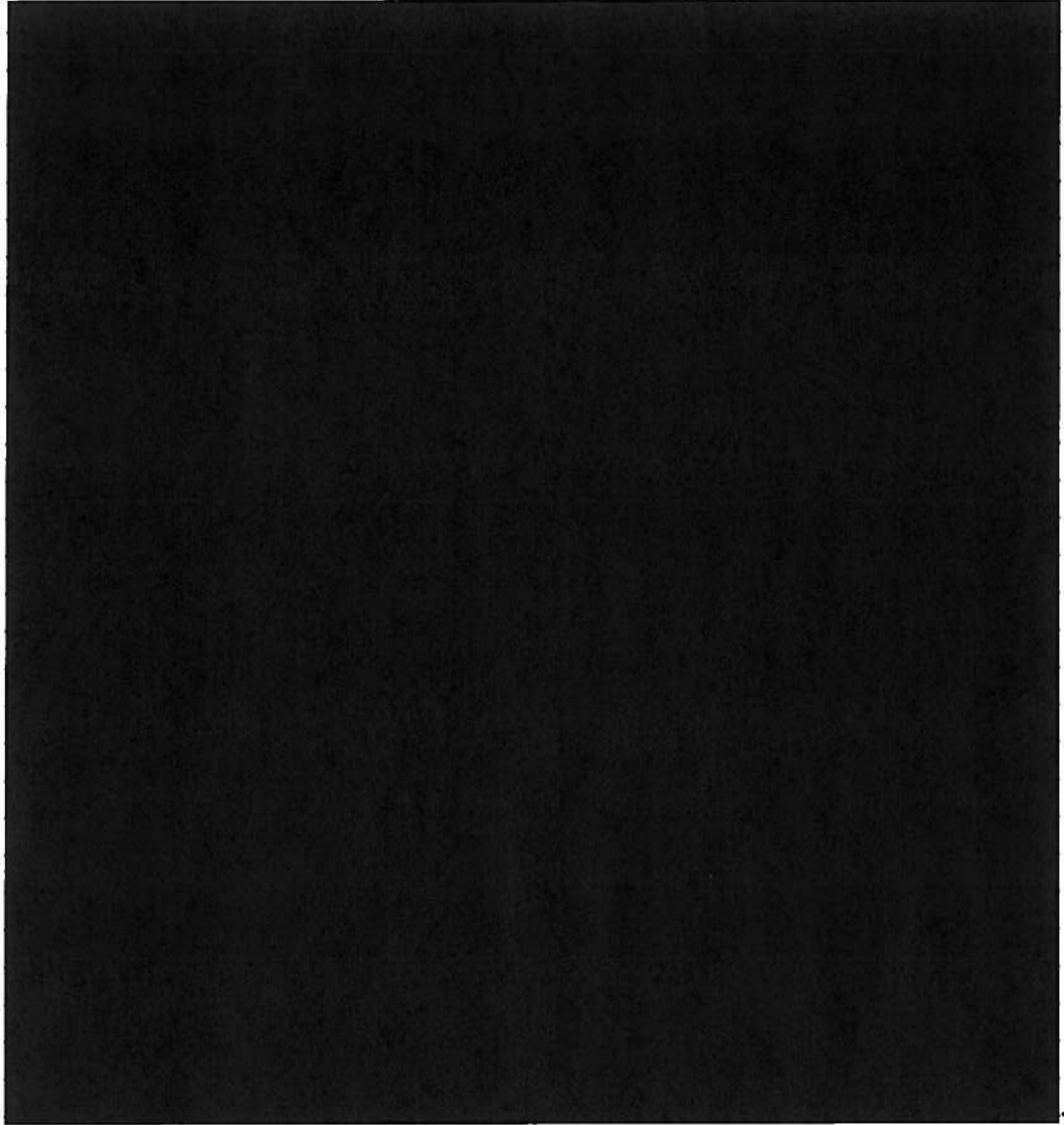
39) If you are aware of other building security measures not mentioned above, please specify what those measures are and whether you find them useful.

Non-Federal Facility

Other Building Security Measures	Not Useful	Somewhat Useful	Neutral	Useful	Very Useful	Did Not Specify Usefulness

N=

•



40) If you checked any of the building [REDACTED] in Question 38 as not useful, please explain.

Non-Federal Facility

Reasons Building Security Measures Are Not Useful	Number of Responses
[REDACTED]	
Total	

N=X

41) If your office IS in a federal courthouse or federal building, which of the following security measures are used for building security? (Check all that apply or check "don't know" if you are not familiar with the security measures used in your building.)

Federal Facility

Building Security Feature	Number	Percentage (of 254)
[REDACTED]		

[REDACTED]

Federal Facility

Other Security Measures	Number of Responses
Total	
N=	

42) How useful do you find the following building [REDACTED]? (Check N/A if you are not aware that your building has a particular measure)

Federal Facility

Security Feature	Not Useful	Somewhat Useful	Neutral	Useful	Very Useful	N/A

43) If you are aware of other building [REDACTED] not mentioned above, please specify what those measures are and whether you found them useful.

Federal Facility

Other Building Security Measures	Not Useful	Somewhat Useful	Neutral	Useful	Very Useful	Did Not Specify Usefulness
[REDACTED]						

N= [REDACTED]

44) If you checked any of the building security measures in Question 42 as not useful, please explain.

Federal Facility

Reasons Building Security Measures Are Not Useful	Number of Responses
[REDACTED]	
Total	[REDACTED]

N= [REDACTED]

45) Are there any other [REDACTED] you believe should be taken in terms of building security? Please explain below.

Needed Building Security Measures	Number of Responses
[REDACTED]	
Total	
N=	[REDACTED]

46) Does your office provide parking?

