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

# The United States Marshals Service Judicial Security Process

## September 2007

**I-2007-010**

## EXECUTIVE DIGEST

## INTRODUCTION

One of the critical missions of the United States Marshals Service (USMS) is to protect the members of the federal judiciary. The USMS is responsible for protecting approximately 2,200 federal judges and 5,500 other individuals related to the work of the federal judiciary at over 400 court facilities nationwide.

In March 2004, the Department of Justice (Department) Office of the Inspector General (OIG) issued a report that concluded that while the USMS had placed greater emphasis on judicial security after the September 11, 2001, terrorism attacks, it needed to take immediate steps to improve its ability to assess and respond to threats to the federal judiciary.[1] The USMS's assessments of reported threats were often untimely and of questionable validity. The USMS's capability for collecting and sharing intelligence on potential threats was limited. The USMS also lacked adequate standards for determining which protective measures should be used in response to potential risks. We made six recommendations to improve the USMS's capacity for protecting the federal judiciary. The USMS concurred with all six and took steps to address them.

The OIG conducted this follow-up review to examine the USMS's progress since our March 2004 report. In this review, we examined 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 USMS has taken to improve judicial security and to enhance its capability to respond to judicial security incidents.[2]

[1] 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).

[2] Reported threats are incidents, situations, activities, or communications that are brought to the attention of the USMS by the recipient of the threat or by other law enforcement or intelligence agencies. Potential threats are individuals or groups that pose a threat to a USMS protectee but have not communicated a direct threat to their targets or to law enforcement or intelligence agencies.

## RESULTS IN BRIEF

The OIG found that from the issuance of the OIG's March 2004 report through early 2007, the USMS's efforts to improve its capabilities to assess reported threats and identify potential threats languished. During this period, threat assessments took longer to complete, and over half of the assessments were not completed, resulting in a backlog of 1,190 "pending" threat assessments as of October 1, 2006. Also, the USMS was slow in staffing its recently established Office of Protective Intelligence, and it did not collect and analyze information on potential threats.[3]

In fiscal year (FY) 2007, the USMS assigned additional resources to resolve the backlog of pending threats and began assessing new threats more quickly. The USMS also began enhancing security measures to protect the federal judiciary. For example, the USMS implemented the congressionally authorized home alarm program and, as of July 2007, has installed about 95 percent of the home alarms requested by federal judges. Also, to support the judicial security mission, the USMS is enhancing the use of its Technical Operations Group, which uses sophisticated technologies to provide investigative and intelligence support. In addition, the USMS is developing a Rapid Deployment Team program that will respond to significant incidents involving judicial security around the country.

However, the USMS acknowledges that it needs to further improve its threat assessment process and to more fully develop protective intelligence that identifies potential threats against the judiciary. USMS managers told us that they believe the current headquarters threat assessment process is of limited utility and said that they plan to implement a new process in FY 2008. Moreover, to enable it to collect and analyze information on potential threats, the USMS has identified various protective intelligence initiatives it would like to implement by FY 2010, such as establishing a system for reporting suspicious activities around courthouses and procuring additional analytical tools for evaluating the information. However, the USMS lacks detailed plans that identify the objectives, tasks, milestones, and resources for accomplishing these needed improvements. We believe that the USMS must exhibit a greater sense of urgency in implementing its plans for

[3] The Office of Protective Intelligence was established in June 2004. It is a component of the Judicial Security Division, which is responsible for the USMS's federal judicial security programs.

improving its capability to assess reported threats, developing and sharing protective intelligence on potential threats, and completing the implementation of enhanced security measures for the federal judiciary.

The OIG conducted a survey of all 2,141 federal judges to obtain their perceptions of their safety and security and of the USMS's efforts to protect them. Federal judges reported that they believe the unknown general danger associated with being a judge (which we term "potential threat") poses a greater risk than stated or implied threats (which we term "reported threat"). They reported that they believe that risk varies by the type of cases they hear, with gang, terrorism, and organized crime cases posing higher risks. Regarding the USMS's performance, federal judges reported that they were satisfied with the protection provided by the USMS. Specifically, 87 percent reported that they were either very or somewhat satisfied with its performance, and only 5 percent were somewhat or very dissatisfied.[4] A majority of the judges also reported that they were satisfied with the USMS judicial security personnel assigned to their districts. In response to questions about what measures the USMS should take to further improve judicial security, the greatest number of judges ranked improving intelligence collection and analysis capability as most important.

In addition to surveying federal judges, we interviewed 29 individuals, including representatives from the USMS, federal judges, and officials in the Administrative Office of the U.S. Courts. We also conducted a survey of 82 Judicial Security Inspectors who oversee judicial security operations in USMS district offices. We attended the 40-hour USMS Protective Investigations Training Program course conducted at the Federal Law Enforcement Training Center in August 2006. We also reviewed relevant USMS Directives, policies and procedures, manuals, training materials, clearance rosters, and examples of Office of Protective Intelligence information products. The following sections provide additional details on our findings.

**Assessing Reported Threats**

The threat assessment process begins with the receipt or identification of a threat. The USMS takes measures to ensure the protectee's safety at the district level and then reports pertinent information on the incident to the Office of Protective Intelligence for a threat assessment, which provides data the district uses in determining

[4] Seven percent were neither satisfied nor dissatisfied.

the appropriate protective response. After the issuance of our March 2004 report on judicial security, the USMS failed to improve the timeliness of its threat assessments in FY 2005 and FY 2006. We reviewed a random sample of 568 of the 2,018 threats reported to USMS headquarters in those 2 years and found that the Office of Protective Intelligence did not assess threats within established timeliness standards in about two-thirds of all cases in our sample. Moreover, the USMS did not complete threat assessments on more than half of all reported threats, which led to a backlog of 1,190 "pending" assessments as of October 1, 2006. We also found that the Office of Protective Intelligence did not monitor the timeliness of threat assessments during FY 2005 and FY 2006. Office of Protective Intelligence management said the poor performance was due to the increasing number of reported threats and its inability to hire additional analytical staff.

In early FY 2007, Office of Protective Intelligence management implemented procedures to manually monitor the timeliness and quality of threat assessments and dedicated additional staff time to assessing threats and resolving the backlog of pending cases. We found that those actions taken by the USMS enabled it to assess reported threats more quickly beginning in FY 2007. Our examination of a random sample of 232 threats from the first half of FY 2007 found that the USMS had conducted assessments on all of them and that 93 percent of the assessments were completed within applicable timeliness standards. Although threat assessments are now more timely, Judicial Security Division managers told us that the assessments produced under the current process are of limited utility because they do not provide sufficient information about the threateners' behavior. USMS managers told us that they plan to change the threat assessment process in FY 2008.

USMS managers further explained that the Office of Protective Intelligence is starting to employ a more collaborative method of working with the 94 USMS districts on protective investigations, threat assessments, and case management. Although each protective investigation is unique, Office of Protective Intelligence managers told us that they see the new process as an opportunity to standardize, over time, the protective investigation process performed in each of the districts.

The new threat assessment process described to us by Office of Protective Intelligence managers could improve the ability of the USMS to assess and respond effectively to reported threats. However, the Office of Protective Intelligence has not developed formal plans or guidance for the

new process, with defined milestones, tasks, and outcomes. The new process needs to be formalized and defined in order for the Office of Protective Intelligence to implement it, provide direction to the districts, and provide training to headquarters and district staff involved in the judicial protection mission.

**Identifying Potential Threats**

The USMS has made limited progress at implementing a program to collect and analyze information to identify potential threats. In June 2004, the USMS established the Office of Protective Intelligence to provide a centralized function for assessing reported threats and identifying potential threats. Our current review found that 3 years after the USMS established the office, it still lacks the staff needed to gather and analyze information to develop protective intelligence on potential threats. From May 2005 through July 2007, the USMS added staff to the Office of Protective Intelligence, but the additional resources were primarily assigned to the Investigations Branch where they assessed reported threats.

The USMS has made improvements to its capacity for collecting classified information by increasing the number of staff with Top Secret clearances. The USMS also installed additional secure telephones in district offices and built a secure facility for working with classified information at headquarters. While in August 2003 51 of the USMS's 94 districts had secure telephones to transmit classified information, by April 2005 all 94 districts had them. Also, as of July 2007 the USMS was nearing completion on construction and accreditation of a Threat Management Center housed in a sensitive compartmented information facility. The Threat Management Center will provide the Office of Protective Intelligence with the capacity to electronically receive, access, analyze, and disseminate classified information related to threats to the judiciary.

However, the Office of Protective Intelligence still does not systematically collect and analyze information about potential threats to the judiciary from its districts, other federal, state, and local law enforcement agencies, or courts to produce protective intelligence. For example, we found that:

- The Office of Protective Intelligence does not analyze information it already receives on reported threats to detect national or regional patterns. Analyses that identify trends in the types of USMS protectees receiving threats, threat delivery

methods, and the types of people who threaten the judiciary could help the districts allocate resources and identify areas that need improvement.

- The USMS has not issued guidance on the type of judicial security information to be reported by district office personnel to the Office of Protective Intelligence.

- The Office of Protective Intelligence does not analyze data on courthouse incidents that the Judicial Security Division collects from the districts to identify trends or patterns in suspicious activities that may indicate potential threats. Judicial Security Division managers stated that they plan to develop a Suspicious Activity Report database between FY 2007 and FY 2009 (depending on funding and staff availability) to identify potential threats.

- The Office of Protective Intelligence does not collect and analyze judicial security-related information from federal, state, or local court databases to identify cases that may pose a risk to the federal judiciary.

We also found that the USMS has not assigned full-time representatives to all Federal Bureau of Investigation Joint Terrorism Task Forces to improve access to information and intelligence related to judicial security. From FY 2004 through FY 2007, the USMS reduced the number of full-time Joint Terrorism Task Force representatives from 25 to 17 and reduced the number of part-time representatives from 25 to 23. During this period, USMS districts also began assigning liaisons to Joint Terrorism Task Forces. Unlike full- or part-time representatives, these liaisons do not work on a Joint Terrorism Task Force and do not have direct access to Federal Bureau of Investigation databases. As of July 2007, USMS districts have assigned 39 liaisons.

In a March 30, 2007, memorandum to the OIG, the USMS Assistant Director of the Judicial Security Division listed numerous initiatives that the USMS plans to accomplish by FY 2010 to improve the protective intelligence capabilities of Office of Protective Intelligence, such as establishing a system for reporting suspicious activities around courthouses and procuring additional analytical tools. (See Appendix I for details.) We believe that these initiatives would help the USMS identify potential threats, but as with our review of the threat assessment process discussed previously, we note that the Office of Protective

Intelligence has not developed formal plans with defined milestones, tasks, and outcomes to achieve these goals.

**Implementing Enhanced Security Measures**

Since our March 2004 report, the USMS has implemented additional security measures to protect the federal judiciary, such as the installation of home alarms, the enhancement of its Technical Operations Group, and the creation of a Rapid Deployment Team program to respond to significant judicial security incidents. We describe the status of these initiatives below.

Home Alarms. On June 14, 2005, the Administrative Office of the U.S. Courts asked all federal judges whether they wanted an alarm system installed in their homes. Approximately 1,600 of the 2,200 judges requested alarm systems. In December 2005, the USMS awarded the contract to install the home alarms. After conducting several pilot installations, between March 2006 and July 2007 the USMS contractor installed alarms in 1,531 judges' residences. As of July 2007, the USMS reported that it had 67 outstanding requests for alarm systems. Of the 67 requests, approximately 30 of the judges are undecided and have yet to arrange for the home inspection or installation. The other 37 were requests for which installation was proceeding.[5]

The USMS is not directly notified of events that trigger the federal judges' home alarms. Initially, the USMS Communications Center was included on several judges' Emergency Contact List which identifies individuals who may be called prior to the notification of the authorities. However, according to a JSD manager this presented a problem because the Communications Center is unable to provide immediate physical responses to alarms in the residences across the country. Therefore, the USMS decided that it should not be included on this list. Now, when an alarm is received, the contractor utilizes the judge's Emergency Contact List. If contact cannot be made, the contractor then notifies local law enforcement. Although the USMS told all districts to ask local law enforcement agencies to notify it of any emergency response to a judge's residence, as of July 28, 2007, the USMS did not know how many alarm events had occurred at judges' residences or how many times local police made emergency responses.

[5] Some judges' alarm systems were not installed because the judges have indicated to the USMS that they no longer want the system, are no longer federal judges, or did not work with the USMS and the contractor to design and install the system.

We have several concerns regarding the USMS's lack of awareness about alarm events at judges' residences. We agree that the contractor should immediately notify local law enforcement agencies of all unresolved alarms so that they can respond quickly. We believe, however, that the contractor should also notify the USMS (after it calls the local law enforcement agency) so that the USMS can determine whether a protective investigation is warranted.

Technical Operations Group. The USMS is enhancing its Technical Operations Group support of the judicial security mission. In response to requests from district offices, the Technical Operations Group uses sophisticated technologies to provide investigative and intelligence support, primarily for the USMS fugitive apprehension mission. Our follow-up review found that the USMS made some initial resource enhancements to the Technical Operations Group and plans to provide further resource enhancements in FY 2008.[6] However, at the time of this report the USMS had not yet issued guidance on requesting Technical Operations Group assistance or criteria for when Technical Operations Group resources should be deployed in support of the judicial security mission. The USMS has identified the need for such written requirements and provided a draft of the document to the OIG in May 2007.

Rapid Deployment Team. The Judicial Security Division recently initiated a Rapid Deployment Team program to respond to significant incidents, such as an assault on a judge or a disruption of a U.S. courthouse's operation. In March 2007, the Deputy Assistant Director for Judicial Operations told the OIG that the Judicial Security Division had assigned a working group to draft the operating methodology and plans for the Rapid Deployment Team program by the end of May 2007. As of July 2007, the Rapid Deployment Team program was still in development, and no deployments had occurred. In July 2007, the Deputy Assistant Director stated that the operating methodology and plans for the program would not be completed until September 2007.

[6] In September 2006, the Judicial Security Division transferred three personnel to the Technical Operations Group and, in its FY 2008 budget submission, requested funding for six positions to assist in the enhanced Technical Operations Group support of the judicial security mission. The USMS also requested $890,000 for Technical Operations Group equipment and technology.

## CONCLUSION AND RECOMMENDATIONS

We found that from the issuance of the OIG's March 2004 report through early 2007, the USMS's efforts to improve its capabilities to assess reported threats and identify potential threats languished. Threat assessments took longer to complete, and over half of the threats reported by USMS districts remained pending as of October 1, 2006. Also, the USMS did not implement an effective program to develop protective intelligence that identifies potential threats against the judiciary. The USMS acknowledges these deficiencies and plans to revise its threat assessment process. During this review, the USMS also informed the OIG of numerous initiatives it plans to implement by FY 2010 to enable it to better collect and analyze information on potential threats to the judiciary.

Also, since our March 2004 report, the USMS has implemented several security measures to protect the federal judiciary. The USMS has implemented a congressionally authorized home alarm program and worked with a contractor that installed about 95 percent of the home alarms requested by federal judges. The USMS is also enhancing its Technical Operations Group and developing a Rapid Deployment Team program to support the judicial security mission.

We believe that to fulfill its critical mission of protecting the federal judiciary, the USMS must exhibit a greater sense of urgency in implementing its plans for improving its capability to assess reported threats, creating and sharing protective intelligence on potential threats, and completing the implementation of enhanced security measures.

To improve the USMS's capacity to protect the federal judiciary, we recommend that the USMS take the following actions:

1. Develop a formal plan that defines objectives, tasks, milestones, and resources for the new threat assessment process.

2. Create a workload tracking system for threat assessments.

3. Develop a formal plan that defines objectives, tasks, milestones, and resources for implementing a protective intelligence function to identify potential threats.

4. Modify USMS databases to support the new threat assessment process and protective intelligence function to identify potential threats.

5. Require the home alarm contractor to notify the USMS of alarm events after notifying the local law enforcement agency.

6. Issue operational guidance for requesting and deploying Technical Operations Group resources and Rapid Deployment Teams.

## TABLE OF CONTENTS

## INTRODUCTION

In March 2004, the Department of Justice (Department), Office of the Inspector General (OIG) issued a report on the United States Marshals Service's (USMS) judicial security process.[7] The OIG found that:

- USMS assessments of threats against USMS protectees were often untimely and of questionable validity;
- The USMS had a limited capability to collect and share intelligence on potential threats; and
- The USMS also lacked adequate standards for determining which protective measures should be used in responding to potential risks.

The OIG conducted this current review to follow up and examine the USMS's progress since our March 2004 report.

The USMS judicial security operations examined in this report encompass three broad areas: the assessment of reported threats made against USMS protectees; the development of a protective intelligence capability to identify potential threats; and recent measures to improve judicial security and to enhance the USMS's capability to respond to judicial security incidents.

### BACKGROUND

One of the critical missions of the USMS is to protect the members of the judiciary. The USMS is responsible for protecting approximately 2,200 federal judges and 5,500 other individuals who work alongside the federal judiciary, including prosecutors and jurors, at over 400 court facilities nationwide. The primary duties the USMS performs to ensure the security and safety of its protectees and the judicial process are providing personal protection, providing physical security in courthouses, safeguarding witnesses, and transporting and producing prisoners for court proceedings. USMS protectees can include:

[7] Department of Justice, Office of the Inspector General, *Review of the United States Marshals Service Judicial Security Process,* Report I-2004-004, March 2004.

- federal judges (magistrate, bankruptcy, district, appellate);
- U.S. Attorneys, Assistant U.S. Attorneys, and their staffs;
- U.S. Probation Officers;
- Pretrial Services Officers;
- Tax Court Judges (Article I Judges);
- Clerks of the Court;
- Federal Public Defenders;
- Justices of the Supreme Court of the United States (in cooperation with the Supreme Court Police);
- U.S. Trustees; and
- jurors and witnesses.

According to the USMS, in performing its judicial security mission in fiscal year (FY) 2006 it:

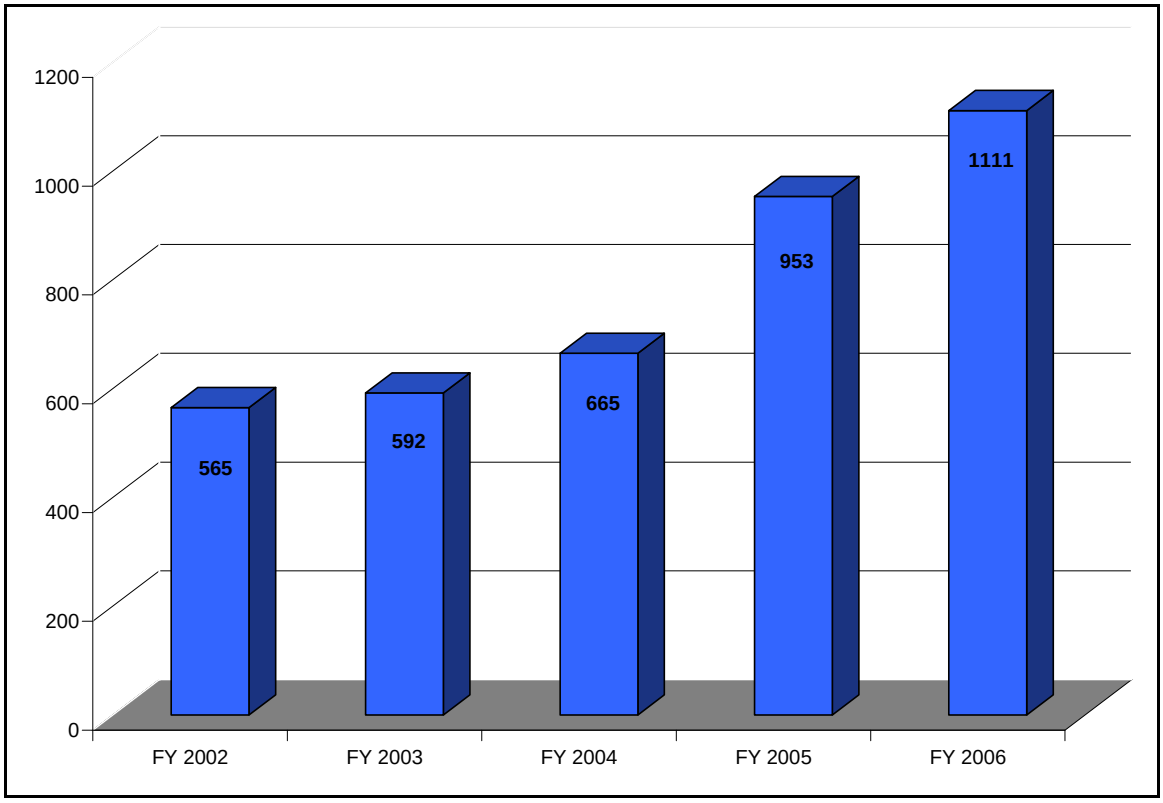
- conducted 215 protective service details for Supreme Court Justices;
- conducted 44 protective details for members of the federal judiciary;
- provided security for 179 judicial conferences and 26 special events attended by members of the federal judiciary;
- coordinated and provided security for 135 high-threat trials;
- performed threat assessments on 1,111 reported threats;
- trained 210 Deputy Marshals in a 3-day Judicial Protection Training Conference; and
- trained 190 Deputy Marshals in a 5-day training seminar on protective investigations.

According to the USMS, the number of reported inappropriate communications and threats against members of the judiciary has continued to increase since FY 2002. The USMS defines an inappropriate communication as any communication directed to a USMS protectee that warrants further investigation. The USMS defines a threat as "any action, whether 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 staff and their family."[8] Inappropriate communications and threats can be delivered in writing, electronically, telephonically, verbally, through an informant, or through some suspicious activity around the protectee. Chart 1 illustrates the number of reported inappropriate communications and threats from FY 2002 to FY 2006. The USMS expects to receive between 1,200 and 1,300 such communications by the end of FY 2007, although this number is not fully comparable to prior years' numbers because of a procedural change implemented in FY 2007. Office of Protective Intelligence managers told us that in FY 2007 they began coordinating and consolidating investigations involving mass mailings and habitual letter writers across districts, which reduced the number of new investigations recorded in the Warrant Information Network/Justice Detainee Information System (WIN/JDIS) by approximately 100 cases.[9]

[8] USMS Directive 10.16, Protective Investigations, April 2006.

[9] WIN/JDIS consolidates judicial threat data with warrant, criminal history, prisoner scheduling, and booking information in a single database. As the USMS's central law enforcement information system, WIN/JDIS is used to manage records and information collected during fugitive investigations and protective investigations involving potential threats made against the federal judiciary. WIN/JDIS contains current and historical case data for all USMS investigations. It is also used to access the National Law Enforcement Telecommunication System and National Crime Information Center systems to obtain criminal record information from other federal, state, local, and foreign law enforcement agencies.

**Chart 1: Number of Reported Inappropriate Communications and Threats, FY 2002 Through FY 2006**




Source: USMS FY 2008 Performance Budget

Table 1 shows the 10 USMS districts with the largest number of reported inappropriate communications and threats for FY 2006.[10]

[10] Based on information contained in the USMS's Warrant Information Network (WIN/JDIS) system that was provided to the OIG for analysis in November 2006, there were 1,059 reported threats in FY 2006. The USMS explained that the data it provided to the OIG does not match the 1,111 threats it reported to Congress in January 2007 (Chart 1) because WIN/JDIS allows case records to be updated or deleted and, therefore, the number of threats recorded in WIN/JDIS changes on a regular basis.

**Table 1: Districts With the Highest Number of Reported Inappropriate Communications and Threats in FY 2006**

| Ranking | District | Number |
|---|---|---|
| **1** | Nevada | 227 |
| **2** | Central California | 46 |
| **3** | Northern Georgia | 44 |
| **4** | Southern Texas | 35 |
| **5** | Northern California | 32 |
| **6** | Southern Florida | 30 |
| **7** | Southern New York | 29 |
| **8** | Northern Illinois | 28 |
| **9** | Eastern Louisiana | 25 |
| **10** | Middle Florida | 20 |
| **Total** | | **516** |

Source: USMS

According to the USMS, of the 1,111 inappropriate communications and threats reported in FY 2006:

- 46.4 percent came from the 10 districts listed in Table 1;[11]
- 64 of the 94 districts reported 10 or fewer inappropriate communications or threats to the Office of Protective Intelligence (OPI) in FY 2006;
- 684 inappropriate communications or threats were directed towards federal judges, 162 were directed at U.S. Attorneys and Assistant U.S. Attorneys, and 265 were directed at other USMS protectees;
- 651 inappropriate communications or threats were conveyed in writing, 141 by telephone, 130 through an informant, 79 verbally, and 110 were reported as suspicious activities;
- 659 inappropriate communications or threats were from identifiable individuals, 132 were anonymous, and 320 were initiated by individuals already incarcerated; and
- 10 inappropriate communications or threats were relayed in the form of a bomb threat and 2 as a biological-chemical threat.

[11] In the District of Nevada, a USMS official estimated that between 180 and 190 of the 227 reported inappropriate communications or threats in FY 2006 were attributable to one high-profile case.

## USMS Headquarters Operations

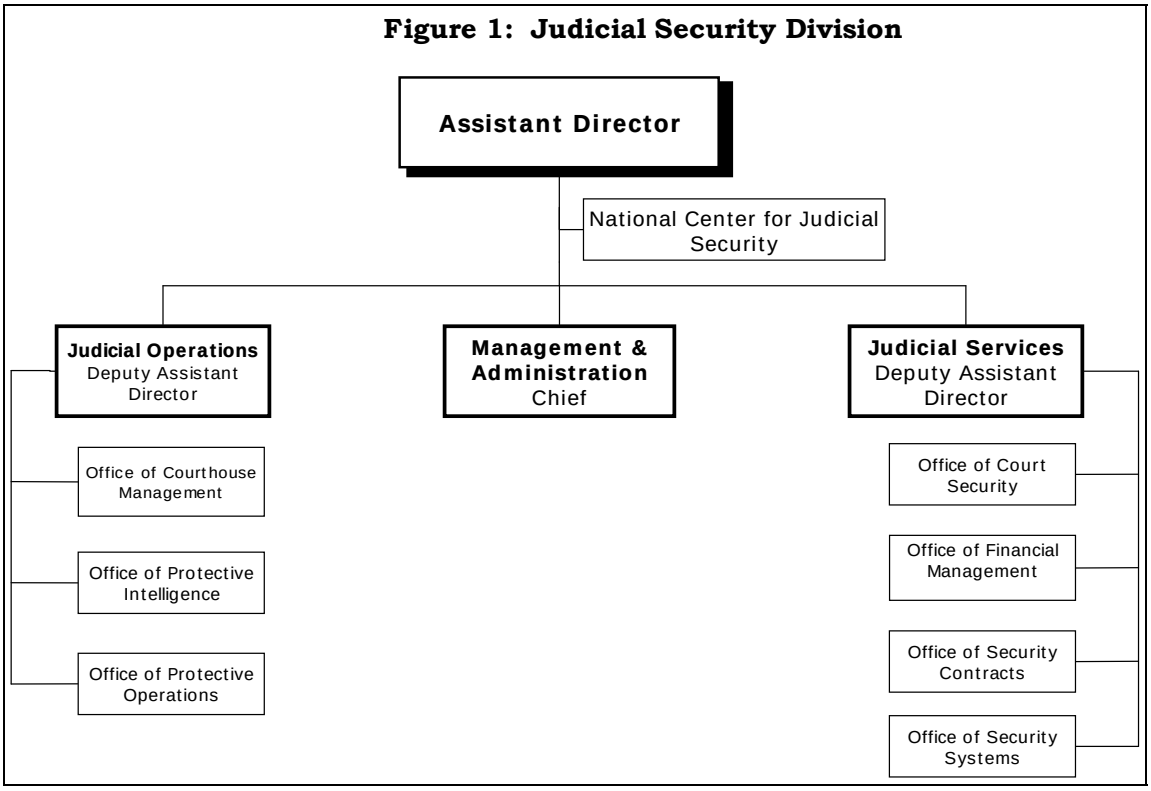
Judicial Security Division

The USMS Judicial Security Division (JSD) is responsible for the USMS's federal judicial security programs, including protective intelligence operations, physical protection of judicial facilities, personal protection, and technical security operations for the judiciary. The JSD's strategic plan for 2007-2011 states that the JSD:

- provides proactive deterrence to threats against the federal judiciary;
- develops and implements innovative protective techniques;
- provides state-of-the-art equipment and new technologies for all physical and personal security requirements; and
- ensures rapid and safe responses to emergency situations as well as unobtrusive counter-surveillance and expert protection during routine judicial security operations.

