Audit of the U.S. Marshals Service Judicial Security Activities

★ ★ ★

21-083

JUNE 2021

EXECUTIVE SUMMARY

Audit of the U.S. Marshals Service Judicial Security Activities

(U) Objectives

(U) The objectives of this audit were to assess the United States Marshals Service's (USMS): (1) judicial security intelligence gathering and threat assessment capabilities, (2) judicial security resources and staffing, (3) Home Intrusion Detection System (HIDS) program, and (4) personal security training provided to judicial officials. The audit covers the USMS's judicial security activities from fiscal year (FY) 2016 through FY 2020.

(U) Results in Brief

(U//~~LES~~) We found that the USMS does not have the resources or proactive threat detection capabilities that the USMS has determined it needs to meet its protective services obligations for USMS-protected persons, including judges. While USMS officials have identified, and sought to implement, improvements to its protective intelligence and threat identification capabilities, we identified several serious challenges facing the USMS. For example, resource limitations and competing agency budget and staffing priorities have impeded the USMS's ability to provide the level of protective services that it has determined is required given the increasing number of threats directed at the judiciary. Further, the USMS does not have adequate proactive threat detection capabilities to monitor the current threat landscape, including in online and social media settings. Additionally, we found that the HIDS program does not offer judges important home security equipment and features [redacted] We also found that [redacted] judges are not participating in the HIDS program, and those judges who are participating use the equipment [redacted]. Finally, we identified areas where USMS policies should be established or revised to improve personal safety and security awareness briefings provided to USMS-protected persons.

(U) Recommendations

(U) Our report contains eight recommendations to improve the USMS's judicial security activities. We requested a response to our draft audit report from the USMS, which can be found in Appendix 3. Our analysis of their response is included in Appendix 4.

(U) Audit Results

(U) The USMS has the primary responsibility for ensuring the safety of the federal courts, including, but not limited to, protecting judicial officers, court employees, and judicial facilities. The USMS is responsible for protecting more than 2,700 sitting judges, the Deputy Attorney General, and approximately 30,000 federal prosecutors and court officials nationwide.

(U) We concluded that the USMS's resources and proactive threat detection capabilities are inadequate to fully meet its protective services obligations to judges and other USMS-protected persons. While the USMS has identified weaknesses in its judicial security capabilities, competing agency priorities have impeded the USMS's ability to fund the judicial security enhancements that it has identified. This is particularly concerning given that from FY 2016 to FY 2019, the USMS experienced an 89 percent increase in security incidents involving, and inappropriate communications and threats made to, USMS-protected officials.

(U) Resources and Staffing

(U) The USMS has determined that it is operating with a significant shortage of Deputy United States Marshals (DUSMs). According to the USMS, it needs about 1,200 additional DUSMs across the entire organization to fulfill its overall mission. When compared to the 3,885 DUSMs currently authorized, this represents a 24 percent agency-wide staffing shortage.

(U) The USMS's recent budget requests demonstrate that the organization believes its judicial security function is understaffed to the same degree. As of October 2020, the USMS's Office of Protective Intelligence (OPI) employed 43 full time staff and 200 DUSMs working on protective intelligence as only a part of their overall duties. OPI maintains that it requires a total of 583 full time employees, including 200 DUSMs dedicated fully to protective intelligence, to adequately meet its mission requirements. However, we found that prior to FY 2021, the USMS submissions for the President's Budget did not reflect the funding and staffing levels that the OPI determined it needed to accomplish its mission.

(U) In contrast, the USMS's FYs 2021 and 2022 budget requests include significant increases in funding and staff. In FY 2021, the USMS requested an additional $30.4 million and 19 full time equivalent (FTE) staff for its Judicial Security Division (JSD). However, even that FTE request was 129 FTEs less than JSD identified as necessary to implement the security initiatives in its FY 2020 budget request. Furthermore, in the USMS's most recent spend plan, JSD was given only a fraction of its request – $4.4 million and no additional FTEs – in FY 2021. The USMS's FY 2022 spring call budget request included an additional $35 million and 104 FTEs to bolster its judicial security operations.