Location of Parking	Number of Responses
[REDACTED]	
N=	[REDACTED]

47) What features does the parking facility have? (Check all that apply.)

Parking Security Features	Number of Responses
[REDACTED]	
N=	[REDACTED]

[REDACTED] and provided answers in their own words. The OIG categorized information within their answers as follows:

Other Parking Security Measures	Number of Responses
[REDACTED]	
Total	[REDACTED]
N= [REDACTED]	

48) If you think the security of your office's parking facility needs improvement, please explain below.

Needed Parking Improvements	Number of Responses
[REDACTED]	
Total	[REDACTED]
N= [REDACTED]	

49) Are there any other [REDACTED] you believe should be taken in terms of parking facility security? Please explain below.

Additional Parking Measures Needed	Number of Responses
[REDACTED]	
Total	[REDACTED]
N= [REDACTED]	

50) Do you have a [REDACTED]?

[REDACTED]	Number	Percentage
[REDACTED]		
Total	[REDACTED]	[REDACTED]

51) Do you believe that [REDACTED] should be offered as a routine protective measure?

Yes/No	Number	Percentage
[REDACTED]		
Total	[REDACTED]	[REDACTED]

52) Please explain why you believe that [REDACTED] should or should not be offered as a routine protective measure.

[REDACTED]

Reasons [REDACTED] Should Be a Routine Protective Measure	Number of Responses
[REDACTED]	[REDACTED]
Total	[REDACTED]

Reasons [REDACTED] Should Not Be a Routine Protective Measure	Number of Responses
[REDACTED]	[REDACTED]
Total	[REDACTED]

Security Training

53) Have you received personal security training at the USAO (either in person, by PowerPoint presentation, or other means)?

Security Training	Number	Percentage
Received security training	291	76%
Did not receive security training	55	14%
Don't recall if received security training	37	10%
Total	383	100%

54) How long after you were initially employed at the USAO did you receive the security training (either in person or by other means)?

Elapsed Time From Initial Employment to Security Training	Number	Percentage
Within the first month	71	24%
Within the first 3 months	6	2%
Within the first 6 months	19	7%
Within the first year	26	9%
Sometime after the first year of employment	53	18%
Don't remember when training received	116	40%
Total	291	100%

55) As part of your initial security training, did you receive instructions to follow if you receive a threat?

Yes/No	Number	Percentage
Yes	220	76%
No	12	4%
Don't know	59	20%
Total	291	100%

56) Have you received subsequent personal security training as a refresher (either in person, by PowerPoint presentation, or by other means)?

Yes/No	Number	Percentage
Yes	217	75%
No	47	16%
Don't know	27	9%
Total	291	100%

57) Did your security training address any of the following topics? (Check all that apply.)

Security Training Topic	Number of Responses	Percentage (out of 291)
Home security	122	42%
Work-related travel	195	67%
Driving	124	43%
Commuting	128	44%
Emergency contact numbers	199	83%
Other	21	7%
None of the above	41	14%

N=291

Twenty-one respondents chose 'Other' and provided answers in their own words. The OIG categorized information within their answers as follows:

Other Topics Covered in Security Training	Number of Responses
Courtroom security	3
Additional aspects of work-related travel	1
Threats	2
Don't recall	7
Total	23

N=21

Some respondents provided more than one response.

58) How useful did you find the security training provided in the following areas? (Check "N/A" if you did not receive training in an area.)

Security Topic	Not Useful	Somewhat Useful	Neutral	Useful	Very Useful	N/A
Home security	15	19	24	73	19	141
Work-related traveling	16	28	29	107	27	84
Driving	12	22	24	76	19	138
Commuting	13	26	25	69	17	141
24-hour emergency contact numbers	7	16	22	108	72	66
Initial security briefing	10	25	32	119	37	68
Subsequent refresher training	10	20	34	104	36	87
Training on threat procedures	6	25	32	124	38	66

N=291

59) If you think any of the security training or briefings provided in your office need improvement, please explain below.

Security Topics That Need Improvement	Number of Responses
Residential and commuting topics	18
Refresher training	11
Overall training content	14
Parking information	3
Preventing and deterring threats	1
Miscellaneous	8
Total	56

N=54

Some respondents provided more than one response.

60) Are there any other measures you believe the training should address in terms of personal safety? Please explain below.

Additional Training Needed	Number of Responses
[REDACTED]	
Total	

N= [REDACTED]

61) Does the District Office Security Manager make websites, brochures, or videotapes on security topics easily available to you?

Yes/No	Number	Percentage
Yes	136	36%
No	68	18%
Don't know	179	47%
Total	383	100%

62) Do you find these websites, brochures, or videotapes on security topics useful?

Usefulness of Websites, Brochures, or Videotapes	Number	Percentage
Not useful	6	4%
Somewhat useful	22	16%
Neutral	43	32%
Useful	57	42%
Very useful	8	6%
Total	136	100%

63) Please explain below why you find these resources to be useful or not useful.

Reasons Resources Are or Are Not Useful	Number of Responses
Information is too general in nature	7
Information is useful and relevant	8
DOSM provides current security information to the USAO	4
Information is a good refresher	4
Comments discuss topics covered in the training	3
Have not reviewed the materials	2
Materials not always consulted	2
Useful once received training as a U.S. Attorney	1
Have to request materials in order to review them	1
Too much information provided	1
Total	33

N=30

Some respondents provided more than one response.