The JSD consists of two operational components – Judicial Services and Judicial Operations – and an Office of Management and Administration (see Figure 1).

**Figure 1: Judicial Security Division**




Source: USMS 12-16-06

Judicial Services

The Judicial Services component has oversight for the USMS judicial security programs, which are funded by the Administrative Office of the United States Courts' (AOUSC) court security appropriation. This funding provides for the Court Security Officer program, security equipment and systems for space occupied by the judiciary, and for USMS employees to administer the daily functions. The Judicial Services component is responsible for overseeing four areas:

- the *Office of Court Security,* which is responsible for the daily operations and personnel management of the Court Security Officer program;

- the *Office of Financial Management,* which has the daily oversight responsibility for a $300 million budget;

- the *Office of Security Contracts,* which performs the daily contract responsibilities with the private contractors and the district Contracting Officers' Technical Representatives, and

- the *Office of Security Systems,* which is responsible for all security and monitoring systems for judicial space.

Judicial Operations

The Judicial Operations component utilizes a national network of operational personnel (Inspectors) and physical security specialists to manage personal and facility security issues for the judiciary. The Judicial Operations component is responsible for overseeing three areas:

- The *Office of Courthouse Management* serves as the center of expertise concerning prisoner movement and detention facilities within federal courthouses. This office also has oversight of the home intrusion detection system installation program for judges' personal residences.

- The *Office of Protective Operations* comprises four branches. The Policy and Operations Coordination Branch manages the Special Assignment Fund that assists districts with high-threat trials, terrorist trials, protection of the judiciary and other government officials, and any other unusual missions. The Dignitary Protection Branch supervises the Deputy Attorney General and the Director of the Office of National Drug Control Policy protection details. The Office of Protective Operations has a total of 33 inspectors and managers, including the 12 inspectors assigned to each of the 12 judicial circuits. The East and West Region Branches supervise their assigned inspectors who are responsible for protecting the Supreme Court Justices when they travel outside Washington, D.C. They also supervise all judicial conferences, supervise judicial and government officials under protection in the field, and assist the districts with the supervision and management of high-threat and terrorist judicial hearings in the field.

- The *Office of Protective Intelligence* is responsible for collecting, analyzing, producing, and disseminating threat analysis information and protective intelligence about groups, individuals, and activities that pose a potential threat to the judiciary and persons and property protected by the USMS. It is also responsible for providing this information to the districts, protective details, and USMS senior leadership. The Office of Protective Intelligence (OPI) is a central resource for guidance, oversight, and coordination for protective investigations and protective intelligence. Because the threat analysis and protective

intelligence operations of the OPI are a major focus of this report, the OPI's operations are discussed in greater detail below.

**The Office of Protective Intelligence**

On June 1, 2004, the USMS Director realigned existing resources and established the OPI within the JSD.[12] The goals of the OPI are to:

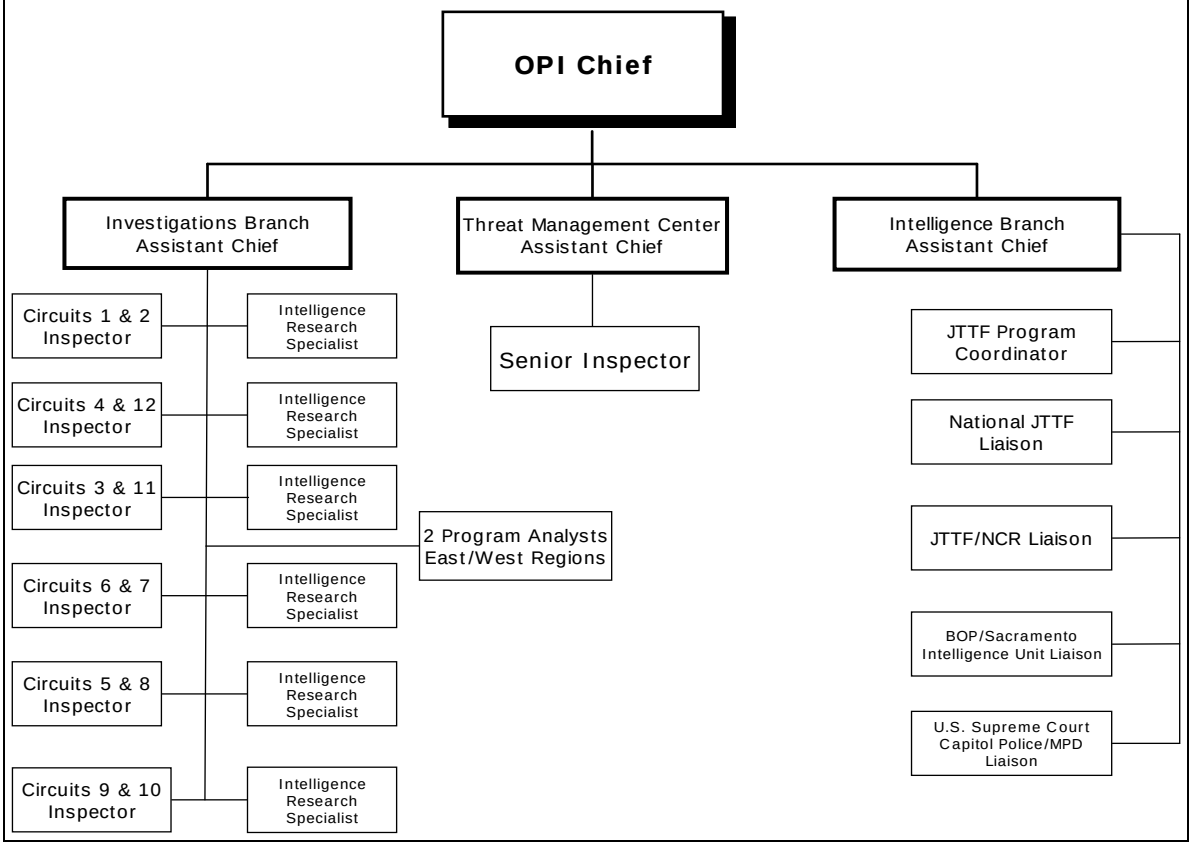
- provide information and intelligence for the planning and execution of USMS operations;
- develop and maintain a comprehensive repository of protective intelligence and information;
- provide information and data for allocation and management of resources, and data for the development and implementation of policies and procedures;
- provide a fusion center for all classified and unclassified information collected for analysis and development of protective intelligence products for applicable dissemination in support of USMS missions; and
- incorporate intelligence and information gathered from other agencies into comprehensive products that support USMS missions.[13]

The OPI comprises three components: the Investigations Branch, the Intelligence Branch, and the Threat Management Center (see Figure 2). The JSD requested six Inspector positions for FY 2008 for the Threat Management Center. In the interim, the JSD plans to staff the Threat Management Center with personnel from the Investigations Branch.

[12] The USMS reported the date of June 1, 2004, to the OIG in response to a recommendation in the OIG's March 2004 report, *Review of the United States Marshals Service Judicial Security Process*. On other occasions, the USMS has also cited July 1, 2005, as the date the OPI began operations, which is when the threat analysis and protective investigation functions were transferred from the Investigative Services Division's Analytical Support Unit to the OPI.

[13] OPI presentation made to USMS Protective Investigations Training Program participants, Federal Law Enforcement Training Center, July – August 2006.

**Figure 2: Office of Protective Intelligence**




Source: USMS June 2007

## Investigations Branch

The Investigations Branch's primary duty is to provide investigative oversight and analysis of inappropriate communications and threats reported by the districts to the OPI. Investigations Branch staff also produce and disseminate judicial security-related information to the districts, including alert notices, information bulletins, and foreign travel briefs. The Investigations Branch staff comprises six circuit teams.[14] Each team is responsible for 2 of the 12 judicial circuits and the respective USMS districts that fall within the circuit court structure.

[14] When fully staffed, each team will consist of one Intelligence Research Specialist and one Criminal Investigator.

Intelligence Branch

The Intelligence Branch is responsible for the collection and review of information and intelligence from USMS districts, through its liaisons with other federal law enforcement entities, and from other sources. Additionally, this branch is responsible for oversight of the USMS program involving its representatives assigned to the Federal Bureau of Investigation's (FBI) Joint Terrorism Task Forces (JTTF).[15]

As of July 2007, the Intelligence Branch had six full-time staff assigned. One Branch Chief and a JTTF Program Coordinator operate out of USMS headquarters. In addition, four Inspectors were assigned as full-time liaisons with other federal law enforcement entities. These Inspectors coordinate with the FBI's National Joint Terrorism Task Force; the FBI Washington Field Office's JTTF; the Federal Bureau of Prisons' Sacramento Intelligence Unit; the Supreme Court Police; the U.S. Capitol Police; the District of Columbia Metropolitan Police Department; and the Department of Homeland Security Office of Intelligence and Analysis.[16]

In addition to assigning full-time liaisons to these law enforcement agencies, the USMS also has established other contacts and working relationships to obtain and share information with the U.S. Secret Service; the Central Intelligence Agency; the National Security Agency; the Department of State's Diplomatic Security Service; the Defense Intelligence Agency; the Pentagon Force Protection Agency; the Drug Enforcement Administration; the Bureau of Alcohol, Tobacco, Firearms and Explosives; the Federal Air Marshal Service; the Transportation Security Administration; Immigration and Customs Enforcement; Customs and Border Protection; and numerous state and local fusion centers, such as those in Virginia, New York, and Texas.[17]

---

[15] In September 2006, the USMS formalized its JTTF Program to collect and disseminate pertinent and timely intelligence to best support USMS core missions and programs. There are currently over 100 FBI JTTFs operating throughout the United States. Each JTTF includes members from federal, state, and local law enforcement organizations. The JTTFs are intended to enhance the collection and sharing of information and intelligence, and to work on specific FBI domestic and international terrorism investigations. The USMS began participating on JTTFs in July 2001 when it entered into a Memorandum of Understanding with the FBI.

[16] One additional position is assigned to the Department of Homeland Security and reports directly to the Deputy Assistant Director for the JSD.

[17] Fusion centers blend relevant law enforcement and intelligence information analysis and coordinate security measures to reduce threats in local communities. (Cont.)

Threat Management Center

At the time of the OIG review, the Threat Management Center was not yet operational, but was scheduled to initiate operations on September 14, 2007. It is organizationally located in the JSD and will eventually be staffed 24 hours a day. The Threat Management Center will initially be staffed by Investigations Branch personnel, but six Inspector positions have been requested for FY 2008 to permanently staff the Threat Management Center. The Threat Management Center is housed within a sensitive compartmented information facility so that information classified as Top Secret can be analyzed and retained. The Threat Management Center will serve as the single point of entry for the reporting of all threats, inappropriate communications, incidents and suspicious activities from the 94 USMS districts and 12 judicial circuits as well as from other law enforcement agencies. According to the USMS, the Threat Management Center will conduct record checks and provide recommendations for protective investigations to the districts. Once the Threat Management Center is operational, the USMS will internally review and assess its capabilities, then create, revise, and formalize the necessary policies and procedures to ensure its effective operation.

**USMS District Operations**

When a USMS district has either identified or had an inappropriate communication or threat reported to it by a member of the judiciary, the initial information gathered during the protective investigation is entered into WIN/JDIS and forwarded electronically to the OPI for research and analysis. The districts are responsible for conducting protective investigations and determining the threat management strategy needed to reduce or control any potential risk to protectees. The district offices are also responsible for making the final assessment of the level of risk.

In the districts, Judicial Security Inspectors oversee the protective investigations, which are conducted by District Threat Investigators.

Judicial Security Inspectors

In FY 2002, Congress appropriated funding for hiring 106 new Judicial Security Inspector positions within the 94 judicial districts and

According to the Department of Homeland Security, fusion centers provide critical sources of unique law enforcement and threat information and facilitate sharing information across jurisdictions and function.

the 12 circuit courts.[18] Judicial Security Inspectors are senior-level Deputy Marshals that:

- investigate or supervise protective investigations conducted by District Threat Investigators involving threats to the judiciary;
- assist the district in planning for all high-threat trials and events;
- assist in the preparation of operational plans and security at district off-site judicial events;
- conduct security briefings and training for members of the judiciary;
- conduct off-site security briefings and reviews for members of the judiciary; and
- act as the USMS contracting officer's technical representative for the Court Security Officer contract to monitor compliance and performance standards in their respective districts.

District Threat Investigators

The District Threat Investigators, in consultation with the district Judicial Security Inspectors, conduct protective investigations into inappropriate communications or threats made against USMS protectees. The District Threat Investigator's primary goal is to devise and implement a threat management strategy to mitigate any potential risk to the protectee.

According to the USMS, as of March 2007 there were 338 Deputy Marshals who had been designated as District Threat Investigators in the 94 districts. The number of District Threat Investigators in a district ranges from 1 to 10 with an average of 4 per district. Because of staffing levels, multiple USMS missions, and variations in the number of reported threats in a district, in some districts the District Threat Investigator duty is a collateral duty. Of the 338 District Threat Investigators, 55

[18] The 94 district Judicial Security Inspectors report directly to the U.S. Marshal or Chief Deputy U.S. Marshal in their assigned district. The 12 Circuit Court Inspectors report to the Chief, Office of Protective Operations, Judicial Security Division. The Judicial Security Inspector Program became operational in May 2003.

have been designated as full time, and 283 performed the District Threat Investigator function as a collateral duty.

**USMS Threat Management Program**

Upon being notified of a suspicious activity, event, or communication, the District Threat Investigator makes the initial determination whether it meets the criteria of an inappropriate communication or threat. If it meets the criteria, the district Judicial Security Inspector and District Threat Investigator work as a team to implement the USMS's threat management program, which involves three elements:

- A *protective response* – The threat management process begins with the district determining and taking the necessary measures to ensure the protectee's immediate safety.

- A *protective investigation* – During a protective investigation, the District Threat Investigator and Judicial Security Inspector attempt to identify the subject, assess the threat, and mitigate the risk of harm to the protectee. The districts make the operational and tactical decisions involving the protection and management components of each threat case.

- A *threat assessment* – The district notifies the OPI of inappropriate communications and threats by opening a case file in WIN/JDIS and entering information gathered during the protective investigation. Based on the investigative information provided, the OPI conducts research and analysis to compare and evaluate the current inappropriate communication with the characteristics of similar types of closed threat cases. The resulting OPI threat analysis provides data to assist the district in determining the appropriate threat level and protective response. The district makes the final threat assessment.

<u>Interim Protective Measures</u>

While an inappropriate communication is being assessed by the OPI, the district determines what level or type of protective response is appropriate based on the information known. Some steps the district may take are:

- briefing the protectee (and family) on security awareness issues;

- updating or completing a judicial personal profile with details about the protectee that the district may need to provide protection;

- initiating or updating a residential security survey;

- installing electronic security measures; or

- arranging for local law enforcement to conduct or increase patrols around the protectee's residence.

After assessing the risk and using risk-based standards, USMS district officials also may initiate a protective detail. The districts are responsible for providing Deputy Marshals, administrative support, and any other resources needed during the first 72 hours of a protective detail. If the protective detail lasts longer than 72 hours, the districts may request additional staffing and funding from the JSD's Office of Protective Operations. The office reviews protective detail funding and staffing requests to ensure the appropriate protective and investigative measures are maintained.

Protective Investigations

A protective investigation is the systematic collection and assessment of available information to determine the individual's or group's true intent, motive, and ability to harm or pose a threat to a USMS protectee. A protective investigation begins immediately at the district upon receipt of an inappropriate communication or threat.

The USMS and the FBI both have responsibility for assessing and investigating threats. The USMS directives state that the USMS reports all threats to the FBI, which has the primary responsibility for conducting criminal investigations of threats to USMS protectees for the purpose of prosecution.[19] The USMS conducts protective investigations that focus on mitigating the potential for harm to a protectee, regardless of the possibility for prosecution. If a protective investigation determines

[19] A criminal investigation focuses on the collection of evidence that shows that the individual made a threat. The FBI conducts the criminal investigations, though in some instances, it may decline to proceed and the USMS conducts the investigation. A protective investigation by the USMS can run concurrently with a criminal investigation and can continue after the criminal investigation is closed. The goal of a criminal investigation is to prosecute, and the goal of a protective investigation is to mitigate the threat.

that a threat is likely to be carried out, the district develops a plan that incorporates a range of tactics and strategies designed to identify, assess, and mitigate any potential risk of harm to a protectee. Tactics may include:

- arresting the individual,
- having the individual committed for psychiatric care or observation,
- ensuring the individual is taking prescribed medications,
- obtaining a restraining order, or
- monitoring the individual through frequent contact (in-person or telephonic).

Threat Assessments

The district prepares an investigative report on a USM-550 form and forwards it to the OPI for research and analysis to assist the district in making an assessment.[20] District personnel also create a case record and enter investigative information and any details, including any supporting documentation (such as photographs), directly into WIN/JDIS. Once the initial case information is in WIN/JDIS, the district uses the system to manage and monitor the progress of the case. District management can also use the system to track and generate reports of how many inappropriate communications have been received, investigated, and closed. Any subsequent information gathered by the district during the protective investigation is entered into the WIN/JDIS record and is also provided to the OPI on a USM-11 form.[21]

OPI staff may be asked to confirm that the communication meets the criteria required for an inappropriate communication. If the criteria are met, the OPI begins its analysis (see Figure 3). The process starts with queries of specific agencies and databases, including the U.S. Secret Service's threat database (called TAVISS), to determine whether the

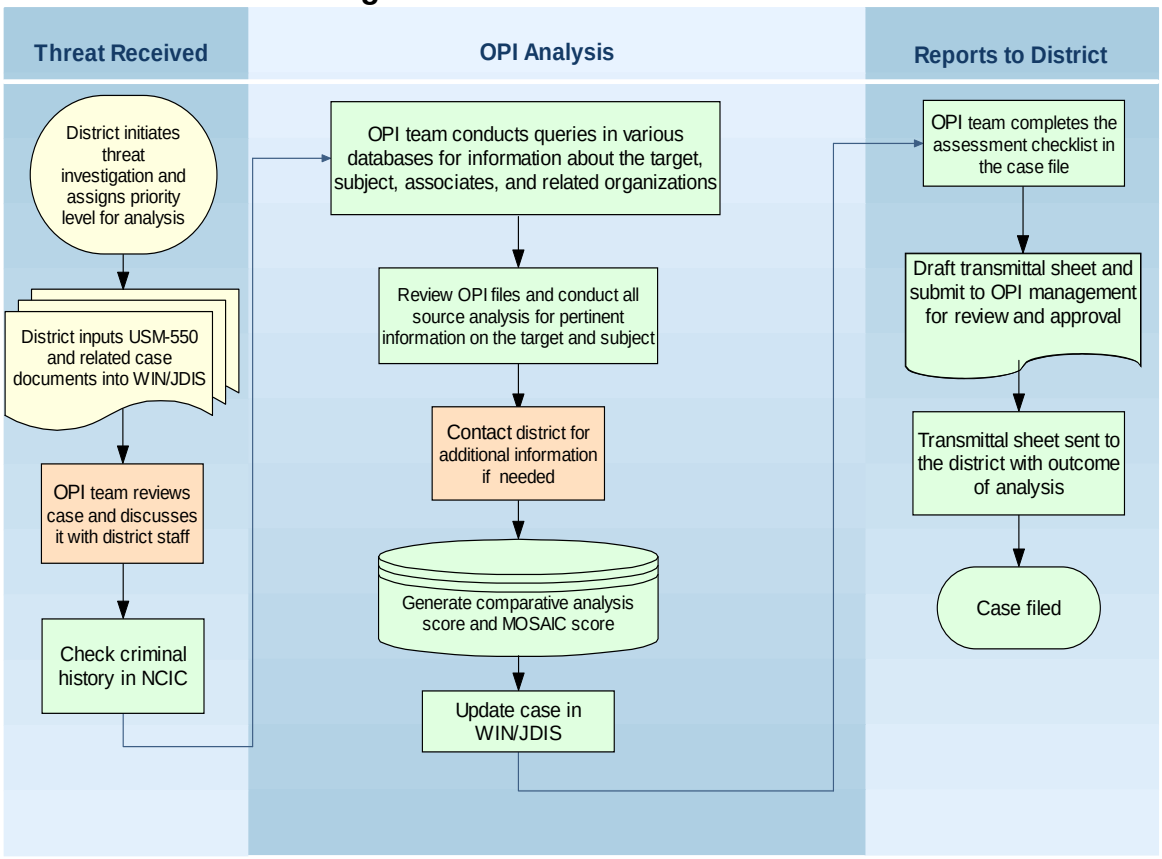
[20] The USM-550 Preliminary Threat Report is a form is submitted by the district in conjunction with a WIN/JDIS entry during the process of initiating a protective investigation. The USM-550 supplements the data in WIN/JDIS so that the OPI can conduct a more thorough threat analysis.

[21] The USM-11 Report of Investigation is a form submitted by the district to update information on a previously reported inappropriate communication.

individual or group has made previous threats or has any law enforcement records. These queries may provide information about the individual's or group's possible intent, motive, or ability to carry out the threat.

JSD managers told us that for cases that are "more serious or threatening," they have established a "major case category." Some of the criteria for these cases are (1) the threatener continues to demonstrate intent, motive, and ability; (2) the threatener is being released from custody following a conviction for threats, stalking, or assault on a USMS protectee; or (3) the threat involves mass mailings crossing over several districts. For major cases, the district closes the case in WIN/JDIS, and OPI staff reopen the case using a new case code and assume management of the case. OPI staff routinely notify other districts of threateners that send mass mailings and that are active in multiple districts.

**Figure 3: OPI Threat Assessment Process**




Source: USMS

The OPI conducts two computer-based analyses using the information from the district and its database queries. The first analysis is a comparative analysis that compares the case's known characteristics with previous threat cases maintained in the USMS's historical threat database. This database contains inappropriate communications and threat cases that have been closed and assigned an outcome of false, enhanced, or violent. The result of the comparative analysis is expressed in a score that indicates how closely the characteristics of the case being assessed match those of prior cases.

The second analysis is called a MOSAIC assessment. Using the investigative information to answer established questions about the case being assessed, the OPI applies the MOSAIC proprietary software to produce a numerical rating and information quotient. The numerical rating is expressed on a scale of 1 to 10. The higher the rating, the more the case under review resembles past cases that have escalated or resulted in violence. The information quotient, which is expressed on a scale of 0 to 200, is based on the number of questions that have been answered by the investigation at that point. The more questions that have been answered, the more reliable the result.

Once the two analyses have been completed, the record in WIN/JDIS is updated with the scores, and the results are sent to the district. The two analyses should have similar outcomes. If the comparative analysis score indicates low risk, then the proprietary analysis score should indicate low risk as well. When the two analyses do not show a similar outcome, the OPI can attempt to resolve the disparity by requesting additional investigative information from the district and reassessing the threat, or it can provide possible explanations for the disparity to the district.

The district can use the scores to help determine if the necessary protective measures have been taken and if the protective investigation is on the correct path. If significant new information on the case is collected during the course of the protective investigation after the assessment scores have been disseminated, the district can request that the OPI reassess the threat. The USMS has indicated that both scores are viewed as "tools" to assist the district in making a determination of the potential risk the threat does or does not present to the protectee.

The OPI expects to depart from reporting only the scores that result from this process at the end of FY 2007. OPI officials said that beginning in October 2007, they will work more collaboratively with the districts on assessing threats over the length of the protective

investigations through an ongoing exchange of information between the District Threat Investigator and the investigator/analyst team in the OPI.

**March 2004 OIG Report on Judicial Security**

In our March 2004 report, we evaluated the USMS's efforts after September 11, 2001, to improve its protection of the federal judiciary. 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 when they are away from the courthouse. We found that:

- The USMS had placed greater emphasis on judicial security by hiring 106 Judicial Security Inspectors and increasing courthouse security.

- The USMS assessments of threats against members of the federal judiciary were often untimely and of questionable validity.

- The USMS had a limited capability to collect and share intelligence on potential threats to the judiciary from USMS districts, the FBI's JTTFs, and other sources.

- The USMS lacked adequate risk-based standards for determining the appropriate protective measures that should be applied to protect the judiciary against identified potential risks during high-threat trials and when protectees are away from the courthouse.

Consequently, the OIG made six recommendations to the USMS:

1. Ensure that all threats to the judiciary are assessed within established time frames.

2. Update the historical threat database or develop a new database to perform comparative assessments.

3. Assign full-time representatives to all 56 FBI field office JTTFs and ensure effective USMS liaison with other intelligence agencies.

4. Create a centralized capability to identify, collect, analyze, and share intelligence.

5. Ensure that all Chief Deputy Marshals and all JTTF representatives have Top Secret clearances and ensure that each district has operational secure communication equipment.

6. Revise USMS guidance to establish risk-based standards and require after-action reports for high-threat trials and protective details.

The USMS concurred with all six of the recommendations 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 OPI; increased the number of Top Secret security clearances and secure communications equipment in the districts; and issued revised judicial security directives that included risk-based standards and after action reports.

## PURPOSE, SCOPE, AND METHODOLOGY OF THE OIG REVIEW

In this review, we examined the USMS's progress since our March 2004 report in improving its capability to collect, analyze, and disseminate information and intelligence related to protecting the judiciary. This review also assessed the progress the USMS has made in implementing corrective actions to address the recommendations made in our March 2004 report. Lastly, this review examined the status of initiatives or organizational changes that the USMS has recently undertaken to improve its capacity to identify and respond to threats and provide protection to the judiciary, including the installation of home alarms for judges.

As described below, the methodology used in this review included interviews of USMS personnel and members of the judiciary. We also conducted surveys of all federal judges and all Judicial Security Inspectors. We attended a protective investigative training course conducted by the USMS. We also reviewed USMS reported threat data and documents related to judicial security.

### Interviews

To examine the USMS judicial security efforts and activities, we interviewed USMS officials from headquarters, the JSD, and the Investigative Services Division. We also interviewed officials outside of the USMS. In total, we interviewed 29 individuals.

At the USMS headquarters, we interviewed the USMS Director, the Deputy Director, and the Chief of Staff. At the JSD, we interviewed the former and current Assistant Directors, the Deputy Assistant Director for Judicial Services, and the Deputy Assistant Director for Judicial Operations. Within the OPI, we spoke with the former and current Chiefs of the OPI; the Assistant Chief, Investigations Branch; two analysts and one Inspector assigned to the Investigations Branch; the Assistant Chief, Intelligence Branch; the Joint Terrorism Task Force Coordinator; and three Inspectors designated as liaisons to task forces assigned to the Intelligence Branch. We interviewed three Chief Inspectors assigned to the former Operational Support Team. We also interviewed the Assistant Chief, Office of Courthouse Management, responsible for the Home Intrusion Alarm Initiative. At the Investigative Services Division, we interviewed the Deputy Chief of the Technical Operations Group and the Chief of its Tactical Support Branch.