(U) Intelligence Gathering and Threat Assessment

(U) We found that the USMS's threat detection capabilities are insufficient to proactively monitor the current threat landscape, which has largely moved to online and social media settings. Additionally, we found that the DUSMs responsible for conducting district-level threat investigation and mitigation perform this function as a collateral duty, and therefore are only dedicated to this responsibility on a part-time, rotational basis.

(U) In its USMS Protective Intelligence Enterprise Strategic Plan for FYs 2019-2022, OPI identified the shortcomings in its current protective intelligence and threat identification capabilities and established objectives and milestones it will seek to achieve to improve or correct those shortcomings. However, the USMS has not allocated the funding and resources requested by OPI to fully implement several of the remaining plan initiatives. We found that, in the 3 years since identifying 30 objectives in its strategic plan, OPI has completed only 4 of them, made some progress on 20 of them, and made no progress on the remaining 6. Ten of these 26 remaining objectives require additional funding before they can be completed.

(U) For example, OPI does not have the resources necessary to employ and adequately train DUSMs as full-time District Threat Investigators (DTIs), which OPI identified as the most important position in its protective intelligence operation. OPI's current 200 DTIs conduct threat investigation and mitigation as a collateral duty to their traditional DUSM responsibilities, and therefore are only part-time resources dedicated to this function. In addition, OPI has concluded that the DTI training curriculum is inadequate, as many DTIs are unable to operate independently even after completing the current 1-week DTI training course.

(U) Our review also found that the USMS lacks consistency in its policies and standard operating procedures related to protective intelligence and has not established policies and procedures for proactively identifying threats, which is a focus of OPI's recent efforts to improve its protective intelligence capabilities.

(U) Home Intrusion Detection System

(U//~~LES~~) We found that the HIDS program offers limited or outdated equipment options to its users, which could dissuade judges from opting into the program or force them to choose an alternative security system that suits their needs better but operates outside of the USMS's purview. For example, the HIDS program does not include the option of [redacted] and could provide additional protection from certain security threats.

(U//~~LES~~) We found that [redacted] percent of eligible federal judges choose to participate in the HIDS program. In addition, during the 33 months from January 2018 through September 2020, [redacted] percent of those federal judges participating in the HIDS program armed their HIDS alarm system each month, and roughly [redacted] percent did not arm their system at all. The HIDS Program Management Office had not determined why participation and system usage was [redacted].

(U) Personal Security Education

(U) The USMS is required to provide an orientation briefing to judicial nominees and newly appointed federal judges to communicate comprehensive knowledge and security practices that, if implemented,

should effectively aid in ensuring their safety while they are outside of the courthouse. Thereafter, the USMS is required to provide annual briefings to protected persons. However, we found that the USMS's policies and procedures for ensuring protected persons are regularly educated on offsite security measures are inadequate. As a result, we witnessed significant differences among districts in the frequency, content, administration, and documentation of the required annual briefing to USMS protected persons.

(U) Table of Contents

(U) Introduction

(U) The United States Marshals Service (USMS) stated mission is to protect, defend, and enforce the American justice system. The USMS has a wide variety of statutory responsibilities, including protecting the federal judiciary, apprehending federal fugitives, transporting and housing federal pre-trial detainees, locating and recovering missing children, enforcing sex offender compliance, operating the Witness Security Program, and managing and selling federally seized assets acquired by criminals through illegal activities. To address these responsibilities, in February 2021 the USMS employed 5,743 people and operated with a budget of $1.496 billion.

(U) In 2020, the USMS was responsible for protecting approximately 2,700 federal judges, the Deputy Attorney General, the Secretary of Education, U.S. Attorneys, and over 30,000 federal prosecutors and court officials spread over its 94 districts. The USMS's protective responsibilities are also extended to the immediate families of federal judiciary officials and include security measures both within and outside of federal facilities and courthouses. Historically, the safety of federal judges is at greater risk when they are away from the courthouse, as demonstrated by the July 2020 attack at the home of a federal judge during which the judge's son was murdered and the judge's spouse critically injured.

(U) In fiscal year (FY) 2020 the USMS responded to 4,261 threats or inappropriate communications against protected persons, an increase of 81 percent over the 2,357 threats made against the federal judiciary in FY 2016 and a roughly 233 percent increase from the 1,278 threats in FY 2008 that we referenced in the OIG's 2010 judicial security report.[1] Over the same timeframe, the USMS budget for judicial and courthouse security increased by about 49 percent, from $344 million to $473 million in FY 2016, to $514 million in FY 2021.[2]

(U) Judicial Security Division

(U) The USMS's Judicial Security Division (JSD) is responsible for protecting court officials and safeguarding the public by anticipating and deterring threats to the judiciary. JSD is comprised of nine program offices. Those related to our audit are outlined below.