**APPENDIX IV: THE UNITED STATES MARSHALS SERVICE'S
RESPONSE**

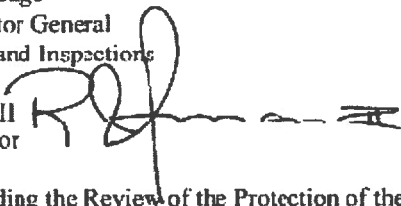


U.S. Department of Justice
United States Marshals Service
Operations Directorate

Alexandria, Virginia 22301-1625

December 16, 2009

MEMORANDUM TO: Michael D. Gulledge
Assistant Inspector General
for Evaluation and Inspections

FROM: Robert J. Finan, II 
Associate Director

SUBJECT: Response Regarding the Review of the Protection of the Judiciary
and the United States Attorneys, Assignment Number A-2008-006

This is in response to your correspondence seeking comment on the draft subject report. Attached please find the USMS response to the applicable recommendations.

Should you have any questions, please contact Ms. Isabel Howell, Audit Liaison, at 202-307-9744.

Attachment

cc: Isabel Howell
External Audit Liaison
United States Marshals Service

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

USMS Response to Draft Recommendations

Recommendation 1) The USMS clearly explain to protectees the detrimental effect that delays or the failure to report has on the security provided.

Response: Concur

The USMS constantly interacts with protectees and emphasizes the need for immediate reporting of threats, inappropriate communications, and other security issues. The USMS also emphasizes to its employees the importance of communication with, and support of, federal prosecutors who receive inappropriate communications and/or threats. Specifically, Protective Intelligence Investigators (PIIs), District Threat Investigators (DTIs), and Judicial Security Inspectors (JSIs) receive training that explains the role of the District Office Security Manager (DOSM) within the United States Attorneys Office (USAO), and further emphasizes the significance of maintaining a close working relationship with the DOSM. The USMS also regularly provides training to the court family, to include USAO, on issues that include off-site security, personal security, and timely threat reporting. These training sessions utilize a number of resources, including USMS Publication 94, *Off-Site Security for Judges, United States Attorneys, and Their Families*, USMS Publication 6, *Personal Security Handbook*, and a Department of Justice, National Institute of Justice (DOJ/NIJ) publication, *Protective Intelligence and Threat Assessment Investigations*.

Through coordination with the Administrative Office of the United States Courts (AOUSC), the USMS also provides security presentations during Judicial Nominee Briefings and New Chief Judge Orientations. During these presentations, the USMS stresses security issues and provides copies of USMS Publications 6 and 94. When Judges update Form USM 50, *Judicial Personnel Profile*, the USMS emphasizes the importance of reporting threats and inappropriate communications. The USMS has also begun emphasizing the importance of threat reporting through presentations at magistrate judges conferences, judicial conferences, and at Judicial Security Committee meetings.

The USMS will continue to emphasize the need for immediate reporting of threats, inappropriate communications, and security issues whenever an opportunity arises.

Recommendation 2) The USMS update its security handbook to emphasize both the importance of immediately reporting threats to the USMS and the consequences of delays or failures to report.

Response: Concur

USMS Publication 94 is widely distributed both to the Judiciary and USAOs. Publication 94 was last edited and updated for distribution in December 2008. The USMS is currently collecting information to make necessary edits for a future edition. Future revisions to Publication 94 will include verbiage emphasizing the importance of immediately reporting threats and inappropriate communications to the USMS, as well as the consequences of delaying or failing to report these issues.

Recommendation 3) EOUSA

Recommendation 4) The USMS review trends in reporting timeliness annually and provide results of that analysis to the Administrative Office of the U.S. Courts (AOUSC) and the EOUSA for their use in judicial conferences and attorney conferences.

Response: Concur

The USMS will review trends in reporting timeliness annually and provide results of that analysis to AOUSC and EOUSA for use in judicial and attorney conferences.

Recommendation 5) The USMS implement controls to ensure that required risk assessments are completed and documented in the USMS threat database, including the assignment of risk levels, and that the protective measures provided in response to each threat also be documented in the USMS threat database.

Response: Concur

The USMS conducts protective investigations using the behavior based approach to assess the threat and assign a risk level. DTIs/PIIs in the field notify the USMS Threat Management Center (TMC) and receive support in the form of recommendations and analysis. For low and potential risk cases, the case is designated as "standard." For high risk cases, the DTIs/PIIs assign the priority rating of "expedite" to the Form USM 550, *Preliminary Threat Report* to identify the urgency for analysis. As the protective investigation progresses, the facts and behavior that are developed may change, and are documented on a Form USM-11, *Investigative Report*. Because the risk level changes during the investigation, either escalating or deescalating, no fixed risk level is entered into the Justice Detainee Information System (JDIS).

The District Judicial Security Inspector (JSI) is responsible for recommending and coordinating the protective response. The JSI and the DTI/PII then consult with district management to identify the appropriate protective measures and the protective response. The JSI frequently coordinates the protective response with USMS Headquarters.

As a result of this process, risk levels are communicated between the DTI/PII, the JSI, and district management so that protective responses help ensure the safety of our protectees. Unfortunately there is no way to quantify how many attacks have been prevented through this process.

The USMS is revising the *Guide to Protective Investigations and Contemporary Threat Management*, a working guide and instruction manual for DTIs/PIIs that was last revised in 2008. The USMS is also revising its Policy Directive 10, *Judicial and Court Security*. This policy directive was last revised in 2006. Following these revisions, both documents will provide consistent instruction and guidance concerning risk assessments and the assignment of risk levels.

Recommendation 6) Establish internal controls at USMS Headquarters to ensure that the USMS database contains full and accurate information, including ensuring that district offices regularly enter data in the “FBI notified” and “Notification Date” fields.