Outside of the USMS, we interviewed the federal judge who currently chairs the U.S. Judicial Conference Committee on Judicial Security and the federal judge who formerly chaired the U.S. Judicial Conference Committee on Security and Facilities. At the Administrative Office of United States Courts (AOUSC), we interviewed the Assistant Director, Office of Facilities and Security, and the Chief and the Deputy Chief of the Court Security Office.

**Surveys**

The OIG surveyed all federal judges and 82 Judicial Security Inspectors assigned to USMS district offices.

Judicial Survey

With the cooperation of the AOUSC and the federal judiciary, we conducted a voluntary web-based survey that was e-mailed to 2,141 federal judges. Prior to distributing the survey, we received comments or suggested additions from the USMS, the AOUSC, and 10 federal judges serving on the Judicial Conference Committee on Judicial Security. The OIG conducted the survey to obtain the federal judiciary's views and opinions on the current status of security provided to federal judges. The OIG also sought judicial observations and perspective that would provide the USMS with ideas, methods, or data for improving judicial security. The survey contained 29 questions. The survey period started on October 16, 2006, and ended on November 3, 2006. Of the 2,141 federal judges, a total of 705 (32 percent) responded.[22] The judicial survey results appear in Appendix II.

Judicial Security Inspector Survey

We also conducted a telephone survey of 82 of the 92 USMS district Judicial Security Inspectors.[23] The survey instrument asked for each Judicial Security Inspector's perspective regarding various policies and procedures on threat investigations, protective details, and the information they received from the OPI concerning judicial threat

[22] The total number of judicial responses was well above the 327 required for statistical validity, based on a confidence level of 95 percent and a confidence interval (margin of error) of ±5 percent.

[23] Two of the 94 district positions were vacant at the time of our survey. While we contacted all 92 Judicial Security Inspectors, 10 did not respond to the survey.

investigations and security operations. The survey contained 73 questions. The survey period started on November 24, 2006, and ended 4 days later. The Judicial Security Inspector survey results appear in Appendix III.

**Site Visits**

We attended the 40-hour USMS Protective Investigations Training Program course conducted at the Federal Law Enforcement Training Center in August 2006. The course content was designed to provide Judicial Security Inspectors and District Threat Investigators instruction in areas such as protective investigation policy and new USMS directives; overviews of various USMS entities and their capabilities; reporting requirements; and threat management strategies.

**Data and Document Reviews**

We reviewed and analyzed reported threat data maintained by the USMS in its WIN/JDIS database for FYs 2005, 2006, and the first half of FY 2007.[24] After selecting a random sample from each fiscal year, we reviewed the data to determine USMS adherence to its revised timeliness standards for threat assessments. To calculate timeliness, we identified the date that the OPI received the threat from the date embedded in the assigned warrant number for each case and counted the number of days between that date and the date when the OPI provided the district office with the assessment results. Weekends and holidays were removed for the analysis. The USMS's established time standards, depending on the level of threat, were used as the criteria for determining timeliness.

We also reviewed relevant USMS Directives, policies and procedures, manuals, training materials, clearance rosters, and examples of OPI information products.

[24] We did not analyze the threat data for FY 2004 because the USMS used a different timeliness standard then.

## Assessing Reported Threats

**From the issuance of the OIG's first report on judicial security in March 2004 through FY 2006, the USMS made little progress with improving its assessments of threats against the judiciary. The USMS did not meet its timeliness standards for conducting threat assessments, and over half of the threats reported by USMS districts were never assessed, resulting in a backlog of 1,190 "pending" threats awaiting assessment as of October 1, 2006. Moreover, the USMS did not track the timeliness of threat assessments.**

**However, in early FY 2007, USMS headquarters initiated a review of the pending cases and assigned additional resources to complete the outstanding cases. By May 2007, the USMS had eliminated the backlog of pending threat assessments. The additional resources also enabled the USMS to assess new threat reports more quickly during the first half of FY 2007. Yet, USMS headquarters managers and district staff believe the current threat assessment process is of limited utility for protective investigations because it does not provide sufficient information about a threatener's behavior. USMS managers told us they plan to change the threat assessment process in FY 2008.**

In our March 2004 report, the OIG determined that USMS headquarters did not meet its timeliness standard of assessing threats within 24 hours after receipt from the districts for 73 percent of the threat assessments it conducted in FYs 2000 through 2003. To ensure the most serious threats were assessed on a timely basis, after 2003 the USMS began designating reported threats as either "expedite" or "standard" and, in August 2004, the USMS established longer timeliness standards of 3 business days for expedite cases and 7 business days for standard cases. We also reported that the threat assessments were of questionable validity.

In this section, we examine the USMS's effort to improve its performance under its revised timeliness standards in FY 2005 and

FY 2006; an FY 2007 effort by the USMS to monitor timeliness and resolve a large backlog of cases that accrued in FY 2005 and FY 2006; and the USMS's plans to revise the threat assessment process in FY 2008 and improve the quality of its assessments.

Timeliness of USMS assessments of reported threats decreased during FY 2005 and FY 2006.

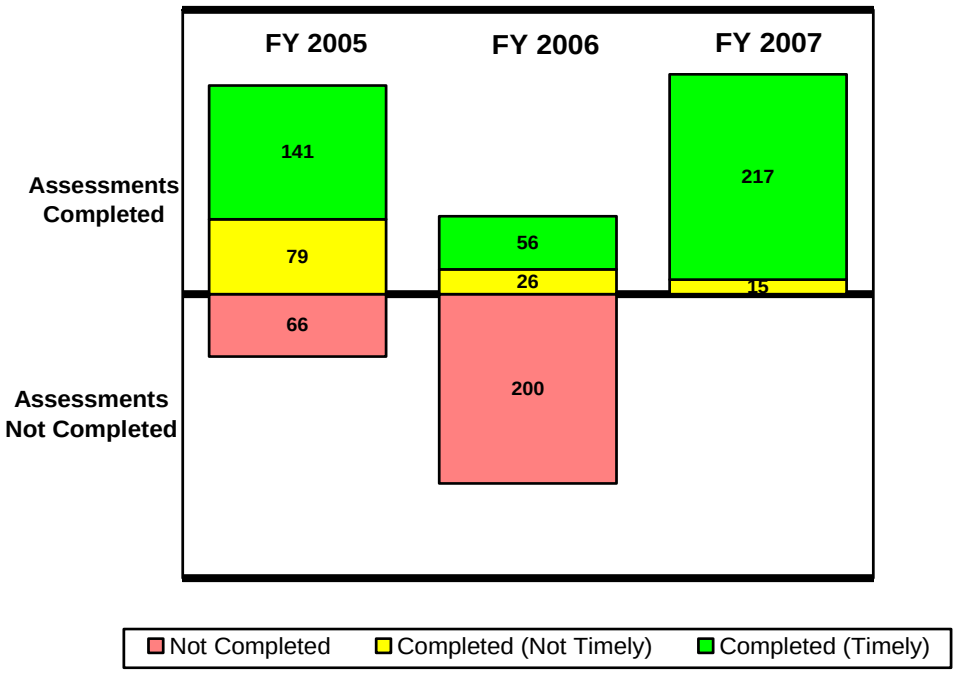
In FY 2005 and FY 2006, the USMS failed to improve the timeliness of its threat assessments. We reviewed a sample of 568 of the 2,018 threats reported to USMS headquarters in FY 2005 and FY 2006. We found that although the USMS extended its timeliness standard from 24 hours for all cases to 3 days for expedited cases or 7 days for standard cases, the OPI failed to meet those standards in about two-thirds of all cases in our sample.[25] Moreover, the USMS did not complete threat assessments on more than half of all threats reported in FY 2005 and FY 2006, which led to a backlog of 1,190 "pending" assessments as of October 1, 2006.

For each year, we examined how many of the threat assessments met the timeliness standard for the applicable category. We also examined the average time it took the USMS to assess reported threats. We found that the OPI took longer to process both expedited and standard cases in FY 2006 than it did in FY 2005.

Chart 2 illustrates the OPI's improvement in assessing the reported threats in our sample in FY 2005, FY 2006, and the first half of FY 2007.

[25] The USMS does not count weekends and holidays when determining timeliness of the threat assessment.

**Chart 2: OPI Assessment of Reported Threats in FY 2005, FY 2006, and FY 2007**




Source: OIG

FY 2005. We selected a random sample of 286 threats reported to the OPI in FY 2005 and found that the USMS had completed assessments for 220 of the cases (77 percent). As of November 3, 2006, when the USMS provided data on its operations to the OIG, the USMS had still not conducted threat assessments on 66 of the cases (23 percent), which remained in a "pending" status at the time of our analysis.[26]

We next analyzed whether assessments were completed within applicable timeliness standards based on the case category. Of the 286 cases, 14 were categorized as expedited and 195 were categorized as standard. Eleven threats that had been processed and all 66 of the pending cases were not categorized as either expedited or standard. We found that 141 of the threats were assessed within the applicable 3-day

[26] The USMS uses the term "pending" to describe those cases for which the OPI has completed no comparative analysis or MOSAIC assessments.

or 7-day timeframe.[27] Another 79 threat assessments were completed but not within the applicable 3-day or 7-day timeframe.[28] The 66 cases that were pending as of November 2006 were at least 13 months old and so failed to meet either timeliness standard.

FY 2006. Our random sample of 282 cases reported to the OPI in FY 2006 found that the USMS had completed assessments for only 82 of the cases (29 percent). The remaining 200 threats (71 percent) were still pending as of November 3, 2006. Of the 82 threats that had been assessed, 9 were categorized as expedited and 73 were categorized as standard. We found that 56 of the threats were assessed within the applicable 3-day or 7-day timeliness standard.[29] Another 26 threats had been assessed, but the assessment was completed later than the applicable 3-day or 7-day standard. The 200 cases that were pending as of November 2006 were at least 1 month old and so failed to meet either timeliness standard.

OPI managers attributed the increase in time to the increasing number of reported threats and the OPI's inability to hire additional qualified analytical staff, specifically Intelligence Research Specialists.

The USMS made efforts to improve processing timeliness in FY 2007.

In early FY 2007, the USMS initiated several actions to improve its ability to monitor threat assessments and to resolve the backlog of 1,190 pending cases. An OPI manager told us that, beginning in FY 2007, the USMS dedicated additional staff, including investigators, to perform threat assessments. According to OPI management, the OPI had two analysts conducting threat assessments in FY 2005 and 2006. A third analyst was hired in late FY 2006. Also, the OPI began to identify and

[27] The 141 assessments completed within established timeliness standards in FY 2005 included 13 of the 14 expedited cases that were assessed within 3 days (average: 0.5 day) and 122 of the 195 standard cases that were assessed within 7 days (average: 14 days). We also considered six of the uncategorized cases that were assessed in under 7 days to have met the timeliness standard.

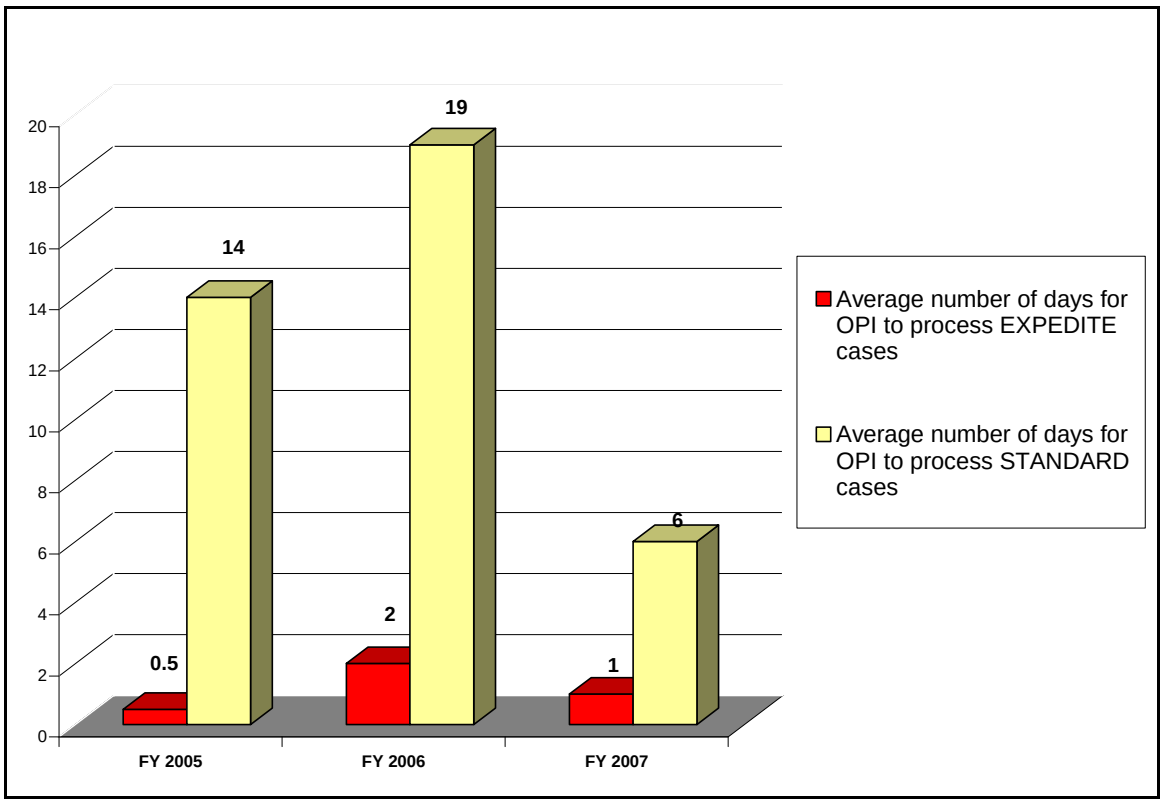
[28] This includes 1 threat categorized as expedited, 73 threats categorized as standard, and 5 threats that were not categorized but that were not assessed within 7 days.

[29] The 56 assessments completed within established timeliness standards in FY 2006 included 7 of 9 expedite cases that were assessed within 3 days (average: 2 days), and 49 of 73 standard cases that were assessed within 7 days (average: 19 days).

process pending threat assessments that were still needed by the districts and implemented procedures to begin monitoring the processing of threat assessments. Because the actions taken by the USMS were pertinent to addressing the problems we identified in our review of FY 2005 and FY 2006 threat assessments, we expanded the scope of our review to include the first half of FY 2007.

Chart 3 illustrates how many days it took, on average, for the OPI to assess each threat received in FYs 2005, 2006, and the first half of 2007, as reflected by our random samples.

**Chart 3: Average Number of Days for OPI to Assess Cases in FYs 2005, 2006, and First Half of 2007**




Source: OIG analysis of a random sample of cases provided by the USMS

Processing of threat assessments improved. We found that the actions taken by the USMS enabled it to assess reported threats more quickly in FY 2007. According to USMS data, the districts reported 590 threats during the first two quarters of FY 2007. We randomly selected 232 cases for review and found that the USMS had conducted

assessments for all 232 of the cases.[30] Further, our analysis showed that 93 percent of the threat assessments were completed within applicable timeliness standards. Of the 232 threats, 3 were categorized as expedited and all were assessed within 3 days. The remaining 229 were categorized as standard, and 214 were assessed within 7 days. For our FY 2007 sample of 232 cases, it took an average of 6 days to conduct a threat assessment.

The USMS eliminated its backlog of pending threat assessments. On October 1, 2006, the OPI identified l,190 threats that had not been assessed. The OPI contacted the districts that reported the threats to determine the status of the investigations related to each of the 1,190 pending assessments. District personnel reviewed the cases and informed the OPI whether each case had been closed or whether the district still considered the case active and therefore still required a threat analysis from the OPI. The OPI determined that analyses were still required for 538 of the 1,190 cases and, by March 2007, had completed the analyses and disseminated the results to the districts. For the remaining 652 threats, the OPI determined that the districts had already closed their investigations. These cases were then "administratively closed" by the Assistant Director of the JSD.[31] This effort was completed in May 2007, at which time the USMS no longer had any pending threat analyses.

The USMS began monitoring threat assessment timeliness and quality in FY 2007. In response to the OIG's March 2004 finding that 73 percent of threat assessments conducted during FY 2000 through FY 2003 did not meet timeliness standards, the USMS stated:

> The USMS will be revising its policy on time frames for the ASU [Analytic Support Unit] to complete assessments. The new policy will establish criteria that categorize requests according to urgency. **Once the policy is implemented, adherence to the time frames will be made a factor in the annual performance evaluations of the ASU staff.** The USMS estimates that the new policy will be implemented by the end of August 2004. The USMS will also review the

[30] We originally selected 233 cases and found 1 case for which no assessment was conducted. However, we determined that case to have been a reporting error and excluded it from our sample.

[31] The administrative closure was annotated in the case file in WIN/JDIS and a memorandum from the Assistant Director was placed in the actual case file.

workload of the ASU and will request additional resources during the FY 2006 budget process if necessary.[32] [emphasis added]

Despite that plan, the USMS did not monitor the timeliness of threat assessments during FY 2005 and FY 2006. The USMS also did not modify WIN/JDIS to enable it to better manage threat assessment processing. As currently configured, WIN/JDIS cannot be used to automatically calculate elapsed time or determine whether the elapsed time meets established standards because it does not contain dedicated data fields for this information.[33] Because of WIN/JDIS's limitations, calculating the time taken to complete an assessment and determining whether the assessment met USMS standards must be done manually.[34] Further, data needed to determine timeliness is often missing from WIN/JDIS. For example, in our sample of 568 threats reported in FY 2005 and FY 2006, 274 (48 percent) were not identified as either expedited or standard cases.

In late 2006, OPI management implemented procedures to manually monitor the timeliness and quality of threat assessments. Data from each case is now entered by the Inspector or analyst responsible for the analysis into a spreadsheet for management review. At the conclusion of the research segment of the threat assessment process, the responsible staff initials a checklist maintained in the case file to document that all steps required to complete the research have been accomplished. OPI managers then review the case file to determine the timeliness of the research, review all information from the district, and direct the investigator or analyst to obtain any additional information from the district deemed necessary for a comprehensive assessment. After OPI management ascertains the research is adequate, the OPI transmits the assessment scores to the originating district for use in its protective investigation. OPI managers told us that they

[32] Prior to the establishment of the OPI in June 2004, analysts assigned to the Analytical Support Unit within the Investigation Services Division were responsible for conducting threat investigations at USMS headquarters.

[33] The information to calculate timeliness may be present, but the calculation cannot be automated even when the information is included. For example, the date a threat assessment is forwarded to the OPI is embedded within the case file number and must be extracted. The case category and assessment completion date, if entered, are contained (along with other information) in a text-based remarks field.

[34] The OIG manually calculated the number of elapsed days for each threat to determine the number of days it took to complete each threat assessment.

believe that the improvement in threat assessment timeliness in the first half of FY 2007 is directly attributable to the implementation of this oversight mechanism.

The USMS plans to revise the threat assessment process in FY 2008.

During our review, USMS managers told us that threat assessments produced under the current process were of limited utility to support protective investigations in the districts because they do not provide sufficient information about the threatener's behavior. Further, responses to our Judicial Security Inspector survey confirmed that threat assessments infrequently provide information that affects how protective investigations are conducted. Because of the deficiencies in the current process, USMS management told us that they plan to change the threat assessment process in FY 2008 so that it provides better information and continuing support from the OPI to District Threat Investigators for the duration of protective investigations. In the following paragraphs, we discuss the perceptions expressed to the OIG regarding the usefulness of the current threat assessment process and the USMS's plans for changing the process.

We noted an apparent contradiction between our survey results and actual OPI performance that we believe indicates that Judicial Security Inspectors did not highly value the OPI's threat assessments. When we asked the Judicial Security Inspectors whether they received threat assessments from the OPI in time to assist them in conducting protective investigations, a large majority (80 percent) stated that they did.[35] However, as we discussed previously, the OPI failed to complete threat assessments on about half (1,190 of 2,018) of the threats reported to it during FY 2005 and FY 2006. We believe the dissonance between the Judicial Security Inspectors' stated belief that they received timely threat assessment results and the fact that they did not receive assessments for half of the threats they reported to the OPI indicates that Judicial Security Inspectors placed only limited value on threat assessments in their protective investigations.

The OPI is planning to implement a new threat assessment process. In a memorandum dated March 30, 2007, the Assistant Director of the JSD informed the OIG that the USMS will "move away from MOSAIC" and comparative analysis to "concentrate on the behavior

[35] Only 6 percent stated that they did not receive results in time to be useful to the protective investigation. The remaining 14 percent had no opinion.

of subjects who make threats and inappropriate communications." USMS managers further explained that the OPI is starting to employ a more collaborative method of working with the districts on protective investigations, threat assessments, and case management. As envisioned by USMS managers, the analytical steps carried out on reported threats will be revised, and the extent and duration of the OPI's involvement in protective investigations will increase.

Under the revised threat assessment process, districts will report all suspicious activities, inappropriate communications, and threats to the Threat Management Center. Once the initial records checks and recommendations for a protective investigation are provided to the district, the Threat Management Center staff will turn the case coordination over to the Investigations Branch circuit team responsible for protective investigations in its assigned circuits.

When a case is turned over to the Investigations Branch, it will be assigned to a team consisting of an analyst and an Inspector for evaluation. Through the use of the protective investigation case information supplied by the District Threat Investigator and further research and analytical work, the Investigations Branch team will develop a work product to send back to the district for consideration and use in its investigation. As described by OPI managers, the process of gathering information and providing feedback will continue until the OPI and the district determine the case can be closed.[36]

While each protective investigation is unique, OPI managers told us that they see the new process as an opportunity to further standardize, over time, the protective investigation process in each of the 94 districts. For example, the OPI will request that each District Threat Investigator provide certain core information to answer specific analytical questions so that higher-quality assessments can be produced. Because the OPI will ask the District Threat Investigators to obtain and provide consistent and complete investigative information, officials expect some uniform investigative work will be performed in each case. Further, the continuing dialogue between the OPI and the districts during the course of protective investigations could result in more consistently useful threat assessment products for the District Threat Investigators. The new process is also expected to achieve more consistent reporting of judicial security information. Under the existing threat assessment

[36] The final determination to close a case will remain the district's responsibility.

process, districts simultaneously notify the OPI and create a record in WIN/JDIS only after they determined that an event meets the criteria for an inappropriate communication. Under the new process, the districts will be expected to report any event or issue involving judicial security (including all suspicious activities, inappropriate communications, or threats) to the Threat Management Center as soon as possible.

The new threat assessment process OPI managers described to us could improve the ability of the USMS to assess and respond effectively to threats against the judiciary. However, OPI has not yet developed formal plans with defined milestones, tasks, and outcomes. OPI managers told us they have decided to eliminate the 3-day and 7-day timeliness standards. Instead, the Threat Management Center staff will provide the results of their analyses to the districts verbally or by fax and then follow up with a written response within 1 business day.

In August 2007, JSD managers told the OIG that they have drafted a new process for the Threat Management Center and an updated protective investigation policy, and that they planned to distribute the drafts to the districts. Because these drafts were not available for our review, we cannot fully evaluate the USMS's planning and implementation of the new process or assess the potential for the new process to improve the USMS's ability to respond to threats against the judiciary. The OPI needs to fully define the new process, provide direction to the districts, and provide training to district and headquarters staff involved in the judicial protection mission.[37]

[37] Although the new process has not been fully defined, the USMS told us that it has already conducted training on the behavioral aspects of this new approach. In July and August 2006, the USMS conducted 4 separate 1-week Protective Investigations Training courses focusing on behavioral methodologies of investigation for 190 Deputy Marshals at the Federal Law Enforcement Training Center. These seminars were provided by experts from the USMS, the Bureau of Alcohol, Tobacco, Firearms, and Explosives, the FBI, United States Attorneys' Offices, the U.S. Secret Service, and the Diplomatic Security Service. The USMS conducted 2 additional Protective Investigations Training courses for 96 Deputy Marshals in July 2007. JSD managers stated that they are working with USMS staff assigned to the Training Center to conduct four more courses in FY 2008.

## Identifying Potential Threats

**In response to the OIG's March 2004 report, in June 2004 the USMS established the Office of Protective Investigation to provide a centralized protective intelligence function for the judicial security mission. However, the USMS was slow to staff the protective intelligence function and has not developed a strategy to effectively collect, analyze, and share information on potential threats against the judiciary. Consequently, the USMS is still in the early stages of implementing a centralized program to collect information and analyze it to develop protective intelligence on potential threats.**

To identify and address the risk posed by individuals or groups who may not make overt threats to the judiciary in advance of an attack, in March 2004 the OIG recommended that the USMS create a centralized capability to collect, analyze, and share intelligence on potential threats. In 2005, separate reviews conducted by an Attorney General Working Group and a USMS committee examined the USMS judicial security mission and also recommended improvements to the USMS's protective intelligence capabilities. (See the text box on the next page for details.)

Our current review found the USMS is making slow progress at implementing a protective intelligence function to identify potential threats. Three years after the OPI was established, it still lacks the staff needed to gather and analyze information to effectively develop protective intelligence. During the past 3 years, the USMS has made some improvements to its capacity for collecting information, including secure equipment and a new facility for working with classified information. However, the OPI still does not systematically collect and analyze information from its districts; from other federal, state, and local law enforcement agencies; or from the courts to produce protective intelligence about potential threats to the judiciary. Although the Assistant Director of the JSD identified a wide range of capabilities scheduled to be implemented in the Intelligence Branch over the next 2 years, the OPI lacks plans for achieving these capabilities.

**Two 2005 Reports Identify the Need to Improve the USMS's Protective Intelligence Capability**

In 2005, the Department and the USMS conducted separate reviews of the USMS judicial security mission and made recommendations for improving the protective intelligence function to identify potential threats.

Attorney General Judicial Security Working Group. In a June 2005 report, this Working Group called for the USMS to develop "a first-rate system of intelligence gathering and threat assessment which the Marshals Service currently lacks" and recommended improvements in information sharing with the judiciary and other law enforcement agencies. On September 15, 2005, the Attorney General informed the Chairman of the Executive Committee of the Judicial Conference of the United States that he had directed that the USMS implement the Working Group's key recommendations. Specifically, he stated that he directed the USMS to increase the OPI's staff and resources "to enhance the USMS's ability to collect, analyze and store and retrieve intelligence and information, and to share that intelligence and information promptly and effectively within the USMS and with our Federal, state and local partners."

USMS Judicial Threat and Analytical Assessment Commission. In the fall of 2005, the Acting Director of the USMS established the Commission and directed it to:

> assess the current methodology and capability of [the USMS's] judicial threat intelligence and protective investigation programs; to determine what support services and assessment activities are needed for field managers to make informed decisions regarding judicial security operations; and to make substantial recommendations regarding policies, process, and functions of the newly developed Office of Protective Intelligence.

In December 2005, the Commission made 22 recommendations, including that the USMS provide additional staffing for the OPI; that the OPI work closely with federal, state, and local law enforcement, including full-time USMS representation with Top Secret clearances on JTTFs; and that the USMS provide the OPI with the equipment necessary to receive and transmit classified information expeditiously.