Response: Concur

The USMS will strengthen existing internal controls at USMS Headquarters to ensure that the USMS database, the Justice Detainee Information System (JDIS), contains full and accurate information.

The USMS will adjust JDIS to reflect both notification of the FBI (date, location, and Special Agent) on a threat, as well as non-notification of the FBI when an inappropriate communication has been reported but does not rise to the level of prosecutorial investigation. The current database only allows the district to report when and where notification of the FBI was accomplished, and does not take into account the numerous cases that have no prosecutorial merit, including nuisance calls, repetitive pro se filing, inappropriate attraction, and others.

The current internal controls consist of personnel in the Threat Management Center (TMC) reviewing all cases as they are entered into JDIS by the district. Once the change discussed above is made in the JDIS database, the USMS will provide additional direction to the field, as well as additional training for TMC personnel, to ensure each case is thoroughly completed.

Per USMS Directive 10.3, *Protective Investigations*, all threats are inappropriate communications, but not all inappropriate communications are threats. In this review, the OIG used the term threat to encompass both threats and inappropriate communications, and did not differentiate between the two. Per USMS Directive 10.3, section E.l.c., “Report to Office of Protective Intelligence (OPI) Duty Desk: In the event of a threat or inappropriate communication, district managers will immediately report the situation to the OPI duty desk and the local office of the FBI (if the inappropriate communication contains a threat).”

Recommendation 7) Coordinate with the FBI to establish a memorandum of understanding to formalize the coordination of protective and criminal investigations.

Response: Concur

The USMS will consult with the FBI about establishing a memorandum of understanding to formalize the coordination of protective and criminal investigations.

Recommendation 8) Develop a mechanism to track the USMS district office responses to emergency notifications from local law enforcement agencies regarding emergency responses to federal judges’ residences.

Response: Concur

The USMS is developing a mechanism to track USMS district office responses to emergency notifications from local law enforcement agencies regarding emergency responses to federal judges' residences.

Recommendation 9) Ensure that all districts send the required notification letters to local law enforcement agencies and that the letters contain a working contact number that connects directly to the local USMS duty officer.

Response: Concur-in part

The USMS requires that all districts send notification letters to local law enforcement agencies. This is tracked within a USMS database that lists all federal judges. A new memorandum will be issued that clearly explains that the notification letters contain a working contact number that connects directly to the local USMS office. After business hours, the USMS answering service, which is often an area law enforcement agency, will contact the USMS Duty Officer. As USMS Duty Officers rotate frequently, it is impractical and unnecessary to have the number connect "directly to the local USMS duty officer" as they may be transferred, on vacation, or on leave.

It is believed that this finding of non-working numbers was primarily driven by the past issuance of a "working contact number that connects directly to the local USMS duty officer." The problem would continue if contact numbers were issued in this fashion, and we cannot support it.

The USMS agrees that it is critically important that the notification letter must list a working contact number for the local USMS office, and have connectivity to the local USMS Duty Officer at all times.

Recommendation 10) EOUSA

Recommendation 11) The USMS and EOUSA sign a MOU that defines their roles and responsibilities in protecting U.S. Attorneys and AUSAs who receive threats.

Response: Concur

The USMS will consult with EOUSA about establishing a memorandum of understanding that defines their roles and responsibilities in protecting United States Attorneys and Assistant United States Attorneys who receive threats.

Recommendation 12) EOUSA

Recommendation 13) EOUSA

Recommendation 14) EOUSA

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

The Office of the Inspector General provided a draft of this report to the United States Marshals Service (USMS) for its comment. The report contained 14 recommendations: Recommendations 1, 2, 4, and 5 through 9 are directed to the USMS. Recommendations 3, 10, 12, 13, and 14 are directed to the Executive Office for United States Attorneys (EOUSA). Recommendation 11 is directed to both the USMS and EOUSA.

The USMS's response is included in Appendix IV to this report. The OIG's analysis of the USMS's response and the actions necessary to close the recommendations are discussed below.

Recommendation 1. The USMS clearly explain to protectees the detrimental effect that delays or the failure to report has on the security provided.

Status. Resolved – open.

Summary of USMS Response. The USMS concurred with this recommendation. According to the USMS, it already emphasizes to protectees the need for immediate reporting of threats, inappropriate communications, and other security issues. The USMS stated that it regularly provides training to federal court officials, including United States Attorney's Office (USAO) staff, on issues that include off-site security, personal security, and timely threat reporting.

The USMS further stated in its response that through coordination with the Administrative Office of the U.S. Courts (AOUSC), it provides security presentations during Judicial Nominee Briefings and New Chief Judge Orientations. According to the USMS, it stresses security issues during these presentations and provides copies of USMS security publications. The USMS stated that when judges update their judicial personnel profiles, the USMS emphasizes the importance of reporting threats and inappropriate communications. According to the USMS, it has also begun emphasizing the importance of threat reporting through presentations at magistrate judges' conferences, judicial conferences, and Judicial Security Committee meetings. The USMS stated that it will continue to emphasize the need for immediate reporting of threats, inappropriate communications, and security issues whenever an opportunity arises.

OIG Analysis. The actions taken by the USMS are partially responsive to our recommendation. The USMS has described the training it provides to the judges, but did not mention training for attorneys. Please provide the OIG, by March 1, 2010, with copies of the security presentations from Judicial Nominee Briefings, New Chief Judge Orientations, magistrate judges' conferences, judicial conferences, and a sample of the presentations from the Judicial Security Committee meetings for fiscal year (FY) 2009. Also please provide a list of the training provided to the other federal court officials, including the attorneys, and copies of the training presentations.

Recommendation 2. The USMS update its security handbook to emphasize both the importance of immediately reporting threats to the USMS and the consequences of delays or failures to report.

Status. Resolved – open.

Summary of USMS Response. The USMS concurred with this recommendation and stated that it is currently collecting information to edit its security handbook, *Off Site Security for Judges, United States Attorneys and their Families*, which was last updated in December 2008. The USMS stated in its response that future revisions to this handbook will emphasize the importance of immediately reporting threats and inappropriate communications to the USMS, as well as the consequences of delaying or failing to report these incidents.

OIG Analysis. The actions proposed by the USMS are responsive to our recommendation. Please provide the OIG with an updated copy of the security handbook or a status report of the edits to the handbook by March 1, 2010.

Recommendation 4. The USMS review trends in reporting timeliness annually and provide the results of that analysis to the Administrative Office of the U.S. Courts and EOUSA for their use in judicial conferences and attorney training seminars.

Status. Resolved – open.

Summary of USMS Response. The USMS concurred with this recommendation. The USMS stated that it will review trends in reporting timeliness annually and provide the results of that analysis to AOUSC and EOUSA for use in judicial and attorney conferences.

OIG Analysis. The actions proposed by the USMS are responsive to our recommendation. Please provide the results of the analysis of the timeliness of threat reporting and the methods used to obtain the results by March 1, 2010.

Recommendation 5. The USMS implement controls to ensure that required risk assessments are completed and documented in the USMS threat database, including the assignment of risk levels, and that the protective measures provided in response to each threat also be documented in the USMS threat database.

Status. Resolved – open.

Summary of USMS response. The USMS concurred with this recommendation. However, the USMS stated that the risk level may change during the investigation and therefore no fixed risk level is entered into the threat database. According to the USMS, risk levels are communicated between the District Threat Investigator, the Protective Intelligence Investigator, the Judicial Security Inspector, and district management. The USMS is revising the *Guide to Protective Investigations and Contemporary Threat Management*, which is a working guide and instruction manual for District Threat Investigators and Protective Intelligence Investigators that was last revised in 2008. The USMS is also revising its Policy Directive 10, *Judicial and Court Security*, which was last revised in 2006. The USMS stated that following these revisions both documents will provide consistent instruction and guidance concerning risk assessments and the assignment of risk levels.

OIG Analysis. The intent of this recommendation was to ensure that the risk level and the protective measures are documented in the USMS threat database. If the risk level changes during the course of the threat response process, this change can be updated in the database. Without documentation of the risk level or the protective measures provided, the only way USMS headquarters can verify that the appropriate protective measures have been taken is to contact the districts and rely on the memory of district personnel.

In addition, in its response the USMS did not specify what instruction and guidance concerning risk assessments and the assignment of risk levels would be provided in the revision of the USMS directive and the instruction manual. Please provide a copy of the revised directive and instruction manual that shows that the risk level and protective measures provided are

to be documented in the USMS threat database or a status report on the progress of the revisions by March 1, 2010.

Recommendation 6. Establish internal controls at USMS headquarters to ensure that the USMS threat database contains full and accurate information, including ensuring that district offices regularly enter data in the “FBI Notified” and notification date fields.

Status. Resolved – open.

Summary of USMS Response. The USMS concurred with this recommendation and stated that it will strengthen existing internal controls at USMS headquarters to ensure that the threat database contains full and accurate information. The USMS will adjust the threat database to reflect both notification of the Federal Bureau of Investigation (FBI) of a threat, including the date, location, and Special Agent notified, as well as non-notification of the FBI when an inappropriate communication has been reported but does not rise to the level of a criminal investigation. Once the database is modified, the USMS will provide additional direction to the field, as well as additional training for headquarters personnel, to ensure each case is thoroughly completed.

OIG Analysis. The actions proposed by the USMS are responsive to our recommendation. Please provide, by March 1, 2010, a screen capture of the threat database showing the changes made to the database, showing notification of the FBI of a threat, including the date, location, and Special Agent notified, as well as non-notification of the FBI when an inappropriate communication has been reported but does not rise to the level of a criminal investigation. In addition, please provide the internal controls to be implemented to ensure that this data is recorded.

Recommendation 7. Coordinate with the FBI to establish a memorandum of understanding to formalize the coordination of protective and criminal investigations.

Status. Resolved – open.

Summary of USMS Response. The USMS concurred with the recommendation and stated that it will consult with the FBI about establishing a memorandum of understanding to formalize the coordination of protective and criminal investigations.

OIG Analysis. The action proposed by the USMS is responsive to our recommendation. Please provide a copy of the memorandum of understanding between the USMS and the FBI formalizing the coordination of protective and criminal investigations, or a status report of the progress in establishing the memorandum, by March 1, 2010.

Recommendation 8. Develop a mechanism to track the USMS district office responses to emergency notifications from local law enforcement agencies regarding emergency responses to federal judges' residences.

Status. Resolved – open.

Summary of USMS Response. The USMS concurred with our recommendation and stated that it is developing a mechanism to track USMS district office responses to emergency notifications from local law enforcement agencies.

OIG Analysis. The action proposed by the USMS is responsive to our recommendation. Please provide a description of the mechanism that the USMS will use to track its district office responses to emergency notifications from local law enforcement agencies, or a status report on the creation of this mechanism, by March 1, 2010.

Recommendation 9. Ensure that all districts send the required notification letters to local law enforcement agencies and that the letters contain a working contact number that connects directly to the local USMS duty officer.

Status. Resolved – open.