Developing a protective intelligence function is essential to meeting the security risks identified by judges and a Department study. To determine how federal judges viewed the risks associated with potential threats, we surveyed them about the types of threats that pose the greatest risk. In response, 527 out of 696 (76 percent) respondents reported that the unknown general danger associated with being a federal judge posed the greatest risk. In contrast, only 134 out of 696 (19 percent) reported that the known threat posed the greatest risk. The results of our survey are consistent with a 5-year study by the Department of Justice and the U.S. Secret Service of 83 individuals who

attacked or approached to attack a prominent public figure. This study documented that less than 10 percent had communicated a direct threat to their targets or a law enforcement agency. In the following sections, we discuss the efforts of the USMS to develop its capability to identify potential threats to the judiciary.

Three years after the USMS established the Office of Protective Intelligence, it is still not fully staffed.

In response to an OIG recommendation, on May 14, 2004, the USMS reported that it would establish the OPI on June 1, 2004, in the JSD. The OPI was directed to collect, analyze, and disseminate all intelligence relating to the safety of USMS protectees, employees, facilities, and missions. The OPI staff consisted of a Chief, three Criminal Investigators, and one Intelligence Analyst. In addition, the USMS stated that "a number of analysts from the Analytical Support Unit" would be reassigned to the office shortly thereafter. The USMS reported that the OPI's priorities were to (1) immediately develop a plan to transfer all threat analysis responsibilities from the Analytical Support Unit to the OPI, (2) prepare and propose an organizational and staffing plan, and (3) assist in preparing an FY 2006 budget submission that supported the creation and continuity of the OPI.

On April 26, 2005, the USMS stated to Congress that it had established the OPI "to analyze and disseminate protective intelligence," but added the caveat that "the availability of resources will determine the rate of progress with regard to staffing the office."[38]

On May 13, 2005, the OIG met with the Chief of the OPI to discuss the staffing and implementation of the office. We found that the assigned staffing level remained at the five positions that were transferred to create the office in June 2004. In July 2005, the USMS transferred responsibility for assessing reported threats from the Analytical Support Unit in the Investigative Services Division to the OPI. From May 2005 through July 2007, the USMS increased the OPI's staffing to 21, with 2 applicants under consideration. The additional resources were primarily assigned to the OPI's Investigations Branch, where they were directed at assessing reported threats, including the large backlog of pending assessments that accumulated in FY 2005 and FY 2006. The OPI only

[38] Statement of the United States Marshals Service before the Subcommittee on Crime, Terrorism, and Homeland Security, Committee on the Judiciary, House of Representatives, concerning H.R. 1751, *The Secure Access to Justice and Court Protection Act of 2005,* April 26, 2005.

recently began to dedicate staff to the collection, analysis, and dissemination of intelligence related to potential threats. According to JSD managers, when the Threat Management Center becomes operational and can receive classified information, more Intelligence Research Specialists will be assigned to the Intelligence Branch. OPI will assign dual responsibilities to other Intelligence Research Specialists to monitor classified intelligence and work protective investigations.

Within the OPI, the Intelligence Branch is responsible for collecting and analyzing information to develop protective intelligence on potential threats. As of July 2007, it was staffed by a branch chief, a JTTF program coordinator, and four Inspectors who serve as liaisons to other federal law enforcement agencies. However, no Intelligence Research Specialists were assigned to the Intelligence Branch.[39] Since the establishment of the OPI in June 2004, the USMS has increased from three to five the number of Inspectors assigned as full-time liaisons to other federal law enforcement agencies to collect information on potential threats to the judiciary.[40] In March 2007, the Assistant Director of the JSD told the OIG that the USMS plans to increase the number of liaisons assigned to other agencies further by FY 2009 if the JSD receives additional resources. JSD managers are developing reporting requirements for the liaisons, but they told us that the requirements will not be formalized or distributed until after the Threat Management Center is operational.

In addition, the USMS has not assigned full-time representatives to all JTTFs to improve access to information and intelligence related to judicial security. Assigning full-time representatives to all 56 FBI field office JTTFs was recommended in our March 2004 report. It was also recommended by the Attorney General's Working Group, and the USMS's

[39] OPI managers stated that the Intelligence Research Specialists in the Investigations Branch were available to assist the Intelligence Branch as needed to conduct research and disseminate information.

[40] The three liaisons that existed when the OPI was started were assigned to the Federal Bureau of Prisons' Sacramento Intelligence Unit, the Central Intelligence Agency, and the FBI's National Joint Terrorism Task Force. As of September 2006, the USMS had cancelled the liaison position at the Central Intelligence Agency, but maintained full-time liaisons to the Department of Homeland Security and the FBI's National Joint Terrorism Task Force and the Washington Field Office. The USMS also assigned a Senior Inspector to serve as a liaison to the Supreme Court Police, the U.S. Capitol Police, and the Metropolitan Police Department.

Judicial Threat and Analytical Assessment Commission in 2005.[41] The FBI has since increased the number of JTTFs to 101. The USMS actually reduced the number of full-time JTTF representatives from 25 to 17 after the issuance of our March 2004 report and reduced the number of part-time JTTF representatives from 25 to 23. During this period, USMS districts also began assigning liaisons to JTTFs. Unlike full- or part-time representatives, these liaisons do not work on a JTTF and do not have direct access to FBI databases. As of July 2007, USMS districts had assigned 39 liaisons to JTTFs. The USMS JTTF program coordinator in the OPI's Intelligence Branch monitors the program and receives and disseminates information, but has no operational authority over the representatives and liaisons the districts have assigned to the JTTFs. These representatives and liaisons report to the district management that assigned them.

**Judicial Security Information From JTTFs**

- A USMS JTTF representative reviewed an FBI report and concluded that several suspect individuals had crossed the U.S. southern border and were heading to a city where a high-threat terrorism trial was being held. This information was forwarded to the affected USMS district, which further coordinated trial security with the FBI.
- A threat against a U.S. Attorney was brought to the attention of a USMS JTTF representative by a JTTF member from another agency. He immediately reported the incident to the OPI.

The USMS improved its capacity for working with classified information.

To operate an effective protective intelligence function, USMS staff must have appropriate security clearances and the equipment and facilities required to store and work with classified information.[42] We determined that since our 2004 report, the USMS has increased the number of staff with Top Secret clearances:

- In 2004, 72 of 94 Chief Deputy Marshals (76 percent) had Top Secret security clearances. By February 2007, all 94 Chief Deputy Marshals had Top Secret clearances.

[41] In March 2004, the OIG recommended that the USMS assign full-time representatives to all 56 FBI field office JTTFs. The Attorney General's Judicial Security Working Group report made a similar recommendation that the Director of the USMS should strive to staff all of the JTTFs. In December 2005, the Judicial Threat and Analytical Assessment Commission report also recommended that the USMS assign full-time representatives to each of the 56 FBI field office JTTFs.

[42] In our March 2004 report, we recommended that the USMS require that all Chief Deputy U.S. Marshals and USMS JTTF representatives have Top Secret clearances and that each district have secure communications equipment.

- In 2004, 33 of 50 USMS JTTF representatives (66 percent) had Top Secret security clearances. As of February 2007, 37 of 43 full- and part-time JTTF representatives (86 percent) had Top Secret Clearances.

- As of February 2007, 29 of 37 new JTTF liaisons (78 percent) had Top Secret clearances; 70 of 91 district Judicial Security Inspectors (76 percent) had Top Secret clearances; and 17 of 18 OPI employees (94 percent) had Top Secret clearances.

The USMS also improved the facilities and equipment it has to work with classified information. In August 2003, 51 of the USMS's 94 districts had secure telephones for communicating classified information. By April 2005, the USMS reported to the OIG that all 94 districts had secure telephones. Also, as of July 2007, the USMS was nearing completion on construction and accreditation of a Threat Management Center housed in a sensitive compartmented information facility. The Threat Management Center will provide the OPI with the capacity to electronically receive, access, analyze, and disseminate Top Secret information related to judicial threats with other agencies.

The OPI has not developed the capability to systematically collect and analyze information to identify potential threats to the judiciary.

While the USMS has made some improvements to its capacity for collecting information, we found that the OPI's Intelligence Branch has not yet implemented a protective intelligence function to systematically collect and analyze information from the districts, from other federal, state, and local law enforcement agencies, or from courts to identify potential threats.[43] Specifically, the USMS has not defined the protective intelligence products it needs and has not developed a strategy for obtaining and analyzing information to produce and disseminate protective intelligence products. For example, we found that:

[43] OPI analysts in the Investigations Branch have generated some information products that are shared with the districts, including information bulletins, alert notices, and foreign travel briefs. The OIG reviewed 14 products provided by the USMS to determine whether they contained analytical information such as why the information provided was relevant to the judicial security mission, how the information could or should be used, and how the recipient should respond. We found that out of the 14 products, 9 had an analytical section, and 4 of the analytical sections contained analytical information.

- The OPI does not analyze information it receives on reported threats to detect national or regional patterns. Analyses that identified trends in the types of USMS protectees receiving inappropriate communications, threat delivery methods, and the types of threateners could help the districts allocate resources or identify areas that need improvement to address potential threats.

- The OPI does not routinely update case information on individuals who already have threat cases in JDIS by searching the U.S. Secret Service's threat database (called TAVISS) for new information.

- The OPI does not analyze data it collects on courthouse incidents. Judicial Security Inspectors and the Office of Court Security provide the OPI with reports of suspicious activities at and around federal courthouses.[44] However, the OPI does not analyze these reports to identify trends or patterns in suspicious activities that may indicate potential threats. JSD managers stated that they plan to initiate a Suspicious Activity Report database project between FY 2007 and FY 2009, depending on funding and staff availability. The project would merge the suspicious activity reports in the USMS's Court Security System into JDIS to develop a database of suspicious activities that can be analyzed to identify patterns and trends.

- The OPI does not systematically collect and analyze judicial security-related information that is available in federal, state, or local court databases, such as the AOUSC's Public Access to Court Electronic Records (PACER).[45] By analyzing PACER data and comparing it to case information in JDIS and TAVISS, the OPI could identify cases that may pose a risk for the federal judiciary. In our survey, federal judges identified the types of judicial proceedings that they believe generally pose a high risk

[44] In our survey of 82 Judicial Security Inspectors, 42 (51 percent) stated that, in addition to reporting threats, they sent the OPI other types of judicial security information, such as reports on indictments or arrests, courthouse incidents, information on domestic terrorist groups, and suspicious activities.

[45] The PACER system provides real time public access to case and docket information from Federal Appellate, District and Bankruptcy courts, including a listing of all litigants and judiciary involved in the case, case related information such as the nature of the suit, and the status of the case.

to judges' personal safety, such as criminal cases involving gangs, organized crime, terrorism, and perjury (see Appendix II).

- The USMS has not issued guidance on the type of judicial security information to be reported by district office personnel. Although the USMS has issued guidance on reporting inappropriate communications and threats to the judiciary, it has not issued guidance for the districts on reporting incidents such as suspicious activities. This could enable the USMS to proactively identify potential threats and augment existing knowledge of known threats. The Attorney General's Judicial Security Working Group report pointed out that because individuals who threaten public figures often switch targets, it is important to share information about individuals who have expressed violent intentions or an affinity for violence.

In April 2007, the Assistant Director of the JSD acknowledged to the OIG that the OPI was not focusing on potential threats because it still did not have sufficient staff resources. Although the OPI has not developed a protective intelligence capability to identify potential threats, we found that it does use some external information sources to identify potential risks to the judiciary. For example:

- The USMS liaison to the Federal Bureau of Prisons' Sacramento Intelligence Unit obtains information on when serious offenders who have threatened public officials are to be released from any federal prison and sends it to the OPI to be forwarded to the districts. The districts use this information to decide what protective measures need to be employed to minimize the risk of harm to the federal judiciary.

**Protective Intelligence: How State and Local Databases Can Assist in Identifying Potential Threats**

State and local law enforcement and court databases are a potential source of information to develop protective intelligence on threats to the federal judiciary. Although the USMS is not systematically collecting and analyzing data from these sources, 52 percent of the USMS district Judicial Security Inspectors we surveyed said they routinely obtain state and local data as part of their protective investigations. We interviewed six Judicial Security Inspectors to obtain additional details on the databases they used and how they used the information in their investigations. The inspectors said that the information in these databases relates to bookings, misdemeanors, incident reports, court cases, and state prison records. The inspectors said they learned about the databases either through personal outreach or as a result of participating in a task force.

The Judicial Security Inspectors reported using the information in the databases in several ways, such as background for interviews with individuals, to identify possible motives for inappropriate communications, to determine if a person had a history of misdemeanors, or to provide leads to other cases that might assist in the current investigation. For example:

- After an individual made an inappropriate communication to a judge, the Judicial Security Inspector used information from state databases to determine that the individual had made similar threats to other judges. The databases also provided information on the type and outcome of the individual's cases at the state level, which provided the inspector with background on why the individual had filed a case in federal court.

- In another case, a state inmate sent a judge a letter written in blood. There was no information on the inmate in the USMS system. The Judicial Security Inspector contacted the state prison administrator's office to learn whether the inmate had committed assaults on other individuals while in prison or had threatened state judges.

Although the above examples involve cases in which threats were made, they demonstrate the types of information in state and local databases that a protective intelligence function could use to identify when individuals known to have threatened state or local officials become federal defendants or litigants.

- In July 2007, the USMS told the OIG that it had proposed to the FBI that some individuals who have threatened the members of the judiciary be included in the FBI's National Crime Information Center (NCIC) pointer system.[46] Including

[46] The NCIC provides police officers and federal agents with criminal history and open warrant information. Although the criteria are not final, the USMS might add 100 to 200 individuals who have threatened the judiciary and who have a violent history, are known to have taken any overt or covert action to carry out an assault or assassination, or have recently purchased a weapon. The USMS would remove the names when the individuals no longer pose a threat.

these individuals would enable the USMS to monitor its most serious threateners, disseminate information about them to other law enforcement agencies, and learn when another law enforcement agency queries the NCIC for information on any of them. If the FBI approves the request, the USMS plans to add the data to the NCIC by the spring of 2008.

- In FY 2007, the USMS initiated a pilot program with the state of Virginia to establish a database of threateners that the USMS would enter into JDIS. In August 2007, OPI managers told us they were conducting a survey of Virginia law enforcement agencies regarding their responsibilities in investigating threats and inappropriate communications and their interest in participating in a database of these cases.

In addition, in a March 30, 2007, memorandum, the Assistant Director of the JSD identified other initiatives related to improving the protective intelligence function that the USMS plans to accomplish by FY 2010. The memorandum appears in Appendix I. Regarding protective intelligence, the Assistant Director stated that the USMS plans to:

- formalize procedures and initiate operation of the Threat Management Center;
- expand and finalize the OPI website;
- establish, as a long-term initiative, a Suspicious Activity Report project to collect, store, and analyze information on suspicious activities other than inappropriate communications;
- complete, as a short-term initiative, modifications to JDIS and move the Court Security Information System's Suspicious Activity Report module into JDIS to capture incidents, demonstrations, and suspicious activity information;
- create a counter-surveillance or surveillance detection program to collect Suspicious Activity Report information;
- increase full-time liaison and detailee positions at other agencies, including the Department of Homeland Security, the Supreme Court Police, the Federal Protective Service, the Central Intelligence Agency's Counter-Terrorism Center, the Diplomatic Security Service; and the Office of Director National Intelligence;
- finalize the polygraph policy for liaison positions;

- procure a new OPI threat management database;
- procure additional analytical tools and search engines;
- establish a full-time information technology position or contractor to manage the sensitive compartmented information facility, classified systems, and OPI database;
- increase the Criminal Investigator staff, including District Threat Investigator, Intelligence Research Specialist, program analyst, and contractor positions (32 requested for FY 2009, with another 30 to be requested in FY 2010); and
- request additional JTTF positions in the districts and Secret/Top Secret computers where appropriate to receive classified information.

Also, in June 2006 JSD managers told us that the USMS intended to initiate the development of a National Center for Judicial Security (Center) in FY 2007 to serve as a repository for information pertaining to the security of courthouses and the protection of judicial officials. The National Support Division of the Center will be responsible for information sharing initiatives such as the Virginia pilot project discussed above. JSD managers have not identified a target date for completion of the Center.

While the OIG believes that the extensive initiatives would be valuable, we also note that the OPI has not developed formal plans to achieve these goals. Formalizing and fully defining the new process will be required for the OPI to obtain resources to carry out its plans, as well as to provide direction to the districts and provide training to district and headquarters staff involved in the protective intelligence mission.

## Implementing Enhanced Security Measures

**Since our March 2004 report, the USMS has implemented additional security measures to protect the federal judiciary, including the congressionally authorized home alarm program. Working with a contractor, the USMS has installed about 95 percent of the home alarms requested by federal judges. The USMS is also enhancing its Technical Operations Group support of the judicial security mission and creating a Rapid Deployment Team program to respond to significant judicial security incidents.**

### Home Alarms for Federal Judges

In May 2005, Congress appropriated $11.9 million to the USMS to provide home intrusion detection systems requested by federal judges and to pay for security measures used by the USMS to investigate and counter threats to judges when they are away from a courthouse.[47] With these funds, the USMS created the Home Intrusion Alarm Program to improve the residential security of federal judges. In our survey, federal judges' responses on their perceptions regarding their security at home highlighted the need for a home alarm program. When we asked federal judges about their feelings of security in different settings, of the 696 who responded, only 114 (16 percent) felt very secure at home (see Appendix II). In this section, we describe our examination of the USMS's implementation of the Home Intrusion Alarm Program, including the USMS's identification and installation of the initial group of alarms pursuant to the legislation; the USMS's management of the program; and the USMS's oversight of alarm monitoring and responses to alarm activations.

Identification and installation of initial alarm systems. On June 14, 2005, the AOUSC sent a survey to federal judges to identify those judges who wanted an alarm system installed in their homes. As of July 8, 2005, 1,363 responded, of whom 1,176 replied that they wanted home alarm systems installed. Judges could request that they

[47] The *Emergency Supplemental Appropriation Act for Defense, the Global War on Terror, and Tsunami Relief of 2005* (P.L. 109-13) provided funds for ongoing military and intelligence operations in Iraq and Afghanistan and other selected international activities, including tsunami relief and reconstruction.

be included in the home alarm program after the survey as well. In December 2005, the USMS directed each district to determine the number of judges in their district who wanted home alarm systems. By November 2006, a total of 1,616 judges had requested alarm systems.

Contracting for the alarm systems and program initiation. According to USMS documents, a solicitation for the home alarm contract was issued in November 2005, and in December 2005 the USMS awarded the contract to install the home alarms. However, the original contract did not include monitoring services or maintenance, leading to objections from the judiciary. Members of the Judicial Conference Committee on Judicial Security contended that the supplemental funding should pay for the monitoring and maintenance because both were part of the USMS's statutory responsibility for judicial security. In late 2005, the USMS agreed and informed the AOUSC and Judicial Conference Committee members that it would pay for central station monitoring.[48] The contract was amended to reflect this change on February 9, 2006. For each system installed in a judge's home, the USMS pays its contractor a monthly fee for monitoring the system. On January 2007, the USMS added a maintenance component to its contract and pays a monthly fee for maintenance of each system.

In February 2006, the USMS and its contractor conducted pilot installations of alarms in the homes of three judges in the Washington, D.C., metropolitan area, and the contractor finalized its "pre-installation plan" format as a result of the pilot test. Meanwhile, the USMS and the AOUSC drafted policies and procedures to govern the administration of the home alarm program. On March 27, 2006, the USMS and the AOUSC issued a joint memorandum that launched the home alarm program nationally.

After the program was initiated, the cost of proposed alarm systems submitted in April 2006 was almost 100 percent higher than had been projected based on the three pilot installations. The higher costs resulted from additional features included in the proposed systems by contractor sales representatives who were not familiar with the scope and parameters of the USMS program. For example, contractor representatives were proposing to install higher-cost systems in some residences, were proposing to use contracted system components improperly (such as placing motion sensors in bathrooms), and were

[48] Central station monitoring occurs at the contractor's facility in Aurora, Colorado.

proposing other features that were deemed redundant by the USMS. In April 2006, the USMS and its contractor reviewed and revised 92 pre-installation plans. To control costs, the USMS issued new guidance regarding the types of equipment authorized for the USMS-funded systems, directed Judicial Security Inspectors to take a more active role in the installation process by inquiring about the components suggested in the pre-installation plans, and directed additional reviews of pre-installation plans.

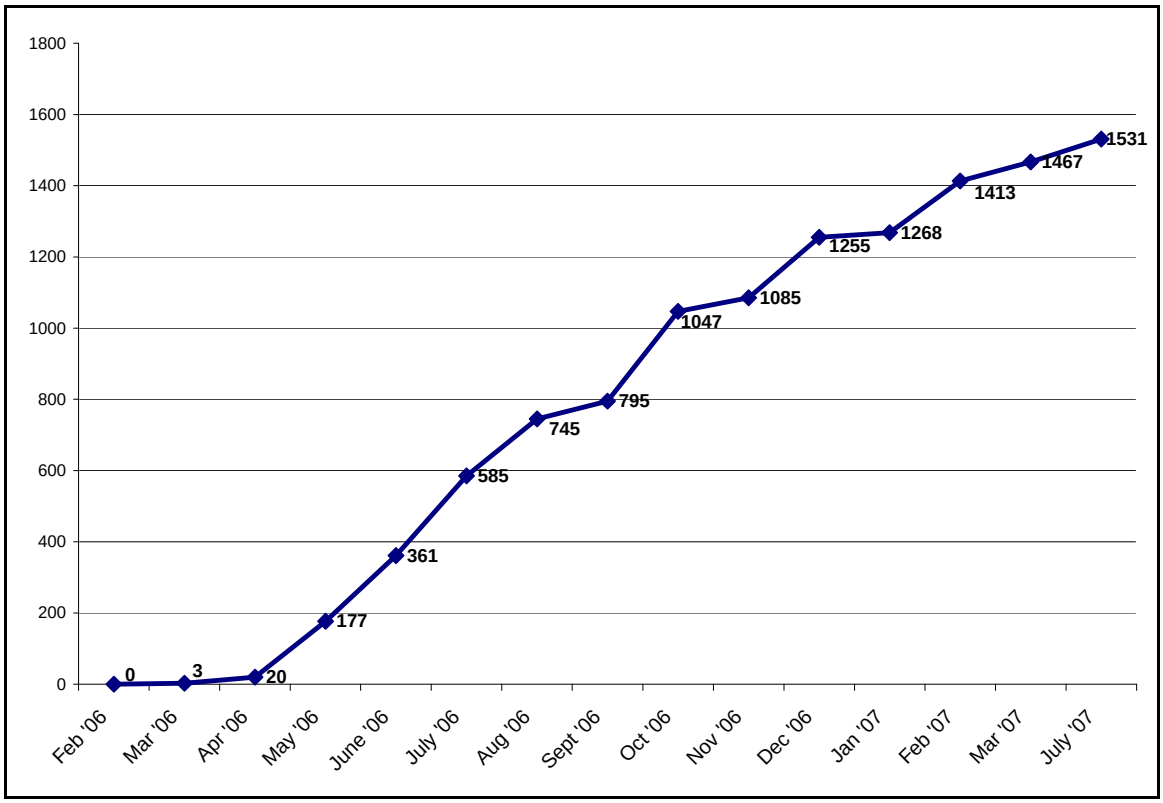
Also during the first months of installations, an issue arose concerning contract termination fees for judges who were replacing personal systems with USMS-provided systems. Initially, to participate in the USMS program, judges were required to terminate their existing contracts, which sometimes left judges responsible for paying early termination penalties. In addition, the contractor believed that under the terms of the December 2005 contract, it was obligated to install new home intrusion systems, even if a judge was already a customer with the contractor. These issues were resolved when the contractor agreed to terminate existing contracts with those judges who had its system without penalty. However, the contractor could not consider contracts the judges had with other security vendors. The contractor was able to use many of the existing home alarm components during installation of the new system.

Alarm installation progress. The USMS and its contractor follow a three-step process for installing alarms. First, the Judicial Security Inspector in the district and a representative from the contractor arrange with the judge to conduct a home inspection to determine the system requirements and select the appropriate alarm features for the judge's residence. Next, based on the inspection, the contractor and the Judicial Security Inspector develop a proposed system configuration for acceptance by the judge. The judge provides the contractor with emergency contact information, and the Judicial Security Inspector presents the proposal to USMS headquarters for review and approval. Finally, after the system configuration is approved for installation by an official at the home alarm program office at USMS headquarters, the Judicial Security Inspector and the contractor contact the judge to arrange a time to install the system. After the system is installed, the judge is trained on how to use the alarm system.

Between March 2006 and July 2007, 1,531 alarms were installed in judges' residences. Chart 4 shows the progress of the alarm installations by month. Installations were prioritized within each

district, with judges that had no alarm system scheduled first, followed by those that had pre-existing alarm systems.

**Chart 4: Number of Home Alarm Installations Completed**




Source: USMS

The USMS Residential Program manager told us that he noticed that some judges' alarm systems had not been installed and sent a message to all districts asking them to query the judges about whether they still wanted the systems. The manager identified several reasons that alarm installations had not been completed. According to the manager, some of the judges indicated to the USMS that they no longer want the home intrusion detection system and some are no longer federal judges. In other cases, judges who requested systems either did not respond to requests from the USMS to arrange a home inspection to determine the system requirements or, after the system requirements were determined, did not work with the USMS and the contractor to establish a time for installation. According to the manager, several of the judges told the USMS that they had not yet made up their minds about whether they wanted the system installed. For these judges, the USMS is holding open the request.

As of July 2007, the USMS reported that it had 67 outstanding requests for alarm systems. Of the 67 requests, approximately 30 of the judges are undecided and have yet to complete the home inspection or installation, and the other 37 were requests for which installation was proceeding.

Monitoring and response to alarms. The USMS is not directly notified of alarm events and receives limited reports of alarm occurrences at judges' homes. When an alarm is received, the contractor first calls individuals identified by the homeowner on their Emergency Contact List. If contact cannot be made, the contractor calls local law enforcement for emergency response. Although the contractor provided the USMS with monthly activity reports from March 2006 through early 2007, these reports did not include data on the number of reported alarm events.[49]

As of July 28, 2007, the USMS was unable to respond to the OIG's request that it identify the number of alarm events that had occurred at judges' residences, including the number of alarms that were accidental or did not require an emergency response, or the number of instances in which the contractor notified local police to make an emergency response. In response to our request during this review, the USMS told us that it did not have an arrangement with the contractor to be notified of alarm events at the residences of judges covered by the USMS program.

Initially, the USMS was included in the list of designated numbers for several of the judges. When the contractor received an alarm notice and was not able to contact anyone on the Emergency Contact List, the contractor called the USMS Communications Center in Washington, D.C., to report that an alarm had been received. According to the USMS Residential Program manager, this presented a problem because the USMS Communications Center is unable to provide immediate physical responses to alarms in the residences of judges across the country. The manager said that the USMS made a determination that it should not be included on the Emergency Contact List used by the contractor. In the event of an alarm, the contractor was directed to contact law enforcement to ensure prompt emergency response for those residences.

[49] According to the USMS Residential Program manager, the monthly reports submitted by the contractor contained data on the number of installations completed and issues encountered, but not on alarm events.

Although the contractor is no longer providing the USMS with reports summarizing alarm events, the USMS has implemented a policy that its districts are to notify local law enforcement that they should be contacted in the event of a "bona fide" alarm event. Specifically, the Residential Program manager told us that he sent a notice to all districts advising them to send letters to each local law enforcement agency that provides coverage of an area in which a federal judge resides. In the letter, the districts were to ask that any local law enforcement agency responding to a call from an alarm at a judge's residence inform the USMS district of the nature of the alarm after it responded. However, the USMS was not able to provide information on how many letters districts have sent to local law enforcement agencies because it did not require the districts to provide copies to headquarters.