Summary of USMS Response. The USMS concurred in part with this recommendation. In its response, the USMS stated that it requires all districts to send notification letters to local law enforcement agencies and tracks in its database whether this notification is done. The USMS will issue a new memorandum that clearly explains that the notification letters are to contain a working contact number that connects directly to the local USMS office. After business hours, the USMS answering service, which is often an area law enforcement agency, will receive the calls and contact the USMS duty officer. The USMS stated that because USMS duty officers rotate frequently, it is impractical and unnecessary to have the number connect directly to them as they may be transferred, on vacation, or on leave. The USMS also stated that it believed that the OIG finding of non-working numbers was primarily driven by the past issuance of a working

contact number that connected directly to the local USMS duty officer. According to the USMS, the problem would continue if contact numbers were issued in this fashion, and it cannot support the part of the OIG recommendation to require that the letters contain a working contact number that connects directly to the local USMS duty officer. However, the USMS agreed that it is critically important that the notification letter list a working contact number for the local USMS office and have connectivity to the local USMS duty officer at all times.

OIG Analysis. The intent of this recommendation is to ensure that the USMS is notified promptly if an emergency occurs at a judge's residence. The USMS has provided a viable explanation for its partial non-concurrence with this recommendation, and we accept the proposed alternative procedure. Please provide the OIG, by March 1, 2010, a copy of the new memorandum that clearly explains that the notification letters must contain a working contact number that connects directly to the local USMS office or the USMS answering service after business hours. Please also provide the OIG some copies of letters the districts send to the local law enforcement agencies in their districts that contain a working number that connects directly to the local USMS office or the USMS answering service after business hours.

Recommendation 11. The USMS and EOUSA sign a memorandum of understanding that defines their roles and responsibilities in protecting U.S. Attorneys and AUSAs who receive threats.

Status. Resolved – open.

Summary of USMS Response. The USMS concurred with the recommendation. The USMS will consult with EOUSA about establishing a memorandum of understanding that defines their roles and responsibilities in protecting United States Attorneys and AUSAs who receive threats.

OIG Analysis. The actions planned by the USMS are responsive to our recommendation. Please provide the OIG with a copy of the memorandum of understanding that describes the roles and responsibilities of EOUSA, USAOs, USMS headquarters, and USMS district offices by March 1, 2010.

APPENDIX VI: THE EXECUTIVE OFFICE FOR UNITED STATES ATTORNEYS' RESPONSE



U.S. Department of Justice

Executive Office for United States Attorneys
Office of the Director

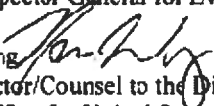
Main Justice Building, Room 2261
956 Pennsylvania Avenue, NW
Washington, DC 20537

(202) 514-212A

MEMORANDUM

DATE: December 11, 2009

TO: Michael Gullledge
Assistant Inspector General for Evaluations and Inspections

FROM: Norman Wong 
Deputy Director/Counsel to the Director
Executive Office for United States Attorneys

SUBJECT: Response to OIG's Report Entitled: Review of the Protection of the Judiciary and the United States Attorneys, A-2008-006

This memorandum is submitted by the Executive Office for United States Attorneys (EOUSA) in response to the audit report by the Office of Inspector General (OIG) entitled, "Review of the Protection of the Judiciary and the United States Attorneys," Report No. A-2008-006.

The safety and security of each and every employee within the United States Attorneys' Offices (USAOs), and within EOUSA, are of paramount importance to EOUSA and the USAOs. EOUSA welcomes and appreciates this review regarding the procedures used to help protect United States Attorneys and Assistant United States Attorneys. We believe the recommendations from the report will have a positive impact on the USAO community.

As the report makes clear, the number of threats to USAO personnel have been increasing since 2006. EOUSA currently has in place an effective and relatively efficient system for learning about, tracking, and helping to respond to threats to United States Attorneys and Assistant United States Attorneys. The system is based upon a threat reporting structure that starts with a report of a threat to the District Office Security Manager (DOSM) in a USAO. The DOSM then reports the threat to EOUSA, the United States Marshals Service, and the FBI, as appropriate.

Of course, the DOSM can only report threats of which he or she is aware. As the report makes clear, not all threats are being reported to the DOSMs, in part perhaps because the threatened individual does not consider the threat to be serious. As noted below in response to recommendation No. 3, EOUSA will continue to notify all USAO employees to promptly notify

the DOSM of any threat, regardless of whether the employee considers the threat to be serious. Reports of non-serious threats are still important in helping EOUSA coordinate with the USMS and FBI, and in giving those agencies a context and pattern to investigate any future threats. The report of non-serious threat may be critical in helping to prosecute a later, serious threat to the same or another employee.

The OIG report also notes that when reports of threat are made, they do not always include full and complete information regarding the threat, and that tracking follow-up activities undertaken in response to reported threats could be improved. Even prior to the OIG report recommendation on this issue, EOUSA had undertaken to convert the current Urgent Report system to a web-based reporting system. We expect that a web-based system will improve the completeness and timeliness of both initial reports of threat and follow-up reports.

The report also suggests additional training for both DOSMs and EOUSA personnel. EOUSA always welcomes and encourages additional training. We note our continued disagreement, however, with the characterization, on pages ii, v, and 27, regarding the level of expertise held by the current EOUSA security personnel. Unlike the DOSM positions in the USAOs, which are collateral duty positions and may properly be filled by persons with varying degrees of security experience, the security personnel at EOUSA, including the Assistant Director for Security Programs, have and properly should have extensive security-related backgrounds. We also strongly disagree with the statement on page 28 that the Assistant Director has limited time to devote to threat response and related training. The safety and security of USAO employees is always the Assistant Director's top priority.¹

¹EOUSA's Assistant Director has 29 years of federal security related experience with the United States Army, the Drug Enforcement Administration, and other agencies. Both as a Counterintelligence Technician (Special Agent) for the Department of the Army and later as Supervisory Physical Security Specialist with the DEA, he has undertaken residential security evaluations of individuals following their receipt of a threat. His evaluations included an assessment of the threat of criminal activity, such as burglaries, as well as more sophisticated intrusions such as electronic eavesdropping. As a Physical Security Specialist with the DEA, he developed, designed, and implemented intrusion detection, access control, and surveillance systems for both commercial and residential locations. He has served as an instructor with the US Army, DEA, the Department of Defense, and EOUSA on security-related topics, including physical security and risk management. He has attended, each year for the past 10 years, the American Society for Industrial Security (ASIS) annual conference, which is a 40 hour annual training event in various security disciplines. In addition, we note that the current Threat Management Specialist at EOUSA is a former Commander of the Technical Investigations Section of the Maryland State Police. In that role he supervised 20 investigators and analysts.