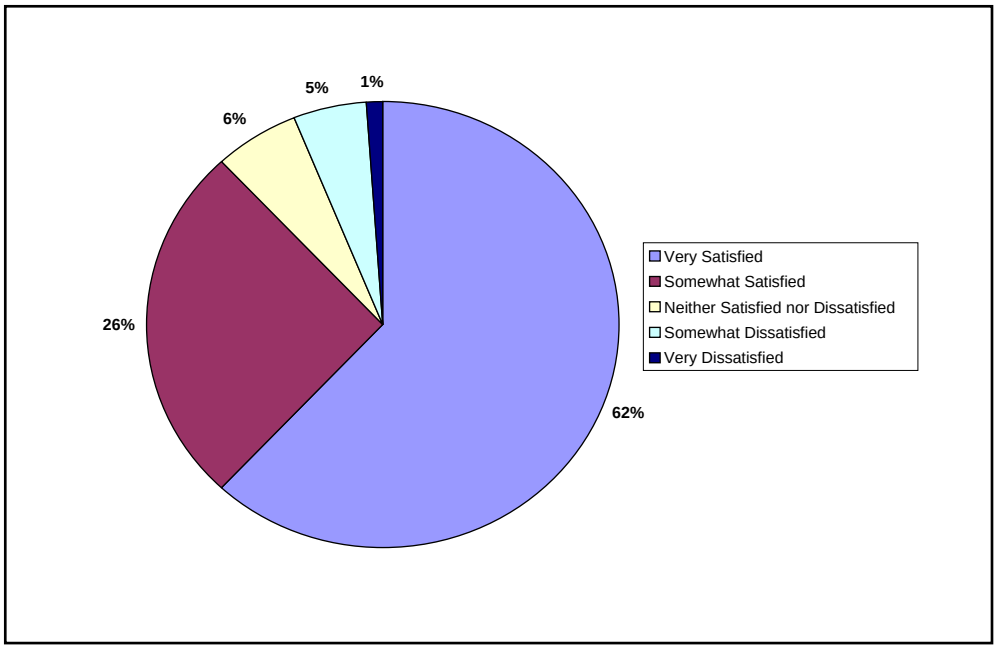
We have several concerns regarding the USMS's approach for learning of alarm events at judges' residences. First, even if a local law enforcement agency identifies that an emergency response is being dispatched to a judge's residence and subsequently notifies the USMS, receiving such "after-the-fact" notifications delays the USMS's awareness of potential security events at judges' residences. Second, the current process places responsibility for notifying the USMS on a local police department rather than on the company responsible for monitoring and providing alarm services. Third, notifications from local police departments may not be reliable, given the difficulty in keeping the information on judges' residences current as they move or retire and given the variation in emergency dispatch systems from jurisdiction to jurisdiction. We agree that the local law enforcement agencies should be immediately notified by the contractor of all unresolved alarms so that they can respond quickly. However, we believe that the contractor should also notify the USMS immediately after notifying the local law enforcement agency.

An opportunity to modify the notification procedures currently exists because the USMS is renegotiating its alarm contract. We believe that the USMS should include as a term of its new contract that the alarm contractor will, after making the required emergency notification to local law enforcement agencies, also notify the USMS, either at the local district office level or at headquarters, that it has referred an alarm at judge's residence to a local law enforcement agency.

Judges' satisfaction with alarm systems. In a survey the OIG conducted in November 2006, 62 percent (281 of 454) of judges who responded stated that they were very satisfied with the home alarm system they received through the USMS, 26 percent (120) were

somewhat satisfied, 5 percent (22) were somewhat dissatisfied, and 1 percent (5) were very dissatisfied (see Chart 5 below).

**Chart 5: Judges' Satisfaction With Home Alarms**




Source: OIG Judicial Survey

When we asked the judges in our survey to provide narrative comments or suggestions on the home alarms systems, some of the positive comments were:

- "Installation of the system was prompt. The contractor representatives as well as the JSI [Judicial Security Inspector] provided a full explanation of the system and its use. This was an upgrade from an existing system, and it provides greater level of protection."

- "It substantially improved what I had. Only a few weeks after installation of the system, it detected vandalism (a broken window) while I was away at a conference. That would not have been detected without the enhancements of the USMS alarm system."

- "The assistance provided by USMS was excellent and much appreciated. Did not feel at risk before, but feel even more secure now."

- "This is a very welcome addition to our security, and I appreciate the manner in which the USMS handled its implementation."

- "It gives us a greater sense of security in our home. All Judicial Officers should have one."

- "I think the system is an important part of the overall security provided to federal judges."

- "I strongly endorse this program and appreciate it being provided to us. This system helps provide security beyond the normal 8:00 am to 5:00 pm office hours."

In contrast, some judges had negative comments about the home alarm program. Many of these respondents stated that they had incurred additional costs for features that were not covered under the USMS contact, the contractor had not been responsive to service calls, or that they had unanswered questions about the system. Below are some of the other critical comments provided by judges.

- "I question whether there was appropriate oversight with respect to the nature and cost of the system provided."

- "There does not appear to be any justification for the length of time that elapsed between the Congressional appropriation of funds to the awarding of the contract and the installation of the equipment."

- "It has already malfunctioned once, causing a screeching beep in the middle of the night. I had to disassemble the system to get it to stop. And it took two months for [the contractor] to replace the defective parts."

- "The system has so many features that it is complicated to learn. Like all new technology and security in particular, it's only effective if people use it. More training for the judges on what features are most efficacious would be helpful."

The USMS Technical Operations Group

The USMS is enhancing its Technical Operations Group's (TOG) support of the judicial security mission. The TOG is organizationally located in the Investigative Services Division and is composed of an electronic branch, an air surveillance branch, a tactical support branch, and an analysis and intelligence group. In response to requests from district offices, the TOG uses sophisticated technologies to provide investigative and intelligence support, primarily for the USMS fugitive apprehension mission.[50] The districts request judicial security assistance from the TOG through the JSD's Office of Protective Operations. The judicial security assistance requested by district offices can include providing technical equipment.

In response to concerns of the Judicial Conference of the United States and Congress, in September 2005 the USMS Director convened a Judicial Security Technology Committee (Committee) composed of USMS and AOUSC staff to review the agency's technology assets and the ability of the JSD to fully respond to the security needs of the judiciary. As part of its review, the Committee also considered whether a single entity within the USMS could support the missions of both the Investigative Services Division and the Judicial Security Division. In January 2006, the Committee reported that JSD headquarters personnel did not provide sufficient support to the districts in accomplishing the judicial security mission because:

- the JSD did not have sufficient assets in place to meet the security needs of the federal judiciary;
- the JSD's technological equipment was outdated and not appropriately distributed around the country to allow for rapid deployment;
- the JSD had not established clear guidelines for requesting TOG assistance; and
- the USMS needed to eliminate the atmosphere of competition between the Investigative Services Division and the JSD.

[50] The Investigative Services Division oversees the enforcement of court orders, fugitive investigations, execution of federal warrants, and operation and maintenance of WIN/JDIS. It also provides electronic surveillance. In FY 2006, the TOG conducted over 7,100 surveillance operations for over 2,900 fugitive cases, an increase of 6 percent from FY 2005.

The Committee recommended that the JSD transfer its judicial security technology resources to the TOG and that the USMS expand the TOG's mission to more adequately address the judicial security mission.

USMS efforts to enhance the capability of the TOG are ongoing. To address the Committee's recommendations, the USMS has provided some additional resources to the TOG and requested additional resources in its FY 2008 budget request. In September 2006, the JSD transferred three personnel to the TOG, including a telecommunications specialist who will manage the Court Security Officer radio program and two criminal investigators.[51]

In its FY 2008 budget submission, the USMS requested funding for six positions (five Deputy Marshals and one analyst) to assist in the enhanced TOG support of the judicial security mission. The USMS also requested $890,000 for TOG equipment and technology.

The USMS has not implemented policies and procedures to guide requests for TOG support. The Office of Protective Operations has not yet developed a policy for referring district requests to the TOG. We asked the JSD Assistant Director in April 2007 about the USMS procedures for districts to request TOG assistance and criteria for providing assistance to districts. He responded that everyone in the field does not have to know what the TOG is capable of as long as headquarters knows because headquarters makes the decisions about approving the requests. Although the USMS has identified that the TOG has limited resources to support judicial security, the JSD has not yet developed criteria for prioritizing and referring district requests to the TOG.

Further, the TOG has drafted, but has not implemented, a policy describing when and how its resources will be deployed. We asked the TOG Deputy Chief in January 2007 about the review process for district requests for TOG assistance since he mentioned that he expected an increase in district requests as awareness of the TOG's capabilities becomes better known. The TOG had already identified the need for written requirements and was drafting and forwarding the document for ISD and JSD review and comment. In May 2007, the TOG provided the OIG a draft of the document.

[51] The Court Security Officer radio program is funded by the Judicial Branch's AOUSC.

From September 2006 through June 2007, the TOG received eight requests for judicial security-related assistance from the districts.[52] The TOG fully supported six of the requests and denied two requests because they did not fall within the TOG's area of responsibility. The following are two examples of TOG support to the USMS's judicial security mission:

- A federal judge already under a protective detail because he had received a letter containing white powder received two calls threatening his life. Later, calls were placed to 911 and a local television station claiming that there was a bomb in the courthouse where the judge worked. The FBI was involved in the investigation and informed the TOG that there were approximately 30 suspects. The TOG determined the location from which the phone was used and where the phone was purchased. A suspect was subsequently arrested after the TOG obtained the store's security video.

- In response to a district request for technical assistance, the TOG provided electronic equipment to monitor the residence of a federal judge who was presiding over a terrorist trial.

The TOG has provided training on its support capabilities to district personnel. In July and August 2006, and again in July 2007, the USMS highlighted the TOG's capabilities during a Protective Investigation Training Program at the Federal Law Enforcement Training Center. During the training, USMS district personnel were informed about the TOG's capability to provide protective intelligence gathering and analysis, information sharing with state and local law enforcement, and tactical support for judicial security missions. However, the training did not make all Judicial Security Inspectors aware that the TOG has increased its support to the judicial security mission. In response to our November 2006 telephone survey of 82 Judicial Security Inspectors, 26 (32 percent) told us that they were not aware of the initiative to expand the use of the TOG for protecting the judiciary.[53] JSD managers told the OIG that the

[52] The TOG began tracking district requests for its assistance on judicial security cases in September 2006.

[53] We noted that 24 of the 26 Judicial Security Inspectors who stated they were unaware of the enhanced TOG capabilities did not attend the training at the Federal Law Enforcement Training Center.

JSD plans to hold training seminars for Judicial Security Inspectors in October and November 2007.

The USMS Rapid Deployment Team Program

The JSD recently began creating a Rapid Deployment Team program to respond to significant judicial security incidents around the country, such as an assault on a judge or a disruption of a U.S. courthouse's operation. The Rapid Deployment Team responds to the location to assist the local USMS district in managing the incident. In a July 2006 interview for an AOUSC staff publication, the USMS Director stated that it was his "goal to change how the Marshals Service protects the Judiciary, from being less reactive to more proactive in our approach. We need to be ready, as much as we possibly can, to respond." The Director said that one key factor in accomplishing this would be to establish rapid deployment teams:

> We want to be fast in getting personnel where they need to be. For example, when someone harms or makes a viable threat to harm a judge or his or her family members, we want to put trained teams in that area as fast as possible to do a couple things: to immediately protect the judge or the family members or whoever needs protection, and also to relieve our field offices of managing both the crisis and their regular day-to-day duties. Rapid deployment teams, as we see them to be, will be a group of several deputies or court security inspectors who will, when the "fire alarm" rings, be on the ground quickly. They will be on call for a set period of time – perhaps 30 days at a time. We'll have a back-up team ready as well, so if there's a secondary incident or there's a need for additional people, we'll have that team available. These teams will be fully trained, equipped, ready to be mobilized. So again, the timeliness of our response is very, very critical.[54]

In March 2007, the Deputy Assistant Director for Judicial Operations told the OIG that the JSD had directed a working group to draft the operating methodology and plans for the Rapid Deployment Team by the end of May 2007. In April 2007, the Assistant Director of the JSD told the OIG that a senior JSD manager could immediately

[54] "Interview: A Dialogue with USMS Director John F. Clark," *Third Branch,* Vol. 38, Number 7, July 2006.

deploy to assess the need for a Rapid Deployment Team that would be composed of JSD managers and circuit court inspectors from around the country. If the JSD manager determined that a team was necessary, the manager would work with the district to define the expertise needed on the team and select the appropriate USMS staff to serve on it. As of July 2007, the Rapid Deployment Team program was still in development and no deployments had occurred. The Deputy Assistant Director told the OIG that the operating methodology and plans for the Rapid Deployment Teams were not expected to be completed until September 2007.

## CONCLUSIONS AND RECOMMENDATIONS

We found that from the issuance of the OIG's March 2004 report through October 2006, the USMS's efforts to improve its capabilities to assess reported threats and identify potential threats languished. Threat assessments took longer to complete, and over half of the threats reported by USMS districts remained pending as of October 1, 2006. Also, the USMS did not implement an effective program to develop protective intelligence that identifies potential threats against the judiciary. The USMS acknowledges these deficiencies and plans to revise its threat assessment process. During this review, the USMS also informed the OIG of numerous initiatives it plans to implement by FY 2010 to enable it to collect and analyze information on potential threats to the judiciary.

Also since our March 2004 report, the USMS has implemented several security measures to protect the federal judiciary. The USMS has implemented a congressionally authorized home alarm program and worked with a contractor that installed about 95 percent of the home alarms requested by federal judges. The USMS is also enhancing its TOG and developing a Rapid Deployment Team program to support the judicial security mission.

We believe that to fulfill its critical mission of protecting the judiciary, the USMS must exhibit a greater sense of urgency in implementing its plans for improving its capability to assess reported threats, creating and sharing protective intelligence on potential threats, and completing the implementation of enhanced security measures.

To improve the USMS's capacity to protect the federal judiciary, we recommend that the USMS take the following actions:

1. Develop a formal plan that defines objectives, tasks, milestones, and resources for the new threat assessment process.

2. Create a workload tracking system for threat assessments.

3. Develop a formal plan that defines objectives, tasks, milestones, and resources for implementing a protective intelligence function to identify potential threats.

4. Modify USMS databases to support the new threat assessment process and protective intelligence function to identify potential threats.

5. Require the home alarm contractor to notify the USMS of alarm events after notifying the local law enforcement agency.

6. Issue operational guidance for requesting and deploying Technical Operations Group resources and Rapid Deployment Teams.

## APPENDIX I: JSD ACCOMPLISHMENTS AND INITIATIVES

U.S. Department of Justice
United States Marshals Service
Judicial Security Division
Washington, DC 20530-1000

March 30, 2007

Mr. Paul A. Price
Assistant Inspector General
Office of the Inspector General
Evaluation and Inspections Division
Department of Justice
1425 New York Avenue, Suite 6100
Washington, D.C. 20530

Dear Mr. Price:

In 2003, your office conducted a review of the United States Marshals Service (USMS) Judicial Security Process and issued a report in March of 2004. In July 2006, your office returned and is conducting an audit to determine what progress we have made since your last review.

The Judicial Security Division (JSD) was reorganized in November 2006. I was appointed as Assistant Director, and transferred several senior field operational personnel to USMS headquarters to assist in managing the division's core functions. The division is now comprised of two mission-oriented components, Judicial Operations and Judicial Services.

Since the March 2004 report, JSD also established the Office of Protective Intelligence (OPI) in July 2005 which falls under the Judicial Operations component. This office is responsible for collecting, analyzing and disseminating information about groups, individuals and activities that pose a potential threat to the judiciary and persons and property protected by the USMS. OPI provides this information to districts, protective details, USMS senior leadership, JSD and other headquarters divisions to support their responsibilities. The most substantive responsibility for OPI is to provide centralized guidance, oversight and coordination for the districts in conducting threat investigations, known as protective investigations.

I would like to share with you some of JSD's accomplishments and initiatives to demonstrate the progress we are making in the area of protective investigations. My staff has been discussing the following accomplishments and initiatives with your staff:

~~Limited Official Use/Law Enforcement Sensitive~~

Staffing:

- In July 2005, OPI was established with nine personnel. At present, our staffing has increased to 19 personnel and, in the next few months, we intend to expand to a total of 25 personnel with an additional Inspector, Intelligence Research Specialists (IRS) and Program Analysts.
- For fiscal year (FY) 2008, the President's budget will request 10 District Threat Investigator positions which will be dedicated to work protective investigations.

Training:

- Since your last review, JSD and the USMS Training Academy conducted five Protective Investigations Training Program (PITP) classes for Inspectors and Deputy U.S. Marshals (DUSM). In December 2004, one class of 48 received training and in July and August of 2006, four PITP classes were conducted with 190 DUSMs and Inspectors receiving training in protective investigations. Four of your Inspectors attended the last two classes.
- We have two PITP classes scheduled in the third and fourth quarters of FY 2007.
- In December 2005, a total of 210 Inspectors and DUSMs attended the Judicial Security Protection Training Conference in Baltimore, Maryland, and received protective investigations training, along with protective operations training.
- OPI is working with the USMS Training Academy to improve the protective investigations training included in the curriculum of the Basic Deputy, the GS-0082 to GS-1811 Conversion classes and the Advanced Deputy classes. The benefit will be more personnel trained in protective investigations.

Interaction with Districts:

- The OPI Investigations Branch is structured with six circuit teams, covering two circuits each. At present, each team consists of an Inspector and shared IRS. This staffing combination offers consistent, frequent and familiar interaction on cases between OPI and the districts. As the new personnel come on board, each team will have an IRS or a Program Analyst assigned.

Case Load:

- Since the PITP classes in July and August 2006, there has been an increase in the number of cases reported to OPI. This is due to the education of the DUSMs and Inspectors to focus on the behavior of protective investigations subjects, rather than the content of their statements or inappropriate communications.
- Compared to FY 2006, where OPI had limited staffing, FY 2007 has seen improvements in meeting the goal of further processing cases with analysis by conducting MOSAIC and Comparative Analysis (CA). Upon receipt of a written report from the field, OPI immediately conducts an initial review of each case and then conducts further analysis. In FY 2006, OPI processed 33 percent of standard cases in the 7 business day time requirement and 22 percent of the expedite cases

in the 3 business day time requirement. In the first quarter of FY 2007, OPI processed 93 percent of standard cases in 7 business days and 100 percent of the expedite cases in 3 business days.

- As late as July 2006, there were approximately 900 pending cases in an active or "open" posture that required MOSAIC and CA analysis. OPI has taken an aggressive approach to these pending cases by communicating with the district Judicial Security Inspectors, Chief Deputy U.S. Marshals and U.S. Marshals to ascertain the status of the investigations by requesting official case updates via the USM-11, Report of Investigations. These USM-11s provide additional information for analysis. OPI's efforts have led to the number of pending cases requiring analysis to be reduced to 73 cases. Analysis of these 73 cases was completed by March 16, 2007. Therefore, as of March 16, 2007, OPI no longer has any pending cases requiring analysis.
- Twelve of the 19 OPI personnel started after May 1, 2006. This staffing increase provided the necessary staffing to address our case load and time requirements.

SCIF and Threat Management Center:

- Currently, OPI has 24/7 coverage by a Duty Inspector. Any call to the main OPI line is call forwarded to the 24/7 Duty Inspector.
- On December 18, 2006, construction began on the Secure Compartmentalized Information Facility (SCIF) which will house the Threat Management Center (TMC). The estimated completion date is May 1, 2007.

OPI Products:

- Update the Protective Investigations Program, a Policy and Procedural Guide for Threat Management (aka: Protective Investigations Handbook). Interaction with the districts since the PITP classes and new management has generated changes in areas such as reporting requirements, the use of MOSAIC and Comparative Analysis and the future introduction of the 24/7 TMC. This document will be finalized after the TMC is in operation and the process is reviewed.
- Update Protective Investigation Policy 10.16 in the areas of reporting requirements, MOSAIC and Comparative Analysis and inclusion of the TMC. This document will be finalized after the TMC is in operation and the process is reviewed.
- In August 2006, instituted a Daily Briefing document for USMS management.
- Since October 1, 2006, issued 19 Alert Notices and 19 Information Bulletins.
- Issued four threat assessments for high threat trials.
- Since October 1, 2006, issued 40 foreign travel briefings for the judiciary.

~~Limited Official Use/Law Enforcement Sensitive~~

Interagency Participation in the Targeted Violence Information Sharing System (TAVISS):

- TAVISS is a pointer system administered by the U.S. Secret Service, National Threat Assessment Center, and consists of a database of over [redacted] subjects who have threatened or inappropriately communicated with protectees from [redacted] federal, state and local agencies.
- The USMS continues to be the third largest contributor to TAVISS [redacted]
- The USMS was one of the original four pilot agencies in TAVISS.
- [redacted]
- Having the opportunity to review the prior behavior of these subjects is of tremendous value to our District Threat Investigators conducting protective investigations. The knowledge of prior behavior offers the investigator insight when conducting the investigation and managing these subjects.

Benefits of Liaison/Detailee Positions:

Full-time:

- Bureau of Prisons/ Sacramento Intelligence Unit (BOP/SIU): notification of the release of subjects that have threatened the judiciary in the past and coordinating prisoner issues. For example, on October 24, 2005, [redacted] mailed an explosive device from USP Leavenworth, Kansas, to the Fourth Circuit Court of Appeals in Richmond, Virginia. The package was detected by Court Security Officers. The USMS detailee worked with the BOP to revise their procedures for dealing with prisoner mail. This detailee routinely obtains information on the pending release of subjects that have been incarcerated for threatening judges. This information is then provided to the respective districts prior to their release.
- National Joint Terrorism Task Force: notification of terrorist cases, situational awareness that impacts the judicial system and provides information valuable to threat assessments for high threat trials. This detailee frequently reviews terrorist and situational awareness information that is beneficial to the USMS. In addition, when OPI or a district has a need for information, this detailee is an expedient conduit to the proper Federal Bureau of Investigation (FBI) unit to obtain valuable information.
- Joint Terrorism Task Force (JTTF) field positions: notification of terrorist cases and situational awareness on the district level and increased communication with area law enforcement agencies. Recently, a JTTF member reviewed an FBI report in regard to several [redacted] subjects crossing the southern border that were headed to a particular district. Our member made the association that these individuals were headed to a district where a high threat trial involving [redacted] funding was being held. The information was important to pass to the USMS district securing the trial and to coordinate with the FBI.

~~Limited Official Use/Law Enforcement Sensitive~~

- Increased the number of JTTF positions from 50 in 2004, to 80 in 2007. This includes 20 full-time, 22 part-time, 37 liaison, an NJTTF representative and a program coordinator.
- [redacted]
- Department of Homeland Security, Office of Intelligence and Analysis: this Chief Inspector started on February 20, 2007. Involvement in the analysis of intelligence information in regard to terrorism, access to intelligence advisories in regard to homeland security, to include information that would affect our Centers for Disease Control (CDC) mission. This detailee is a senior staff member of the Assistant Secretary of Intelligence and Analysis and has access to valuable intelligence products.

Part-time:

- Supreme Court Police, Threat Management Unit: the USMS protects the Supreme Court Justices when they travel outside of the Washington, D.C. area. This relationship improves the flow of information in protective investigations related to U.S. Supreme Court Justices.
- U.S. Capitol Police: subjects that threaten judges frequently threaten members of Congress. This relationship improves the flow of information.
- Washington, D.C. Metropolitan Police Department, Synchronized Operations Command Complex: during major events such as the funeral of former President Ford, the March for Life and the President's State of the Union Address, the USMS is able to tap into real time information concerning these events and provide this information to other USMS entities that may be affected.

Other law enforcement and intelligence agencies that we are networked into include:

- U.S. Secret Service
- [redacted]
- [redacted]
- Department of State, Diplomatic Security Service
- [redacted]
- Pentagon Force Protection Agency
- Drug Enforcement Administration
- Bureau of Alcohol, Tobacco, Firearms and Explosives
- Federal Air Marshal Service
- Transportation Security Administration
- Immigration and Customs Enforcement
- Customs and Border Protection
- Numerous state and local fusion centers (i.e., VA, NY and TX).

~~Limited Official Use/Law Enforcement Sensitive~~

OPI initiatives for FY 2007, FY 2008 and FY 2009 (many of these will require additional positions and funding to implement):

- Formalize procedures and initiate operation of the Threat Management Center
- Finalize the Protective Investigations Handbook
- Update Policy 10.16
- Move away from MOSAIC and Comparative Analysis and concentrate on the behavior of subjects who make threats or inappropriate communications
- Enhance protective investigations training in Conversion, GS-1811 and Advance DUSM classes
- Coordinate with the FBI to enter subjects of concern into the NCIC Database so we are notified when their names are checked
- Expand and finalize the OPI website
- Establish Suspicious Activity Report (SAR) Project: collect, store and analyze SAR information
- Create a Counter-surveillance or Surveillance Detection Program to collect SAR information
- Increase participation on JTTFs in the districts
- Increase full-time liaison/detailee positions
- Finalize polygraph policy for liaison positions
- Short-term IT:

  Modifications to the Justice Detainee Information System (JDIS) ($100k obligated in FY 2006 to ITS)
  Move Court Security Information System (CSIS) SAR module into JDIS to capture incidents, demonstrations and suspicious activity information

- Long-term IT:

  Procure a new OPI threat management database
  Procure additional analytical tools/search engines
  Establish a full-time IT FTE/Contractor to manage the SCIF, classified systems and OPI database.

- Requested 32 Criminal Investigator (includes 10 District Threat Investigators), IRS, Program Analyst and contractor positions for FY 2009 and will request 30 additional positions (25 District Threat Investigators) for FY 2010 to staff the following additional sections in OPI:

  Behavioral Research Section
  Information Technology Section
  Internet Threat Section
  Suspicious Activity Reporting Analysis & Coordination Section
  Training Coordinator
  Threat Assessment Section
  Trip Briefings Section, foreign & domestic

~~Limited Official Use/Law Enforcement Sensitive~~

Domestic Terrorism Section
International Terrorism Section
Country or Continent Sections

- Liaison/Detailee Positions at other agencies:

  Department of Homeland Security, National Operations Center
  Supreme Court Police
  Federal Protective Service
  Central Intelligence Agency, Counter-terrorism Center
  Diplomatic Security Service
  Office of Director National Intelligence

- In FY 2010 will request additional JTTF positions in the districts and Secret/Top Secret computers where appropriate to receive classified information.

[redacted] We request that in your final report you minimize the amount of information published on the open source internet, to ensure that the security of the federal judiciary is not compromised.

If you have any questions in regard to this list of accomplishments and initiatives, please do not hesitate to contact me at [redacted]. Thank you for your cooperation during this audit. We look forward to reviewing a draft of your report.