Recommendations

The recommendations below are numbered according to the numbers given them in the report.

3. *EOUSA amend the U.S. Attorneys' Manual to clearly instruct the AUSAs that all threats must be reported promptly to the District Office Security Manager. Such instruction should include an explanation of the detrimental effect that delays or the failure to report has on the security provided.*

EOUSA agrees to implement this recommendation. EOUSA has already, prior to a formal amendment of the USAM, issued a memorandum to all United States Attorneys reminding them that it is incumbent upon each Assistant United States Attorney and each USAO employee to notify the District Office Security Manager in their district of any and all threats, even if they do not believe that the threat is a serious one. The memorandum notes that the report of threat plays a critical role in helping the USMS assess the pattern and context of future threats. EOUSA is providing OIG with a copy of that memorandum under separate cover. In addition, EOUSA will notify OIG when the USAM has been formally amended.

10. *EOUSA provide, in consultation with the USMS, sufficient training to EOUSA and USAO staff assigned threat response.*

EOUSA agrees to implement this recommendation. EOUSA will consult with the USMS on the training curriculum.

11. *The USMS and EOUSA sign a memorandum of understanding that defines their roles and responsibilities in protecting U.S. Attorneys and AUSAs who receive threats.*

EOUSA agrees to implement this recommendation. While EOUSA and the USMS have a cooperative and effective relationship, a formal memorialization of the roles and responsibilities between EOUSA and the USMS when a threat is received by a USAO employee is appropriate. EOUSA will consult with USMS to produce the memorandum of understanding.

12. *EOUSA provide guidance and periodic reminders to USAOs of the requirement to submit Urgent Reports immediately when a U.S. Attorney or AUSA is threatened.*

EOUSA agrees to implement this recommendation. As noted above, EOUSA has already issued a memorandum to all United States Attorneys reminding all USAO employees to notify their DOSM and office management when a threat is received.

13. *EOUSA revise the Urgent Report template so that it includes a requirement to provide at least the following information:*
- *name and position of targeted employee;*
 - *name and location of the person making the threat, if known;*
 - *date the threat was made, or date the target was made aware of the threat;*
 - *date the District Office Security manager was informed of the threat;*
 - *date the USMS and FBI were notified; and*
 - *date the USAO submitted the Urgent Report to EOUSA*

EOUSA agrees to implement this recommendation. As indicated above and in the report, EOUSA is developing a new, web-based Urgent Report system that will facilitate more timely and complete threat reporting. EOUSA hopes to pilot the new web-based system in the second quarter of 2010. Also, as part of the memorandum issued to all United States Attorneys, referred to above, EOUSA has created and made available to all USAOs a new threat reporting form, to be used in the existing Urgent Report system. The new form covers all the information listed above.

14. *EOUSA establish guidance to require the District Office Security Managers to send updated information via Urgent Reports at regular intervals to inform EOUSA of the status of USAO, USMS, and FBI actions to protect the threatened AUSA.*

EOUSA agrees to implement this recommendation. The memorandum just issued to all United States Attorneys reminds each office of this requirement. Moreover, the new, web-based system will facilitate greater and more complete follow-up reporting from the districts.

APPENDIX VII: OIG'S ANALYSIS OF THE EXECUTIVE OFFICE FOR UNITED STATES ATTORNEYS' RESPONSE

The Office of the Inspector General provided a draft of this report to the Executive Office for United States Attorneys (EOUSA) for its comment. The report contained 14 recommendations: Recommendations 1, 2, 4, and 5 through 9 are directed to the United States Marshals Service (USMS). Recommendations 3, 10, 12, 13, and 14 are directed to EOUSA. Recommendation 11 is directed to both the USMS and EOUSA.

EOUSA's response is included in Appendix VI to this report. In its response, EOUSA concurred with the recommendations addressed to it, and outlined steps to address the recommendations. It also made general comments regarding statements in the report on the level of expertise of EOUSA security personnel. We first address EOUSA's comments and then discuss its response to the recommendations.

General Comments

Summary of EOUSA Response. EOUSA in its response disagreed with the OIG's characterization of the expertise of current EOUSA security personnel in judicial security operations. EOUSA stated that unlike the District Office Security Manager positions in the United States Attorney Offices (USAO), which are collateral duty positions and may be filled by persons with varying degrees of security experience, the security personnel at EOUSA, including the Assistant Director for Security Programs, have extensive security-related backgrounds. EOUSA also stated in response to the OIG's statement on page 28 of the report that the safety and security of USAO employees is always the Assistant Director's top priority.

OIG Analysis. OIG agrees that the Assistant Director of the Security Programs Staff has an extensive background in physical and electronic and security operations appropriate to fulfill his role overseeing many of the security related matters facing USAOs. However, Deputy Marshals involved in ensuring the safety of protectees generally have not only extensive law enforcement training, but also specific training in protecting members of the judiciary, including determining and implementing threat response procedures. Moreover, our concern was primarily with the experience and training of the USAO staff in the 93 judicial districts, since they are the on-site personnel responding directly when United States Attorneys and Assistant United States Attorneys (AUSA) are threatened.

Recommendation 3. EOUSA amend the *U.S. Attorneys' Manual* to clearly instruct the AUSAs that all threats must be reported promptly to the District Office Security Manager. Such instruction should include an explanation of the detrimental effect that delays or the failure to report has on the security provided.

Status. Resolved – open.

Summary of EOUSA Response. EOUSA concurred with this recommendation and stated that it will notify the OIG when the *U.S. Attorneys' Manual* has been formally amended. In the interim, EOUSA issued a memorandum to all U.S. Attorneys reminding them that it is incumbent upon each USAO employee to notify the District Office Security Manager of all threats. The memorandum notes that threat reports play a critical role in helping the USMS assess the pattern and context of future threats. EOUSA provided the OIG with a copy of that memorandum under separate cover.

OIG Analysis. The actions planned by EOUSA are responsive to our recommendation. Please provide the OIG with a copy of the final, approved *U.S. Attorneys' Manual* amendments or a status report regarding the policy amendments by March 1, 2010.

Recommendation 10. EOUSA provide, in consultation with the USMS, sufficient training to EOUSA and USAO staff assigned threat response duties.

Status. Resolved – open.

Summary of EOUSA Response. EOUSA concurred with this recommendation and plans to consult with the USMS on the training curriculum.

OIG Analysis. Although EOUSA concurred with the recommendation, it did not provide any details regarding its training plans. Please provide the OIG with a timeline for implementation of revised training, information on who will be trained and how the training will be delivered, and a copy of the proposed training curriculum or a status report regarding the plans by March 1, 2010.

Recommendation 11. The USMS and EOUSA sign a memorandum of understanding that defines their roles and responsibilities in protecting U.S. Attorneys and AUSAs who receive threats.

Status. Resolved – open.

Summary of EOUSA Response. EOUSA concurred with the recommendation. EOUSA will consult with the USMS to produce a memorandum of understanding that defines the roles and responsibilities of EOUSA and the USMS when a threat is received by a USAO employee.

OIG Analysis. The actions planned by EOUSA are responsive to our recommendation. Please provide the OIG with a copy of the memorandum of understanding that describes the roles and responsibilities of EOUSA, USAOs, USMS headquarters, and USMS district offices by March 1, 2010.

Recommendation 12. EOUSA provide guidance and periodic reminders to USAOs of the requirement to submit Urgent Reports immediately when a U.S. Attorney or AUSA is threatened.

Status. Resolved – open.

Summary of EOUSA Response. EOUSA concurs with this recommendation. EOUSA issued a memorandum to all U.S. Attorneys, First Assistant U.S. Attorneys, District Office Security Managers, and Criminal Chiefs to remind all USAO employees to notify their District Office Security Manager and office management when a threat is received.

OIG Analysis. EOUSA issued a memorandum to all USAOs that is responsive to the intent of this recommendation. The memorandum reiterates the requirement in the *U.S. Attorneys' Manual* to immediately report to EOUSA via Urgent Report any threat to USAO personnel. However, we believe that periodic reminders by EOUSA of the reporting requirement should still be made to the USAOs. Please provide the OIG with a description, by March 1, 2010, of how often EOUSA intends to send reminders to all U.S. Attorneys, First Assistant U.S. Attorneys, District Office Security Managers, and Criminal Chiefs to remind all USAO employees to notify their District Office Security Manager and office management when a threat is received. Also, please provide the OIG with a copy of the next reminder when issued.

Recommendation 13. EOUSA revise the Urgent Report template so that it includes a requirement to provide at least the following information:

- name and position of targeted employee;
- name and location of the person making the threat, if known;

- date the threat was made, or date the target was made aware of the threat;
- date the District Office Security Manager was informed of the threat;
- date the USMS and FBI were notified; and
- date the USAO submitted the Urgent Report to EOUSA.

Status. Resolved – open.

Summary of EOUSA Response. EOUSA concurred with this recommendation and stated that it has made available to all USAOs a new threat reporting form covering the information in our recommendation. EOUSA is also developing a web-based Urgent Report system intended to facilitate timely and complete threat reporting that it hopes to pilot in the second quarter of 2010.

OIG Analysis. EOUSA concurred with the recommendation and provided a new threat reporting form to the USAOs that included the information in the recommendation. Please provide to us by March 1, 2010, the system requirements documents for the web-based Urgent Report system (specifically the section that includes the above elements as functional requirements for completion of the Urgent Report form), and a copy of the instructions to the USAOs for reporting threats using the system.

Recommendation 14. EOUSA establish guidance to require the District Office Security Managers to send updated information via Urgent Reports at regular intervals to inform EOUSA of the status of USAO, USMS, and FBI actions to protect the threatened AUSA.

Status. Resolved – open.

Summary of EOUSA Response. EOUSA concurred with this recommendation. EOUSA has issued a memorandum to all U.S. Attorneys to remind each office of the requirement to send updated information to EOUSA. EOUSA is also developing a web-based Urgent Report system intended to facilitate greater and more complete follow-up reporting from the districts.

OIG Analysis. Although EOUSA concurred with the recommendation, it has not established guidance that requires District Office Security Managers to send updated information via Urgent Reports to inform EOUSA of the status of actions taken to protect threatened USAO employees. The memorandum does not establish a requirement to send this

updated information and is not equivalent to amending current policy. Please provide us with a copy of the amended guidance that includes the requirement to provide updated information to EOUSA by March 1, 2010.