Sincerely,

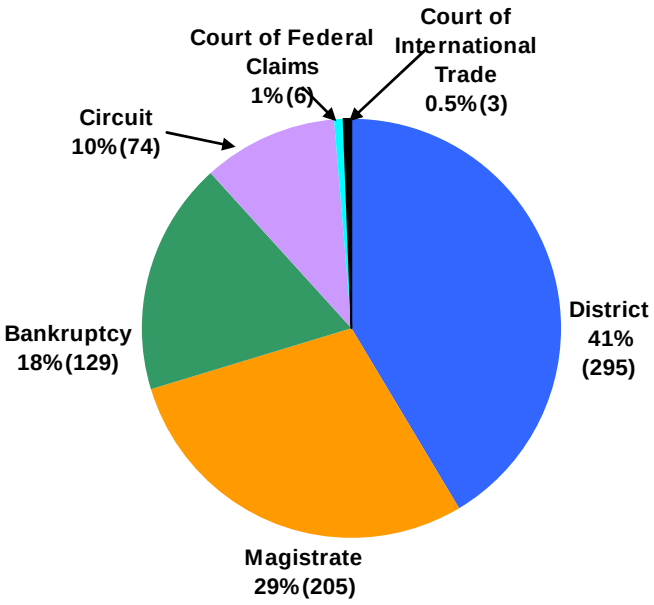
Robert J. Finan II
Assistant Director for Judicial Security

~~Limited Official Use/Law Enforcement Sensitive~~

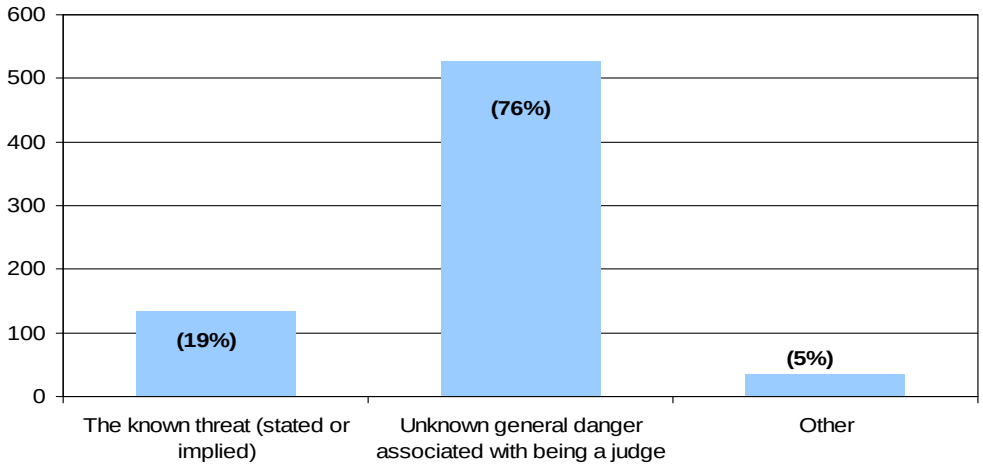
*Sections were redacted to protect the sensitivity of law enforcement operations.

## APPENDIX II: RESULTS OF THE OIG'S JUDICIAL SURVEY

1. Please indicate the type of judgeship you hold. (n=712)




2. What do you believe poses the greatest risk to federal judges? (n=696)



3. How secure or insecure do you feel from job-related threats or danger at the courthouse, away from the courthouse, and at home? (n=712)

| Location | Very Secure | Some-what Secure | Neither Secure or Insecure | Some-what Insecure | Very Insecure |
|---|---|---|---|---|---|
| At the Courthouse | 431 | 197 | 28 | 29 | 11 |
| Away from the Courthouse | 91 | 212 | 264 | 97 | 33 |
| At Home | 114 | 316 | 119 | 123 | 21 |

4. In your opinion, which types of judicial proceedings generally pose a high risk to the personal safety of federal judges?

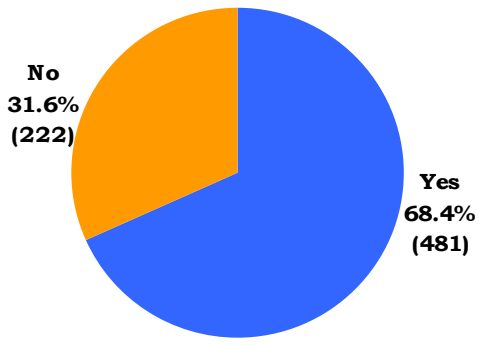
**Civil Matters**

| Type of Case | Number of Responses |
|---|---|
| Admiralty | 2 |
| Animal Rights | 109 |
| Antitrust | 1 |
| Bankruptcy | 212 |
| Civil rights | 298 |
| Contracts | 18 |
| Deportation | 82 |
| Energy Allocations | 1 |
| Environmental Matters | 68 |
| Foreclosure | 205 |
| Forfeiture and Penalty | 126 |
| Freedom of Information | 27 |
| Labor Suits/Employment | 172 |
| Land Condemnation | 62 |
| Personal Injury | 36 |
| Pro Se | 559 |
| Product Liability | 7 |
| Real Property | 29 |
| Social Security | 66 |
| Tax | 160 |
| Tort Issues | 44 |
| Trademark/Patent | 2 |
| Other | 72 |

**Criminal Matters**

| Type of Case | Number of Responses |
|---|---|
| Armed Robbery | 150 |
| Assault | 122 |
| Auto Theft | 17 |
| Burglary | 32 |
| Counterfeiting | 22 |
| Embezzlement | 18 |
| Escape | 156 |
| Espionage | 92 |
| Extortion | 83 |
| Firearms Violation | 200 |
| Forgery | 14 |
| Fraud | 29 |
| Gang Activity | 474 |
| Homicide | 151 |
| Kidnapping | 108 |
| Larceny/Theft | 17 |
| Narcotics | 337 |
| Obstruction of Justice | 116 |
| Organized Crime | 363 |
| Perjury | 16 |
| Pro Se | 385 |
| Public Corruption | 37 |
| Sex Offenses | 42 |
| Terrorism | 321 |
| Treason | 78 |
| Unarmed Robbery | 19 |
| Other | 41 |

5. Throughout your career as a federal judge, have you ever received a threat?



6. In calendar year 2005, how many threats did you receive?

| Response Choices | Number of Responses | Percentage |
|---|---|---|
| None | 254 | 53 |
| 1 | 125 | 26 |
| 2-5 | 96 | 20 |
| 6-10 | 0 | 0 |
| More than 10 | 3 | 1 |
| **Total** | **478** | **100%** |

7. Please estimate how many of the threats you received in calendar year 2005 were related to cases on your docket and how many were not specifically related to these cases. *If none, enter "0."*

| Threats | Average number of threats received |
|---|---|
| Threats related to cases on my docket | 2 (n=197) |
| Threats not specifically related to cases on my docket | 1 (n=87) |
| Threats not known if related to cases on my docket | 1 (n=61) |

8. Of the threats you received during calendar year 2005, how many did you report to the USMS?

| Response Choices | Number of Responses | Percentage |
|---|---|---|
| All | 174 | 78 |
| Most | 14 | 6 |
| Some | 11 | 5 |
| Few | 4 | 2 |
| None | 19 | 9 |
| **Total** | **222** | **100%** |

9. For threats in calendar year 2005 that you did not report to the USMS, to whom did you report the threats that you received?

| Response Choices | Number of Responses | Percentage |
|---|---|---|
| Federal Bureau of Investigation Official | 3 | 7 |
| Local Law Enforcement Official | 5 | 12 |
| Don't Know | 23 | 53 |
| Other | 12 | 28 |
| **Total** | **43** | **100%** |

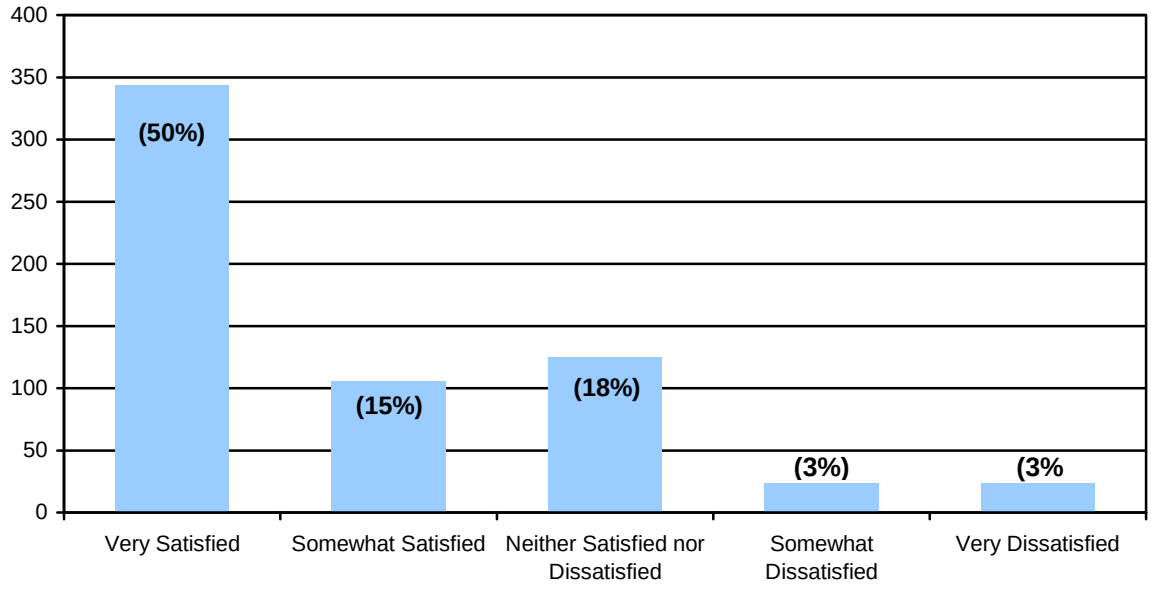
10. Please indicate the reason(s) why you did not report all the threats you received in calendar year 2005 to the USMS.

| Response Choices | Number of Responses | Percentage |
|---|---|---|
| I did not think that the threat posed a real danger. | 34 | 75 |
| I was not familiar with the reporting procedures for threats. | 1 | 1 |
| The threat reporting process was too cumbersome or inconvenient. | 0 | 0 |
| I did not want additional protection. | 0 | 0 |
| Other | 11 | 24 |
| **Total** | **46** | **100%** |

11. Please rate the performance of the USMS in each of the following tasks:

| Tasks | Very Good | Good | Ade-quate | Poor | Very Poor | N/A |
|---|---|---|---|---|---|---|
| Initially responds to a threat with the appropriate protective measures. | 150 | 38 | 14 | 7 | 0 | 10 |
| Keeps you informed during the protective investigation process. | 126 | 36 | 30 | 16 | 2 | 10 |
| Informs you of the final outcome of the protective investigation process, including additional actions or measures required to ensure your safety. | 11 | 42 | 27 | 18 | 3 | 10 |

12. In general, how satisfied or dissatisfied are you with the performance of the Judicial Security Inspector (JSI) assigned your district or circuit?
(n=686)




13. Please explain the reason(s) for your response to Question 12.

The responses were grouped into 11 categories. About half the respondents provided positive comments by describing their JSI as knowledgeable, helpful, and responsive. However, about 100 judges said that they did not know who the JSI in their district is.

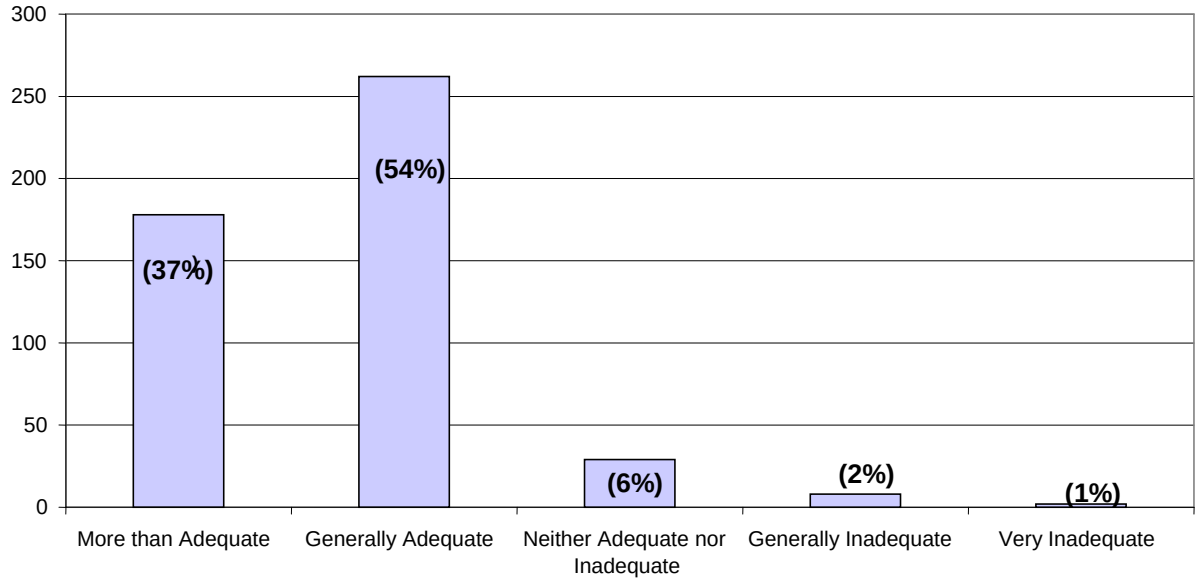
14. In calendar year 2005, did you receive a security briefing or other instruction from the USMS concerning security measures?

| **Response Choices** | **Number of Responses** | **Percentage** |
|---|---|---|
| Yes | 479 | 70 |
| No | 158 | 23 |
| Received instruction, but uncertain of provider | 46 | 7 |
| **Total** | **683** | **100%** |

15. In calendar year 2005, did you request a security briefing from the USMS?

| Response Choices | Number of Responses | Percentage |
|---|---|---|
| Yes | 4 | 2 |
| No | 162 | 98 |
| **Total** | **166** | **100%** |

16. In your opinion, how adequate or inadequate was the security briefing or instruction concerning security measures that you received from the USMS? (n=479)



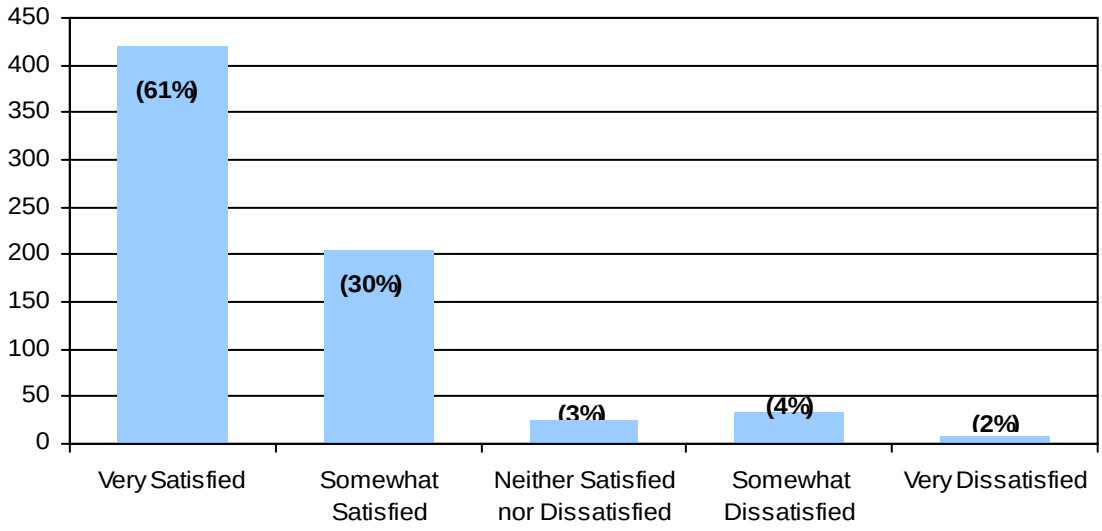

17. Have you completed a Judicial Security Profile for the USMS?

| Response Choices | Number of Responses | Percentage |
|---|---|---|
| Yes | 575 | 83 |
| No | 116 | 17 |
| **Total** | **691** | **100%** |

18. Please indicate the reason(s) why you have not completed a Judicial Security Profile for the USMS. *Check all that apply.*

| Reasons | Number of Responses |
|---|---|
| No need/Insufficient threat against me. | 30 |
| Have not been asked to complete a Judicial Security profile by the USMS. | 15 |
| Have concerns about the security of my personal information. | 34 |
| Other (e.g., too much detail needed on form, no time to complete it, USMS misplaced the last one) | 54 |

19. In general, how satisfied or dissatisfied are you with the performance of the court security officers (CSO) that provide courtroom security? (n=692)




20. In your opinion, how adequate or inadequate is the number of Deputy U.S. Marshals in your district or circuit for providing the security services necessary to protect the judicial process?

| Response Choices | Number of Responses | Percentage |
|---|---|---|
| More than Adequate | 80 | 12 |
| Generally Adequate | 361 | 53 |
| Neither Adequate nor Inadequate | 62 | 9 |
| Generally Inadequate | 135 | 20 |
| Very Inadequate | 43 | 6 |
| **Total** | **681** | **100%** |

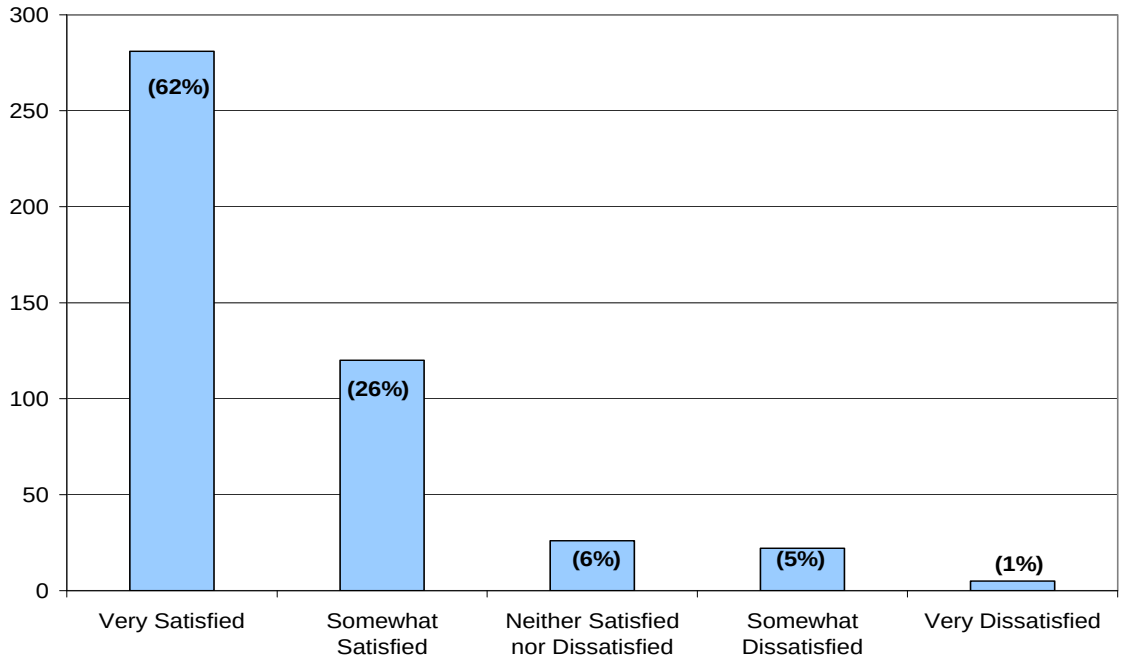
21. Please rank from **1** to **5** (with 1 being the *most* important and 5 being the *least* important) the following measures that you believe the USMS should implement to further improve judicial security.

| Tasks | Number of Respondents per Ranking | | | | |
|---|---|---|---|---|---|
| | **First** | **Second** | **Third** | **Fourth** | **Fifth** |
| Improve intelligence collection and analysis capability | 233 | 131 | 104 | 82 | 71 |
| Provide additional protective investigation training for Deputy Marshals | 46 | 83 | 201 | 172 | 116 |
| Improve analysis of federal, state, and local threat databases for relevant information | 97 | 204 | 136 | 117 | 64 |
| Provide additional protection equipment or technological capabilities | 112 | 134 | 117 | 164 | 91 |
| Increase the security presence in courtrooms | 146 | 70 | 61 | 77 | 269 |

22. Do you have an alarm system provided by the USMS installed in your home?

| Response Choices | Number of Responses | Percentage |
|---|---|---|
| Yes | 450 | 65 |
| No | 238 | 35 |
| **Total** | **688** | **100%** |

23. How satisfied or dissatisfied are you with the home alarm system provided by the USMS? (n=454)



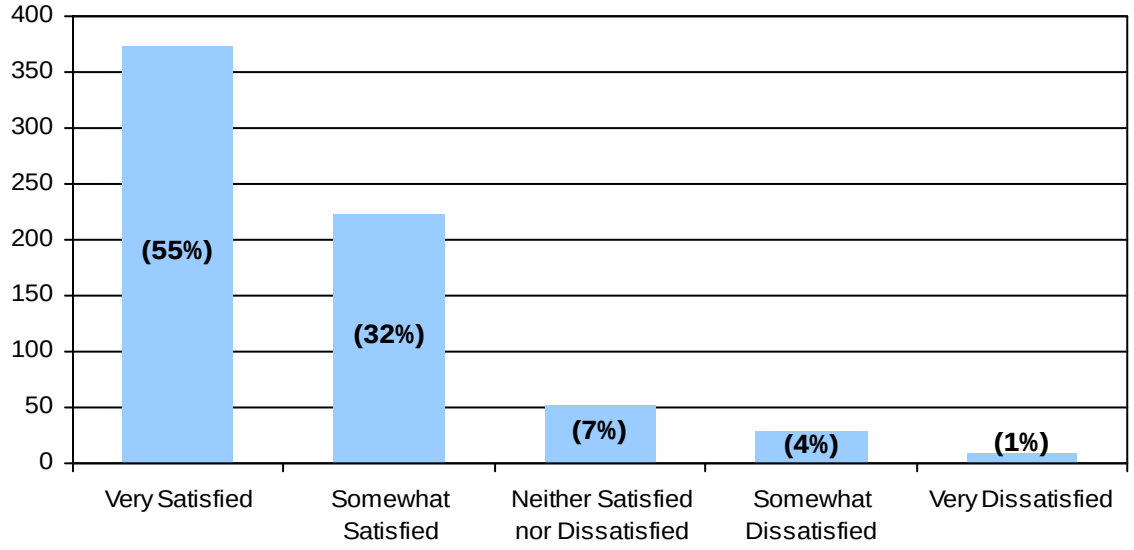

24. Please provide comments or suggestions you have about the home alarm system provided by the USMS.

Judges were generally satisfied with the home alarms they received, but there were areas where some judges noted a need for improvements. One of the more common suggestions was that USMS form partnerships with local police to ensure an appropriate response when an alarm goes off in a home. There were also concerns about continued funding to monitor the alarms and technical issues related to the model of alarm systems that was installed.

25. Please indicate the primary reason why you do not have an alarm system from the USMS installed in your home.

| Reason | Number of Responses | Percentage |
|---|---|---|
| I have requested it, but it has not been installed yet. | 47 | 31 |
| I have other security measures already in place. | 5 | 3 |
| No need/Insufficient threat against me. | 40 | 26 |
| Other | 58 | 39 |
| **Total** | **150** | **100%** |

26. In general, how satisfied or dissatisfied are you with the performance of the USMS in protecting federal judges? (n=686)




27. Please provide additional comments or concerns you have about the USMS's protection of federal judges, including its handling of security briefings and other JSI responsibilities.

Overall, judges were very complimentary about the protection provided by the USMS. USMS staff was characterized as professional, competent, and dedicated. Many judges said that more resources (e.g., money, deputies) are needed in their district and that USMS should be more proactive in terms of identifying potential threats. Concerns were also expressed about the safety of their respective courthouses and off-site security.

## APPENDIX III: RESULTS OF THE OIG'S JUDICIAL SECURITY INSPECTOR SURVEY

### Introduction

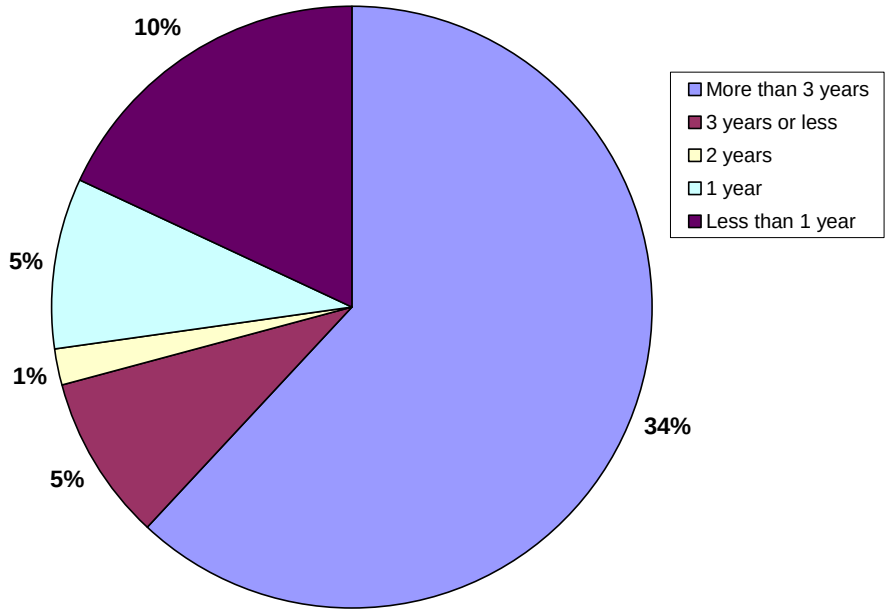
1. What level security clearance do you hold?

| Response Choices | Number of Responses | Percentage |
|---|---|---|
| Top Secret | 63 | 77 |
| Secret | 18 | 22 |
| Don't Know | 1 | 1 |
| **Total** | **82** | **100%** |

2. Are you also a District Threat Investigator?

| Response Choices | Number of Responses | Percentage |
|---|---|---|
| No | 35 | 43 |
| Yes | 47 | 57 |
| **Total** | **82** | **100%** |

3. How many years have you been a District Threat Investigator for this district? (n=82)



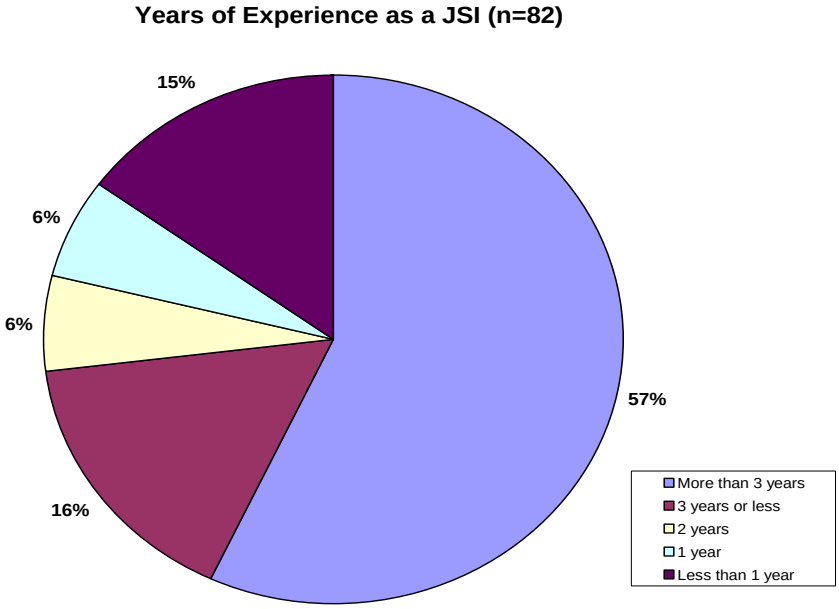

4. Approximately how much of your time is spent investigating threats in a typical week?

| Response Choices | Number of Responses | Percentage |
|---|---|---|
| 75% or more | 0 | 0 |
| 50% to 75% | 1 | 1 |
| Between 25% and 50% | 3 | 4 |
| 25 % or less | 41 | 50 |
| Non-DTIs | 37 | 45 |
| **Total** | **82** | **100%** |

5. Did you attend the Protective Investigation Training Program held at FLETC during July and August?

| Response Choices | Number of Responses | Percentage |
|---|---|---|
| No | 57 | 70 |
| Yes | 25 | 30 |
| **Total** | **82** | **100%** |

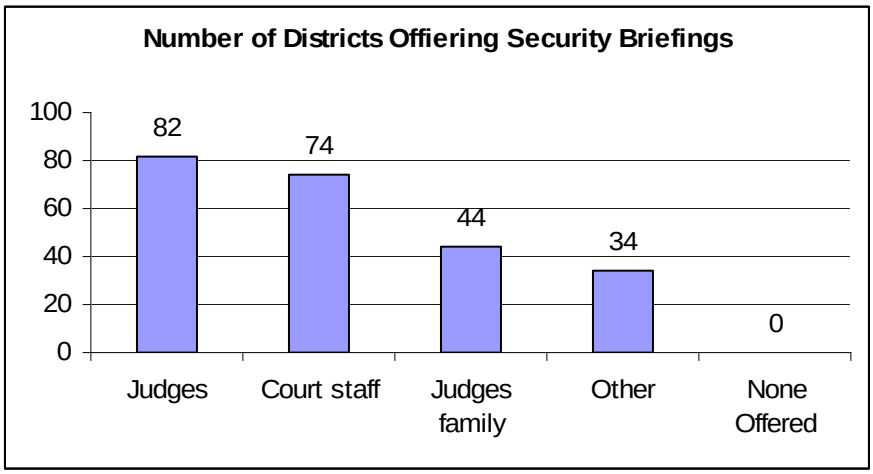
6. How many years have you been the JSI for this district?




7. How many judges does your district currently provide protection for?

The number of judges that district reported providing protection for ranged from 3 to 125.

8. To whom do you offer security briefings? *Check all that apply.*




9. Approximately how many judges in your district have <u>received</u> a security briefing in the past 12 months?

   The number of judges that received a security briefing in the past 12 months ranged from 0 to 80.

10. Approximately how many judges in your district have <u>declined</u> a security briefing in the past 12 months?

    The number of judges that declined a security briefing in the past 12 months ranged from 0 to 29.

11. What is the <u>most common</u> reason given by judges for declining a security briefing in the past 12 months? *Check one.*

| **Response Choices** | **Number of Responses** | **Percentage** |
|---|---|---|
| Insufficient threat | 3 | 7 |
| No reason provided | 14 | 35 |
| No time | 10 | 25 |
| Security briefing is not useful | 2 | 6 |
| Other | 11 | 27 |
| **Total** | **40** | **100%** |

12. Approximately how many judges in your district have declined to provide a Judicial Personnel Profile?

    The number of judges that declined to provide a Judicial Personnel Profile ranged from 0 to 75. On average, six judges per district declined to provide one.

## Protective Details

13. Who in your district primarily supervises protective details?

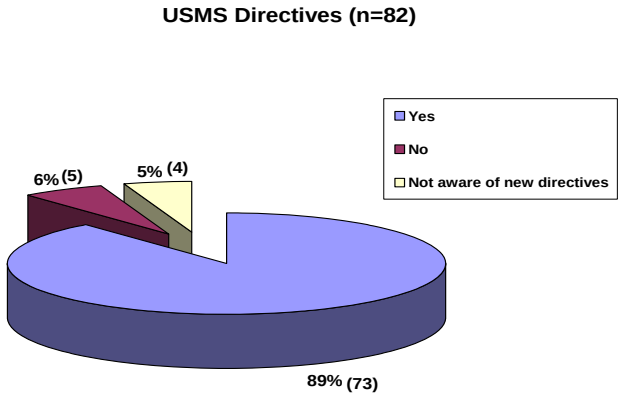
| Response Choices | Number of Responses | Percentage |
|---|---|---|
| US Marshal | 0 | 0 |
| Chief DUSM | 0 | 0 |
| Supervisory DUSM | 5 | 6 |
| JSI | 72 | 88 |
| Don't Know | 4 | 5 |
| Other | 1 | 1 |
| **Total** | **82** | **100%** |

14. Who in your district primarily coordinates with headquarters on resource requests for protective details over 72 hours?

| Response Choices | Number of Responses | Percentage |
|---|---|---|
| US Marshal | 1 | 1 |
| Chief DUSM | 8 | 11 |
| Supervisory DUSM | 2 | 2 |
| JSI | 65 | 79 |
| Don't Know | 4 | 5 |
| Other | 2 | 2 |
| **Total** | **82** | **100%** |

## Office of Protective Intelligence

15. In April 2006, USMS headquarters issued new directives on protective details and investigations, among others. Have you had the opportunity to review the new directives?




16. *Please tell me how much you agree or disagree with the following statement:* My district generally receives threat assessments from OPI in sufficient time to assist in conducting threat investigations.

| Response Choices | Number of Responses | Percentage |
|---|---|---|
| Strongly Agree | 23 | 28 |
| Agree | 43 | 52 |
| No opinion | 11 | 14 |
| Disagree | 4 | 5 |
| Strongly Disagree | 1 | 1 |
| **Total** | **82** | **100%** |

17. According to the new directives, OPI has 3 days to analyze expedited threats and 7 days to analyze standard threats. Is the 3-day time frame for expedited threats sufficient to assist you in conducting these types of threat investigations?

| Response Choices | Number of Responses | Percentage |
|---|---|---|
| Yes | 45 | 55 |
| No | 27 | 33 |
| Don't Know | 10 | 12 |
| **Total** | **82** | **100%** |

18. If no, what would be a sufficient timeframe for expedited threats?

| Suggested Timeframes | Number of Responses | Percentage |
|---|---|---|
| Less than 1 day | 1 | 4 |
| 1 day | 18 | 66 |
| 2 days | 8 | 30 |
| **Total** | **27** | **100%** |

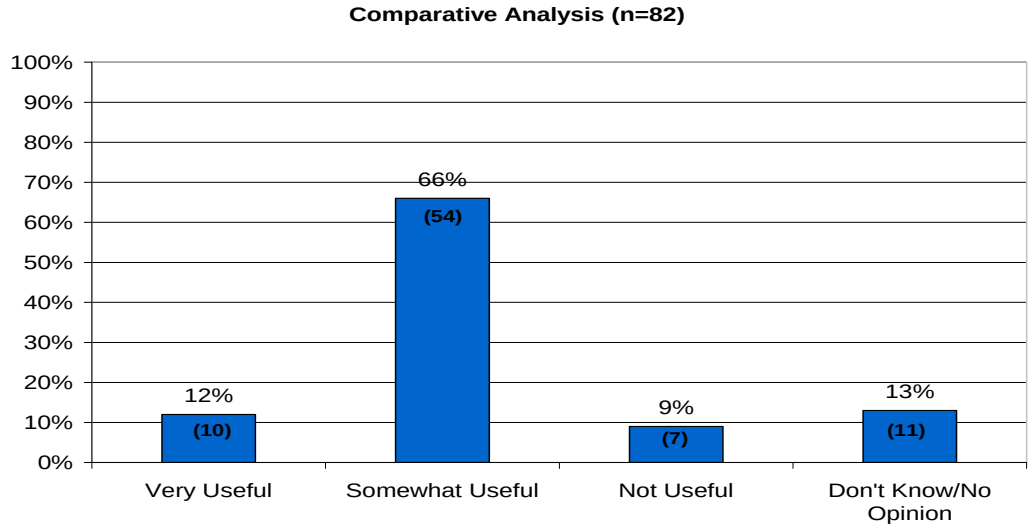
19. Is the 7-day time frame for standard threats sufficient to assist you in conducting these types of threat investigations?

| Response Choices | Number of Responses | Percentage |
|---|---|---|
| Yes | 60 | 73 |
| No | 16 | 20 |
| Don't Know | 6 | 7 |
| **Total** | **82** | **100%** |

20. If no, what would be a sufficient timeframe for standard threats?

| Suggested Timeframes | Number of Responses | Percentage |
|---|---|---|
| 5 days | 7 | 44 |
| 4 days | 1 | 6 |
| 3 days | 5 | 31 |
| 2 days | 3 | 19 |
| **Total** | **16** | **100%** |

21. How useful is the Comparative Analysis score to your district in assessing threats?



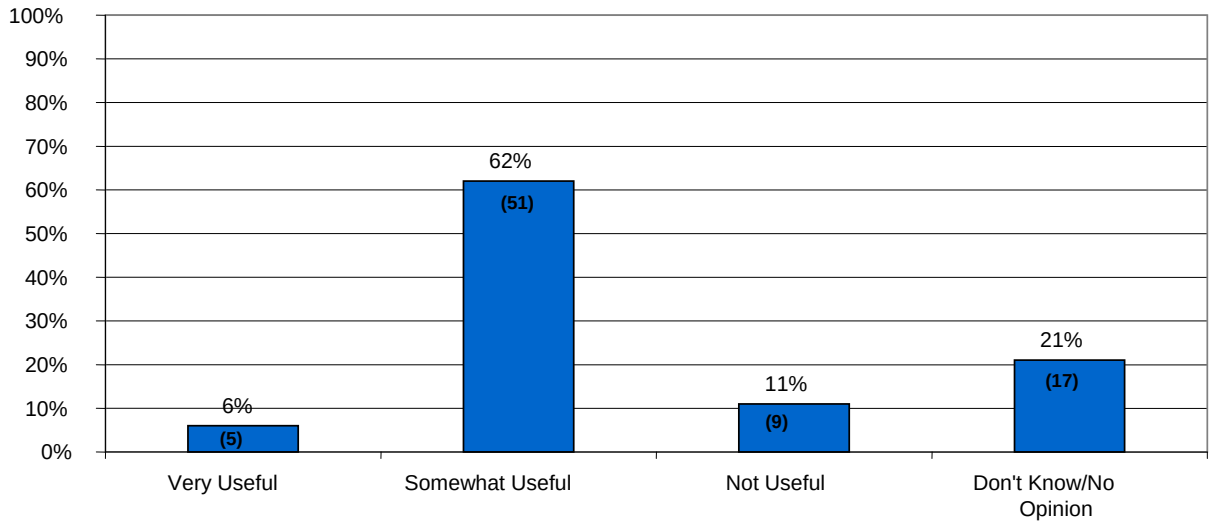

22. Please explain your response to the previous question.

The responses regarding the usefulness of the Comparative Analysis were grouped into 15 categories. The top five response categories were 1) views Comparative Analysis as another tool to make decisions; 2) general comment about Comparative Analysis not being useful; 3) respondents did not know how to interpret the score; 4) rely on information from the field more than Comparative Analysis score; and 5) use score to justify decisions to judges.

23. In the past 12 months, has the Comparative Analysis score caused you to… *Check all that apply.*

| Possible Actions Taken | Number of Responses |
|---|---|
| Close an investigation? | 14 |
| Re-open an investigation? | 0 |
| Enhance a protective response? | 6 |
| Discontinue a protective response? | 4 |
| Confirm the investigator's actions? | 53 |
| Comparative Analysis score has had no impact | 5 |

24. How useful is the MOSAIC score to your district in assessing threats? (n=82)




25. Please explain your response to the previous question.

The responses regarding the usefulness of the MOSAIC were grouped into 14 categories. The top five response categories were 1) views MOSAIC as another tool to make decisions; 2) respondents did not know how to interpret the score; 3) rely on information from the field more than MOSAIC score; 4) use score to justify decisions to judges; and 5) general negative comment about MOSAIC.

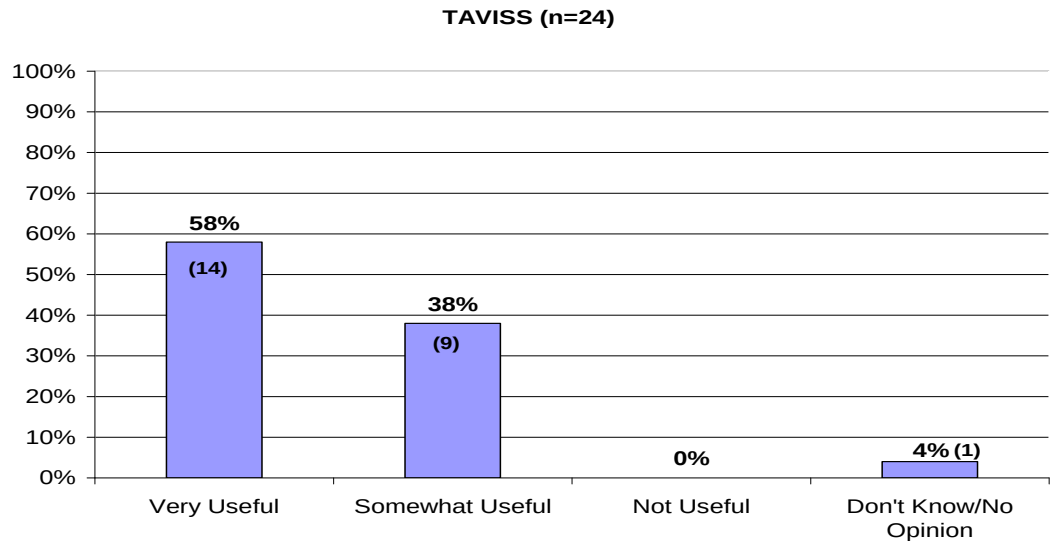
26. In the past 12 months, has the MOSAIC score caused you to… *Check all that apply.*

| Possible Actions Taken | Number of Responses |
|---|---|
| Close an investigation? | 6 |
| Re-open an investigation? | 1 |
| Enhance a protective response? | 6 |
| Discontinue a protective response? | 1 |
| Confirm the investigator's actions? | 49 |
| MOSAIC score has had no impact | 19 |

27. Have you received any TAVISS query results from OPI in the past 12 months?

| Response Choices | Number of Responses | Percentage |
|---|---|---|
| Yes | 24 | 29 |
| No | 40 | 49 |
| Don't Know | 18 | 22 |
| **Total** | **82** | **100%** |

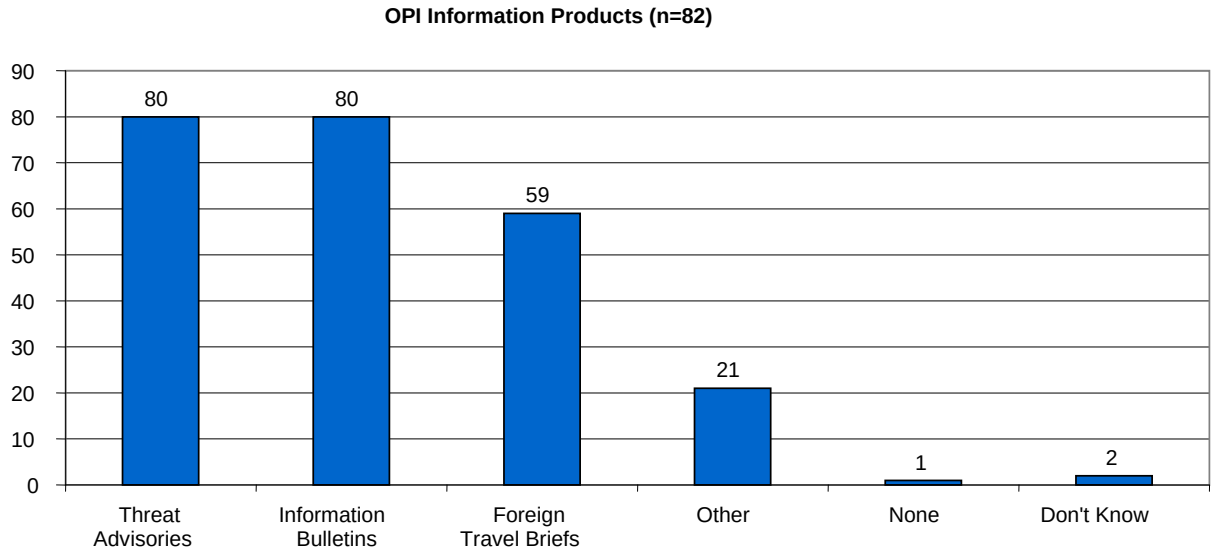
28. How useful are the TAVISS query results to your investigations?



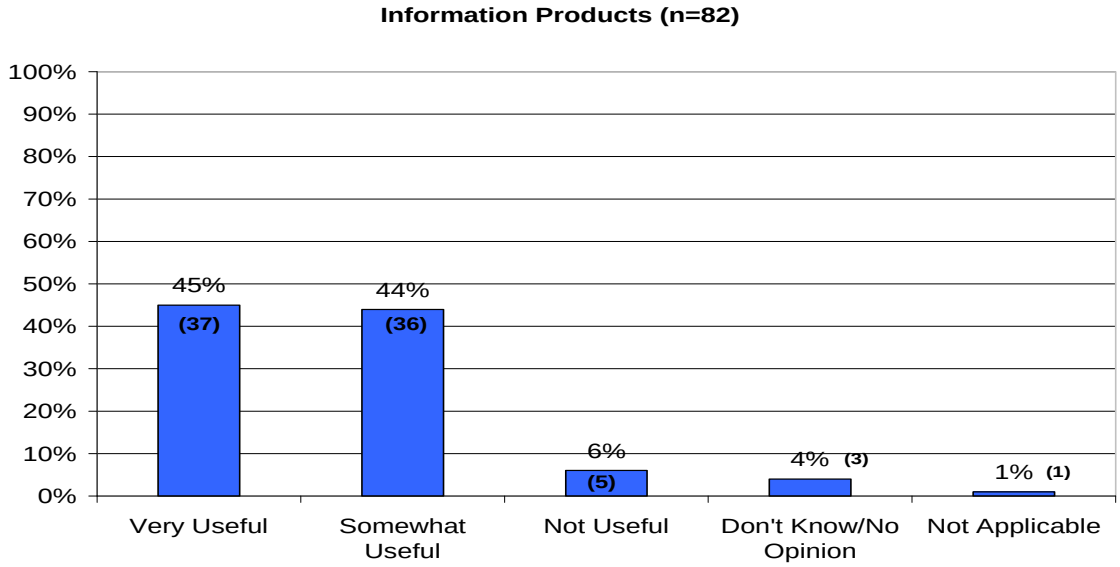

29. Please explain your response to the previous question.

The responses regarding the usefulness of TAVISS were grouped into 3 categories: 1) provides agency contacts; 2) overall positive comment; and 3) JSI had little knowledge of TAVISS.

30. What <u>other</u> information does your district <u>currently</u> receive from OPI? *Check all that apply.*




31. How useful are the other information products from OPI we just listed to your investigations?




32. Please explain your response to the previous question.

The responses regarding the usefulness of the information products were grouped into 11 categories. The top five response categories were 1) overburden by amount of information provided by OPI; 2) information provided was not specific enough; 3) overall positive comment about the information products; 4) information serves as an alert to them; and 5) use information to keep judges and court family informed.

33. What additional information do you need from OPI to better assist you in protecting the judiciary?

    JSIs identified a need in several areas that would assist them in protecting the judiciary. The responses were grouped into 9 categories and the top five response categories are: 1) nothing – overall positive comment about OPI; 2) summaries of threat information; 3) training (primarily on threat investigations); 4) more communication with districts; and 5) regionally focused bulletins, advisories, and local intelligence.

34. Aside from reporting judicial threats for assessment, what other types of judicial security information does your district provide to OPI?

    The responses were grouped into 10 categories and the top five were: 1) no additional information provided to OPI; 2) information on high threat trials and courthouse incidents; 3) information on terrorist groups; 4) suspicious activity, subjects, and packages; and 5) other (i.e., background information).

**Threat Investigations**

35. Approximately how many threat investigations are currently open in your district?

    The responses to this question ranged from 0 to 100. On average, there were 7 open threat investigations per district.

36. Please describe any working relationships—formal or informal—that your district has established with state or local law enforcement or state courts concerning the USMS's judicial security mission.

    JSIs stated that they had good relationships with state and local law enforcement and state courts. Many participated on local task forces, conducted security seminars for state judges, or served a liaison for legal associations (e.g, ABA) in the area.

37. Does your district generally contact the U.S. Attorneys Offices' Intelligence Research Specialists during the course of threat investigations?

| Response Choices | Number of Responses | Percentage |
|---|---|---|
| Yes | 30 | 37 |
| No | 40 | 49 |
| Don't Know | 12 | 14 |
| **Total** | **82** | **100%** |

38. Is your district aware of any state and local law enforcement or court databases that contain information to assist the USMS in threat investigations?

| Response Choices | Number of Responses | Percentage |
|---|---|---|
| Yes | 48 | 58 |
| No | 22 | 27 |
| Don't Know | 12 | 15 |
| **Total** | **82** | **100%** |

39. Does your district routinely query these databases when investigating threats?

| Response Choices | Number of Responses | Percentage |
|---|---|---|
| Yes | 43 | 52 |
| No | 17 | 21 |
| Don't Know | 22 | 27 |
| **Total** | **82** | **100%** |

40. Does your district have direct access to these databases?

| Response Choices | Number of Responses | Percentage |
|---|---|---|
| Yes | 34 | 42 |
| No | 25 | 31 |
| Don't Know | 23 | 27 |
| **Total** | **82** | **100%** |

41. Who in your district is primarily responsible for entering threat information into WIN/JDIS/JDIS? *Check one.*

| Response Choices | Number of Responses | Percentage |
|---|---|---|
| JSI | 13 | 16 |
| DTI | 65 | 79 |
| Don't Know | 1 | 1 |
| Other | 3 | 4 |
| **Total** | **82** | **100%** |

42. What percent of threat cases do you estimate district personnel enter into WIN/JDIS/JDIS?

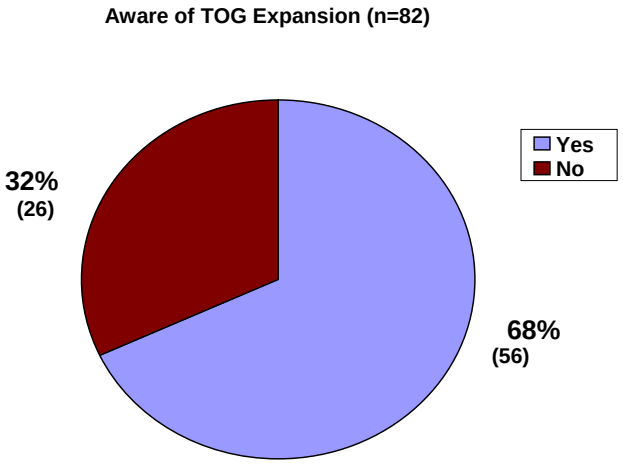
| Response Choices | Number of Responses | Percentage |
|---|---|---|
| 75% or more | 63 | 77 |
| 50-75% | 5 | 6 |
| Between 25 and 50% | 4 | 5 |
| 25% or less | 2 | 2 |
| Don't Know | 8 | 10 |
| **Total** | **82** | **100%** |

43. What is the most important factor that affects how quickly threat information is entered into WIN/JDIS/JDIS? *Check one.*

| Response Choices | Number of Responses | Percentage |
|---|---|---|
| Staff workload | 21 | 25 |
| Perceived severity of threat | 41 | 50 |
| Date threat was reported to USMS | 6 | 7 |
| Don't Know | 10 | 12 |
| Other | 4 | 5 |
| **Total** | **82** | **100%** |

## Director's Initiatives

44. Are you aware of an initiative to expand the use of TOG for judicial security operations?



45. Who in your district normally requests assistance from TOG?

| Response Choices | Number of Responses | Percentage |
|---|---|---|
| US Marshal | 1 | 1 |
| Chief DUSM | 13 | 15 |
| Supervisory DUSM | 2 | 3 |
| JSI | 50 | 61 |
| DTI | 9 | 11 |
| Don't Know | 5 | 6 |
| Other | 2 | 3 |
| **Total** | **82** | **100%** |

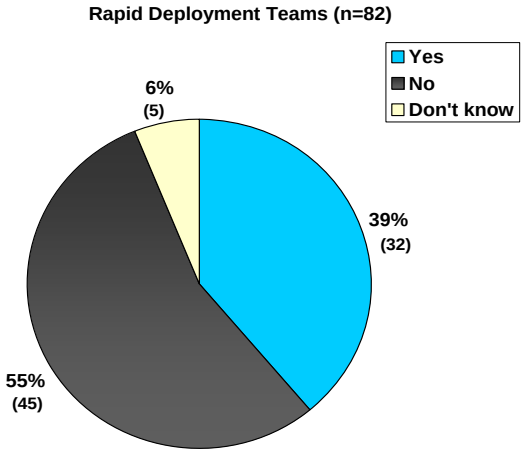
46. Has your district requested TOG assistance for judicial security at any time in the past 12 months?

| Response Choices | Number of Responses | Percentage |
|---|---|---|
| Yes | 24 | 29 |
| No | 54 | 66 |
| Don’t Know | 4 | 5 |
| **Total** | **82** | **100%** |

47. If no, the district did not request TOG assistance because:

| Response Choices | Number of Responses | Percentage |
|---|---|---|
| Not aware of TOG capabilities | 2 | 4 |
| No need for TOG assistance | 50 | 92 |
| Not aware of TOG availability | 0 | 0 |
| Other | 2 | 4 |
| **Total** | **54** | **100%** |

48. Are you aware of the Director's recent initiative that created Rapid Deployment Teams (RDT) to assist districts in crisis situations involving judicial security?




49. Who in your district would request RDT assistance?

| Response Choices | Number of Responses | Percentage |
|---|---|---|
| US Marshal | 2 | 3 |
| Chief DUSM | 32 | 39 |
| Supervisory DUSM | 1 | 1 |
| JSI | 35 | 43 |
| Don't Know | 12 | 14 |
| Other | 0 | 0 |
| **Total** | **82** | **100%** |

50. Has your district requested a Rapid Deployment Team at any time in the past 12 months?

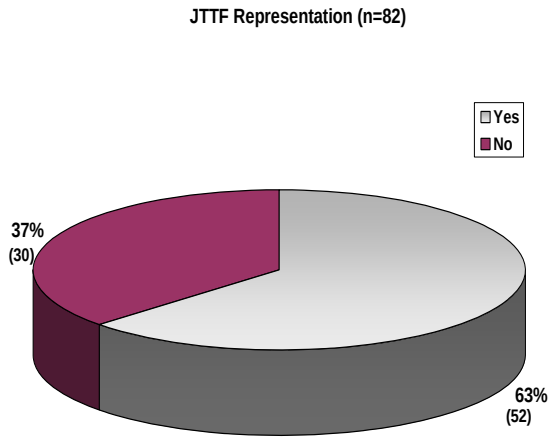
| Response Choices | Number of Responses | Percentage |
|---|---|---|
| Yes | 1 | 1 |
| No | 79 | 97 |
| Don't Know | 2 | 2 |
| **Total** | **82** | **100%** |

51. If no, the district did not request any RDT assistance because:

| Response Choices | Number of Responses | Percentage |
|---|---|---|
| Not aware of RDT capabilities | 3 | 4 |
| Not aware of RDT availability | 23 | 29 |
| No need for RDT assistance | 51 | 64 |
| Other | 2 | 3 |
| **Total** | **79** | **100%** |

## FBI Joint Terrorism Task Force (JTTF)

52. Does your district have a JTTF representative?



53. If yes, is the representative a full-time or part-time member of the JTTF?

| Response Choices | Number of Responses | Percentage |
|---|---|---|
| Full-time | 18 | 35 |
| Part-time | 31 | 59 |
| Don't Know | 3 | 6 |
| **Total** | **52** | **100%** |

54. How much interaction or communication do you have with the JTTF representative?

| Response Choices | Number of Responses | Percentage |
|---|---|---|
| Daily | 26 | 50 |
| Weekly | 12 | 23 |
| Less than once a month | 3 | 6 |
| Monthly | 4 | 8 |
| None | 7 | 13 |
| **Total** | **52** | **100%** |

55. How would you rate the usefulness of your district having representation on the JTTF to the judicial security mission?

| Response Choices | Number of Responses | Percentage |
|---|---|---|
| Not Useful | 7 | 13 |
| Somewhat Useful | 13 | 25 |
| Very Useful | 22 | 43 |
| Don't Know/No opinion | 10 | 19 |
| **Total** | **52** | **100%** |

56. How would you rate the overall usefulness of your district having representation on the JTTF?

| Response Choices | Number of Responses | Percentage |
|---|---|---|
| Not Useful | 2 | 4 |
| Somewhat Useful | 13 | 25 |
| Very Useful | 28 | 54 |
| Don't Know/No opinion | 9 | 17 |
| **Total** | **52** | **100%** |

## APPENDIX IV: THE UNITED STATES MARSHALS SERVICE RESPONSE

U.S. Department of Justice

United States Marshals Service

*Washington, DC 20530-1000*

September 28, 2007

MEMORANDUM TO: Paul A. Price
Office of Inspector General
Department of Justice

FROM: John F. Clark
Director

SUBJECT: Response to the Review of the U.S. Marshals Service Judicial Security Process, Project Number A-2006-007

Before responding to the recommendations contained in the draft report, the USMS would like to take this opportunity to note the progress that has been made and the initiatives that have been undertaken to enhance our protective intelligence program from the time of the 2004 audit to the present.

- In June 2004, the Office of Protective Intelligence (OPI) was established and was staffed with five positions by the close of FY 2004. As in many other government agencies, we worked with the staffing process, and competing priorities, to add more positions. In July 2005, we merged the protective investigations function into OPI from the Investigative Services Division and added four additional positions. In FY 2006, OPI received eight additional positions and four more in FY 2007. Presently, we have 25 positions in OPI.

- In December 2004, we conducted a Protective Investigations Training Program (PITP) class at the USMS Academy in FLETC for 48 DUSMs and Inspectors who received training in protective investigations.

- In January 2005, we drafted concept plans for the Threat Management Center (TMC), which is a secure compartmentalized information facility (SCIF).

- In October 2005, we convened a Judicial Threat and Analytical Assessment Commission (JTAAC). The purpose of the JTAAC was to review and analyze the current protective intelligence and threat investigation activities within the USMS. A total of 10 people sat on the JTAAC which consisted of U.S. Marshals, Chief and Assistant Chief Deputy U.S. Marshals, Senior Inspectors and a member of the

Administrative Office of the U.S. Courts (AOUSC). One U.S. Marshal had experience with the Lefkow case in Chicago, Illinois, and another had experience with the Fulton County Courthouse case in Atlanta, Georgia. The JTAAC made 22 internal recommendations, which were shared with the OIG office. At present, all or part of 12 recommendations have been accomplished. Many of these require additional funding or staffing resources to accomplish.

- In December 2005, the USMS Protective Investigation Policy 10.16 was reviewed and updated. In addition, a total of 210 Inspectors and DUSMs attended the Judicial Security Protection Training Conference in Baltimore, Maryland, and received protective investigations and protective operations training.

- In January 2006, we began the announcement/selection process for additional Supervisors, Senior Inspectors and Intelligence Research Specialist (IRS) positions in OPI. Selections were made on eight positions and in April 2006, they started reporting for duty.

- In June 2006, the Protective Investigations Program, a Policy and Procedural Guide for Threat Management (Protective Investigations Handbook) was updated, but remains as a draft with anticipation of further development of policies and procedures for protective investigations as OPI developed and implemented the TMC.

- In July and August of 2006, four additional PITP classes were conducted with 190 DUSMs and Inspectors receiving training in protective investigations. Four OIG Inspectors attended the last two classes.

- In July 2006, we initiated the staffing of a full-time Senior Inspector at the National Joint Terrorism Task Force in McLean, Virginia.

- In the summer of 2006, the OPI Investigations Branch was structured with Circuit Teams. At present, each team consists of an Inspector and shared IRS. This staffing combination offers consistent communication on cases between OPI and the districts.

- In August 2006, OPI instituted a Daily Briefing document for USMS management.

- Since October 1, 2006, OPI has officially issued protective intelligence products: 47 Alert Notices, 42 Information Bulletins, 7 threat assessments for high threat trials, and 65 foreign travel briefings for the judiciary. Prior to this, e-mails were forwarded unofficially to U.S. Marshals and Chief Deputies. OIG was provided with samples that dated back to March 2006. These products were also provided in 2004 and 2005 by the former Chief of OPI, but due to the limitations of e-mail, he did not have the capacity to save them.

- Compared to FY 2004, 2005, and 2006, when OPI had limited staffing, FY 2007 has seen significant improvement in meeting the goal of processing cases by conducting analysis in a timely manner. OPI also identified and conducted analysis on 1,190 pending cases in an active or "open" status that were referred to as a "backlog." We would like to clarify that these cases were initially reviewed by OPI for their threat potential and the districts that conducted the investigations felt they were appropriate. Due to lack of staffing, they were prioritized for analysis. These cases were not completely neglected as the term backlogged infers. These improvements were due to additional staffing.

- On December 18, 2006, construction began on the SCIF to house the TMC.

- In February 2007, we initiated staffing a full-time Chief Inspector at the Department of Homeland Security, Office of Intelligence and Analysis.

- As of July 2007, the USMS has increased the number of Joint Terrorism Task Forces (JTTFs) positions from 50 in 2004, to 80 in 2007. In 2004, the 50 positions consisted of 25 full-time and 25 part-time DUSMs. In 2007, the USMS increased its participation to a total of 80: 17 full-time, one full-time National JTTF position, 23 part-time and 39 liaison positions. This is an overall increase of 29 positions.[1] Even though 39 are liaison positions, this enhances information sharing for the USMS with other federal, state, and local agencies. These positions increase access to the JTTFs and the flow of information to and from the other agencies on the JTTFs.

- In June 2007, personnel moved into the TMC and in August 2007, the Department of Justice certified the SCIF. Recently, a memorandum announcing the activation of the TMC on September 17, 2007, was sent out to the districts by JSD. This memo discusses policies and procedures for the TMC and identifies examples of protective intelligence information, such as threats, inappropriate communications, demonstrations, suspicious activity and other information that the district should report to the TMC. We hope to receive six additional Inspector positions in FY 2008 to staff the TMC on a 24/7 basis.

The primary mission of the USMS is to protect the judiciary. The USMS takes this responsibility seriously and with a vigilant sense of urgency. We have improved the way we investigate and analyze threats to the Judiciary making it a priority for the USMS in FY 2007 and again in 2008. One outstanding tool that will help us with our mission

[1] It should be noted that the liaison positions are being used due to the lack of increased staffing through the budget process which would allow the USMS to increase actual positions at the JTTFs. Over the past three years, the USMS operational staffing has only seen an aggregate increase of 30 positions. This is due in part to the Joint Resolution for FY 2007, wherein no additional positions were received. As noted in the response to the 2004 audit, in order for the USMS to increase full-time positions assigned to the JTTFs, additional operational positions are needed. Absent that, it would be difficult to increase the USMS presence on the JTTFs without reducing the overall manpower at the courts, where the primary protection of the judiciary occurs.

was the development and construction of a TMC at our Headquarters which was officially opened on September 14, 2007, by the Deputy Attorney General and several members of the Judiciary.

In response to the six recommendations from your office we have the following comments:

**1) Develop a formal plan that defines objectives, tasks, milestones and resources for the new threat assessment process.**

Concur: OPI has developed a new threat assessment process that relies more on the behavior of the subject and interaction with the TMC and Circuit Teams. A memorandum was issued on this subject by Assistant Director Finan to the districts, dated September 10, 2007. The TMC will provide guidance, oversight, and recommendations in the behavior based approach for protective investigations, and will conduct record checks and other analysis for the districts. The 3 or 7-day requirement will be eliminated on October 1, 2007. The TMC analysis will be provided verbally and the district will be given a written response of the analysis and records checks in one business day. After the interaction with the TMC, the case will be forwarded to the Investigations Branch, to the appropriate Circuit Team, for further analysis and coordination with the district.

The districts will be notified of elimination of the 3 and 7-day standard by memorandum before the end of September and this change is also contained in the draft of Policy Directive 10.3, which should be updated by October. An OPI staff person will be assigned to develop a formal plan for the new threat assessment process.

**2) Create a workload tracking system for threat assessments.**

Concur: We note that this recommendation is not specifically discussed in the OIG report other than as a recommendation. OPI contacted the OIG and received guidance on September 13, 2007.

A manual tracking system for analysis of reported protective investigations does exist and is being utilized within OPI. JDIS has the capability of producing reports by date. OPI managers have this report produced weekly (Mondays before noon). This report is studied and analyzed by OPI's Investigations Branch Assistant Chief and is distributed up the chain-of-command and to each OPI employee. The Investigations Branch Assistant Chief identifies any peculiarities and meets with his staff members to discuss the status of the investigation, research and analysis, and any national or regional trends. In addition, the case is logged in upon receipt in an Excel spreadsheet which is maintained on the shared drive (accessible to all OPI employees) and each case is detailed the next business day in the Daily Brief. The Daily Brief and the Weekly Report are also disseminated outside JSD.

The Investigations Branch also prepares monthly status reports from Justice Detainee Information System (JDIS). These reports detail the date the case was received in OPI and what cases are still active investigations. The Investigations Branch Circuit

Teams correspond with the District Threat Investigators and Judicial Security Inspectors of each district via a standard e-mail message and attach a copy of the JDIS report. This correspondence serves as a workload reminder for the field and to OPI management. These e-mails also serve as a request for each case to be updated in JDIS with current investigative activity or to articulate why the potential threat has been mitigated and the case is then closed. Whenever a Circuit Team sees little or no progress beyond the 30-day review requirement, the Investigations Branch Assistant Chief then communicates with the respective district supervisor to determine if there is further assistance OPI can provide to the district to assist the investigation and ultimately mitigate the threat completely, or to an acceptable level of risk.

On the reverse end of the workload tracking systems, the Investigations Branch of OPI already has a manual system in place for ensuring that case analysis is complete within the 3 and 7-day prescribed time-frames allotted by USMS policy. The Investigations Branch Assistant Chief maintains a copy of the weekly report and determines the date the analysis is due in order to stay within compliance. If on either the third or seventh business day (Expedite or Standard), the Assistant Chief has not seen the analysis for his review and signature, he communicates with the respective circuit team to determine if there are issues causing the delay. The process of what analyses are conducted will change on October 1, 2007.

The Investigations Branch Assistant Chief utilizes specific JDIS reports to conduct periodic reviews of the workload distribution internal to OPI. Such reviews are utilized to assist in making decisions about future work assignments. The most recent review was conducted in August 2007, which led to a complete realignment of circuit distribution to be implemented on October 1, 2007. An OPI staff person will be assigned to develop a formal plan for the new workload tracking system.

**3) Develop a formal plan that defines objectives, tasks, milestones, and resources for implementing a protective intelligence function to identify potential threats.**

Concur: OPI collects, analyzes and shares information to identify potential threats in the following manner. To systematically identify potential threats from the districts, OPI keeps track of threats and inappropriate communications and prepares weekly and monthly statistics. The Circuit Teams communicate with the districts, and among themselves, to identify subjects that send mass mailing letters and who are active in multiple districts. The Circuit Teams routinely make notifications to other districts that subjects could potentially become active in their district. OPI frequently issues Information Bulletins and Alert Notices on these subjects. The TMC will continue to do this in addition to the Circuit Teams. From this process, the Circuit Teams and OPI management can identify national or regional trends. A check with other agencies that conduct protective investigations reveals that they use the same process to identify potential threats.

OPI has issued guidance on the type of judicial security information to be reported by the districts. This was covered in the six PITP classes in FY 2006 and

FY 2007 that 280 DUSMs and Inspectors attended. They received instruction in reporting requirements for threats and ICs, but also for suspicious activity, demonstrations, arrests, mental health commitments and any and all incidents that affect the judiciary. This has been added to the curriculum for new GS–1811 Criminal Investigators and Advanced Deputy classes.

With regard to collecting information from other federal, state, and local law enforcement agencies, the districts interact with other law enforcement agencies on a daily basis. Most districts interact daily with their local sheriff's office and share information. In addition, OPI receives information and has a good working relationship with the Virginia, Maryland, and Washington, D.C. fusion centers.

OPI also shares information with state and local agencies by participating with the USMS Eastern District of Virginia in a Pilot Project with Virginia's State Police, Sheriff's Association and State Police Association to catalog cases originally brought in state or local courts which were then raised in the federal courts. A survey is in the process of being sent to Virginia law enforcement agencies to query them as to their agency responsibilities in investigating threats, inappropriate communications, and their interest in participating in a database regarding these cases.

The USMS is initiating the National Center for Judicial Security (NCJS). The NCJS was established to serve as the national subject matter expert for matters pertaining to the security of courthouses and the protection of judicial officials. The operational component, called the National Support Division, will be responsible for the information sharing initiatives such as the Virginia Pilot Project. In addition, the USMS has affirmed its relationship with the National Sheriff's Association (NSA) to improve information sharing for this project.

OPI also participates in the Targeted Violence Information Sharing System (TAVISS) where other agencies contribute the names and identifiers of known threateners into TAVISS. It is a requirement for all USMS subjects to be checked in TAVISS. OPI frequently receives calls from other agencies inquiring about USMS subjects in TAVISS.

OPI's representatives at the National JTTF, DHS, BOP Sacramento Intelligence Unit and liaison to U.S. Capitol Police, U.S. Supreme Court Police and Metropolitan Police also collect and analyze information from other agencies every day. Participation in the JTTFs also maximizes information sharing on a daily basis for the USMS with other federal, state, and local agencies. These positions network with other agencies to exchange and collect information and pass it on to OPI for analysis.

To collect and analyze information from the federal courts, OPI routinely accesses the public PACER database through LexisNexis CourtLink. CourtLink provides all electronic dockets made available from PACER since the early 1990s. In addition, the districts are in the courthouse and routinely deal with the Clerk's office for this type of information and provide the latest information to OPI.

OPI has identified the need for proactive analysis of court records and has identified certain types of cases as significant. The Circuit Teams and OPI management focus more attention on these cases.

OPI has met with the AOUSC regarding access to PACER information. In March 2007, members of OPI attended a presentation by the AOUSC on PACER and the Case Management/Electronic Case Filing (CM/ECF) program. OPI will continue to pursue training and proactive analysis of PACER with the AOUSC. OPI has engaged the AOUSC in discussions on the possibility of an information technology project involving PACER and the CM/ECF to identify potential threateners. However, this project will require extensive funding and staffing requirements.

**4) Modify USMS databases to support the new threat assessment process and protective intelligence function to identify potential threats.**

Concur: The USMS has been in the process of modifying USMS databases to identify potential threats. These initiatives will take place in two phases, short-term and long-term.

Short-term initiatives:

- USMS Information Technology Section (ITS) is working on modifications to JDIS to make it more user friendly to store and search for incidents, demonstrations, and suspicious activity information. This system was created for threats and inappropriate communications and will accept other types of information, but needs improvement for better entry and search capability. OPI transferred funds to ITS in FY 2006 for this project and will transfer more funds by the end of FY 2007. In the interim, JSD presently collects and analyzes suspicious activities at and around federal courthouses based on reporting from the districts and the information is entered in JDIS. OPI receives this information from the districts and JSD Judicial Services.

- ITS is working on moving the Court Security Information System (CSIS) Suspicious Activity Reporting (SAR) module into JDIS to capture incidents, demonstrations and suspicious activity information. This system is used by JSD Judicial Services.

- OPI, in coordination with a dedicated ITS contractor, has obtained an analytical tool for link analysis, information sharing and data mining. This link analysis, or search engine, will be used to search JDIS and other USMS databases, as well as other agency databases. Implementation will begin over the next two months and will enhance our process of identifying potential threats.

Long-term initiatives:

- OPI is researching a new, more versatile threat management database to assist in analyzing protective intelligence information. The DOJ Justice Management

Division moved forward a request to OMB from the USMS for $1.1 million for a new threat management database for OPI for FY 2009. OPI will require the threat management database to have capability to analyze suspicious activity reporting (SAR). This will be used in conjunction with a counter-surveillance or surveillance detection program to collect SAR information. Previous information in JDIS will be merged into the new system.

- Interface PACER and the Case Management/Electronic Case Filing (CM/ECF) information on potential threateners into JDIS. (See number 3 above)

**5) Require the home alarm contractor to notify the USMS of alarm events after notifying the local law enforcement agency.**

Disagree: The USMS Off-Site Judicial Security Program Office has evaluated this subject through extensive consultation with senior USMS management and the national security vendor. The home alarm contractor follows USMS and industry established and approved protocol for alarm events. The USMS will be contacted by local law enforcement if the event occurring warrants USMS participation. The USMS believes this is a reasonable and appropriate program management decision to ensure judicial safety is given the highest priority while remaining cognizant of the agency's limited resources. We believe the current program policies for USMS notification of alarm events are prudent.

**6) Issue operational guidance for requesting and deploying Technical Operations Group resources and Rapid Deployment Teams.**

Concur: It should be noted that the current processes for requesting and deploying these resources are effective. The Chief of Technical Operations and all Technical Operation Group (TOG) personnel work to support the requests as they arise from districts. The TOG management coordinates and communicates effectively with JSD management, ensuring that appropriate resources are deployed in support of judicial security missions. We have provided training to 150 protective operations personnel and district threat investigators to ensure they are aware of the available technologies.

Likewise, the leadership of JSD has a clear understanding and drive to provide the resources necessary in case of a major incident. It should be noted that this report contains references to a Rapid Deployment Team response that is well within the new JSD everyday manner of doing business, and is not accurate. The Rapid Deployment Teams will be used for major events exceeding the capacity and resources of a USMS district. Currently, when a protective detail is activated, the Office of Protective Operations and the Office of Protective Intelligence respond in an extremely coordinated fashion to ensure the resources needed are placed quickly in the field, or moved to the location to support the mission. The Rapid Deployment Team will be utilized when an event exceeds that normal course. The USMS conducts protective details frequently, and often without the need for additional resources. In these cases, JSD, in partnership with the Investigative Services Division, ensures that all possible angles and techniques are

understood and being utilized to combat a threat. These policies will be issued in the first quarter of FY 2008.

We appreciate the courtesy of your professional staff and any further questions or additional information required, please contact Isabel Howell, USMS Liaison Audit Liaison on (202) 307-9744. Prompt resolution to these audit recommendations remains a high priority for the USMS.

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

On September 6, 2007, the OIG sent a copy of the draft report to the United States Marshals Service (USMS) with a request for written comments. In a memorandum dated September 28, 2007, the USMS provided a response in which it agreed with five of the report's six recommendations and described the actions it had taken or planned to take to implement the recommendations. The USMS disagreed with one recommendation. Based on our analysis of the USMS's response, four recommendations are resolved and remain open, and two recommendations are unresolved and remain open.

In its response, the USMS described a number of initiatives that it has undertaken to enhance its protective intelligence program from our initial March 2004 report to the present. The OIG has identified many of these initiatives in the current report and included in Appendix I a March 30, 2007, memorandum from the USMS that provides a detailed list of initiatives, some of which the USMS has completed and others it has planned. While the OIG acknowledges that these initiatives are important steps towards implementing the USMS's new threat analysis process and its protective intelligence program for identifying potential threats, we note, as discussed in our report, that the USMS has made only limited progress in implementing the major components of its judicial security program.

**Recommendation 1.** Develop a formal plan that defines objectives, tasks, milestones, and resources for the new threat assessment process.

**Status.** Resolved – open.

**Summary of the USMS Response.** The USMS concurred with this recommendation. The USMS identified actions that are part of its plan for a new threat assessment process. The USMS's Assistant Director for the Judicial Security Division issued a memorandum to the districts, dated September 10, 2007, on the new threat assessment process. He also announced that the Threat Management Center was activated on September 17, 2007. The USMS is eliminating the 3- and 7-day timeliness standards and updating the draft of Policy Directive 10.3, which should be completed by October 2007. Office of Protective

Intelligence (OPI) staff will be assigned to develop a formal plan for the new threat assessment process.

**OIG Analysis.** The actions undertaken and planned by the USMS are responsive to our recommendation. Please provide the OIG with copies of (1) the memorandum announcing the activation of the Threat Management Center which describes the Center's policies and procedures; (2) the September 10, 2007, memorandum; (3) the memorandum notifying the districts of the elimination of the 3- and 7-day standard; (4) Policy Directive 10.3; and (5) the formal plan that incorporates the policies and procedures defined in the documents referenced in the USMS response. The plan should define objectives, tasks, milestones, and resources for the new threat assessment process. By December 31, 2007, please provide the requested information or a status report describing the progress and expected completion dates.

**Recommendation 2.** Create a workload tracking system for threat assessments.

**Status.** Resolved – open.

**Summary of the USMS Response.** The USMS concurred with this recommendation, and stated that an OPI staff member will be assigned to develop a formal plan for a new workload tracking system. The USMS identified actions that are part of a plan for the new tracking system. Currently, OPI management uses a manual tracking system based on the Justice Detainee Information System to track the analysis of reported protective investigations. The system is used to produce weekly reports to monitor the status of the investigation as well as to perform research and analysis on national or regional trends. The system also is used to produce monthly status reports that detail the dates cases are received in OPI and what cases are still active investigations. OPI uses its manual system to ensure that case analyses are completed within the prescribed timeframes established by USMS policy. The system also can produce reports analyzing the workload distribution in OPI. Such reviews are used in making decisions about future work assignments.

**OIG Analysis.** The actions undertaken and planned by the USMS are responsive to our recommendation. This recommendation was intended to help ensure that the USMS did not permit a reoccurrence of a situation similar to the one in October 2006 when a backlog of 1,190 threat assessments had not been completed by OPI staff. So that the OIG can assess whether the new workload tracking system will enable USMS management to effectively manage the threat assessment

workload, please provide the OIG with a copy of the formal plan for the new workload tracking system being developed by OPI staff. The documents provided should include a complete listing of the data that will be tracked regarding the new threat analysis process and sample weekly and monthly reports. Please provide the requested information or a status report describing the progress and expected completion dates by December 31, 2007.

**Recommendation 3.** Develop a formal plan that defines objectives, tasks, milestones, and resources for implementing a protective intelligence function to identify potential threats.

**Status.** Unresolved – open.

**Summary of the USMS Response.** The USMS concurred with this recommendation, but in its response did not address how it intends to develop a formal plan defining objectives, tasks, milestones, and resources for implementing a protective intelligence function to identify potential threats. The USMS instead provided a description of specific activities it uses to collect information on potential threats. The USMS has also issued guidance on the type of judicial security information to be reported by the districts and has included the guidance in training being provided to its Criminal Investigators and Deputy U.S. Marshals.

**OIG Analysis.** Although the USMS concurred with the recommendation, we believe that the USMS description of its activities is not responsive to our recommendation. Although the USMS's response identifies multiple information sources that can be used to identify threats, it does not discuss what information will be collected, how it will be analyzed, or what reports will be prepared by its district staff to address potential threats. Nor did the USMS address how it will develop a formal plan that defines objectives, tasks, milestones, and resources for implementing a protective intelligence function to identify potential threats. By December 31, 2007, please provide the OIG with a copy of a formal plan, including examples of reports, or a status report on its development.

**Recommendation 4.** Modify USMS databases to support the new threat assessment process and protective intelligence function to identify potential threats.

**Status.** Resolved – open.

**Summary of the USMS Response.** The USMS concurred with this recommendation. The USMS stated that it has been modifying databases to identify potential threats, and that these initiatives will take place in two phases, one short-term and the other long-term.

**OIG Analysis.** The actions undertaken and planned by the USMS are responsive to our recommendation. To enable the OIG to assess the USMS's progress in implementing this recommendation, please provide the OIG with a status report on the implementation of the described short- and long-term initiatives by December 31, 2007.

**Recommendation 5.** Require the home alarm contractor to notify the USMS of alarm events after notifying the local law enforcement agency.

**Status.** Unresolved – open.

**Summary of the USMS Response.** The USMS disagreed with this recommendation. The USMS stated that its Off-Site Judicial Security Program Office has evaluated this issue through extensive consultation with senior USMS management and its home alarm contractor. The USMS stated that its home alarm contractor follows standard industry protocols for alarm events by first calling the resident's emergency point of contact and, if no response is received, contacting local law enforcement. According to the USMS, local law enforcement officials will contact the USMS if they determine the event warrants USMS participation. The USMS stated that it "believes this is a reasonable and appropriate program management decision to ensure judicial safety is given the highest priority while remaining cognizant of the agency's limited resources" and that the current policies for "USMS notification of alarm events at judicial residences are prudent."

**OIG Analysis.** The OIG does not agree with the USMS's position because the USMS's response does not demonstrate that the current protocol provides the USMS with timely information on alarm incidents necessary for it to fulfill its mission of protecting the judiciary. We are concerned that the current protocol makes local law enforcement responsible for determining when the USMS should be notified of an incident at a judge's residence and for notifying the USMS so that it may consider initiating a protective investigation.

We are also concerned that the current protocol offers too many opportunities for errors that would preclude a prompt USMS response to an incident. For example, under the current protocol, for the USMS to

consistently and promptly respond to incidents at federal judges' residences the many hundreds of different local law enforcement agencies that may respond to alarms at the more than 2,000 different judges' residences must (1) have current information from the USMS regarding which addresses are judges' residences; (2) consistently connect that information to the address when responding to an emergency call; (3) accurately identify that an incident may be pertinent to the USMS judicial security mission; and (4) promptly contact the appropriate USMS district office to inform the USMS of the incident. Merely maintaining local law enforcement's awareness of all judges' current addresses as judges are appointed, move, resign, or retire will be a difficult and time-consuming task for the USMS. In contrast, if the USMS arranges for its contractor to notify the USMS district office of an alarm incident after it has been reported to local law enforcement, the notifications will be accurate, immediate, and entirely within the control of the USMS and its single contractor.

The OIG requests that the USMS reconsider this recommendation that the USMS require its contractor to notify the USMS of alarm events after notifying the responsible local law enforcement agency. If the USMS maintains that the current protocol provides adequate protection to the judiciary, we request that the USMS provide a more complete response that demonstrates that in FY 2007 it was notified of home alarm incidents consistently and promptly to enable it to carry out its mission to protect the judiciary. Specifically, the OIG requests information that the USMS did not have available during our review: (1) a list of the local law enforcement agencies that received letters notifying them or providing updated information on federal judges' residences in their jurisdictions; (2) a list of the incidents since the contract was awarded in which the contractor notified a local law enforcement agency that an alarm had occurred at a judge's residence, by district; (3) when each local law enforcement agency subsequently notified the USMS district office of the incident; and (4) the action that the USMS district office took in each case. We request that the USMS inform us of its reconsideration and provide the requested information by October 31, 2007.

**Recommendation 6.** Issue operational guidance for requesting and deploying Technical Operations Group resources and Rapid Deployment Teams.

**Status.** Resolved – open.

**Summary of the USMS Response.** The USMS concurred with this recommendation. The USMS stated that policies addressing this recommendation will be issued in the first quarter of FY 2008.

**OIG Analysis.** The actions planned by the USMS are responsive to our recommendation. Please provide the OIG with formal operational guidance for requesting and deploying Technical Operations Group resources and Rapid Deployment Teams by December 31, 2007.