(U) Office of Protective Intelligence

(U) The Office of Protective Intelligence (OPI) is responsible for providing direct support to field investigators and headquarters components to ensure that all threats to protected persons, facilities, and events are thoroughly investigated, assessed, and mitigated in a timely manner. As of October 2020, OPI is comprised of 43 full time headquarters-based personnel and 200 DUSMs at the district level whose judicial security

[1] (U) Report No. I-2010-002-R, Review of the Protection of the Judiciary and the United States Attorneys.

[2] (U) The USMS's budget for judicial and courthouse security decreased in FY 2017 to $463 million and again in FY 2018 and FY 2019 to $446 million. In addition to the USMS's judicial and courthouse security appropriation, the Administrative Office of the United States Courts transfers funding to the USMS each year – approximately $585 million in FY 2021 – to administer its Judicial Facility Security Program, which provides court security officers, security systems, and equipment to all federal court facilities. The Judicial Facility Security Program was not included in the scope of this audit.

duties are collateral obligations and not their sole responsibilities. The 200 district-based DUSMs are referred to as District Threat Investigators (DTI) and they conduct protective investigations and threat mitigation of USMS protected persons and facilities.

(U) OPI headquarters includes the Threat Management Center, Behavioral Analysis Unit, Counter-Surveillance/Surveillance Detection Unit, Partner Engagement, Investigations and Analysis Branches, and Circuit-based Operational Support Center.[3] The Threat Management Center serves as the agency's central repository for all threat information, protective assessments, and protective investigations. The Behavioral Analysis Unit employs an operational psychologist to improve the protective intelligence collection and investigation capabilities of the USMS. The Counter-Surveillance/Surveillance Detection Unit detects hostile surveillance and pre-attack planning against protected persons and facilities. OPI's three Investigations and Analysis Branches are comprised of more than half of the 43 full time headquarters personnel.

(U) Office of Protective Operations

(U) The Office of Protective Operations (OPO) is comprised of 36 USMS employees responsible for providing subject matter expertise, guidance, and direct support to district offices across all 12 federal judicial circuits on high-threat and high-profile proceedings and risk-based and threat-based protective operations. OPO is also responsible for providing permanent protection details for the Deputy Attorney General and the Secretary of Education.

(U) National Center for Judicial Security

(U) The National Center for Judicial Security (NCJS) is comprised of 10 USMS employees who provide subject matter expertise, training, and development for worldwide endeavors related to court security, the protection of the judiciary, and securing the rule of law. NCJS prepares and publishes various guidance and informational bulletins on judicial security matters, including the primary publication used to educate judiciary members on offsite personal security. NCJS also oversees the Home Intrusion Detection System (HIDS) program, which provides for the installation, maintenance, and alarm monitoring of electronic security systems in the homes of participating federal judges.

(U) OIG Audit Approach

(U) Our objectives were to assess the USMS's: (1) judicial security intelligence gathering and threat assessment capabilities, (2) judicial security resources and staffing, (3) HIDS program, and (4) personal security training provided to judicial officials. The scope of our audit generally covers the USMS's judicial security activities from FY 2015 through FY 2020.

(U) To accomplish our objectives, we interviewed USMS personnel, including officials from JSD and the Financial Services Division, and the federal judge who chairs the U.S. Court's Committee on Judicial Security. We also examined contract requirements for the HIDS program to determine what equipment is offered to participating judges. Finally, we evaluated the USMS's judicial security policies and procedures, and reviewed documentation related to security training provided to judiciary members to ensure it adhered to

[3] (U) The USMS provides security to the 94 federal court districts and 12 federal judicial circuits of the U.S. Court of Appeals.

policy requirements. Due to the COVID-19 pandemic, this audit was conducted remotely. Additional information about the audit's objectives, scope, and methodology is available in Appendix I.

(U) Audit Results

(U) We found that the USMS does not have the resources or proactive threat detection capabilities that the USMS's JSD has determined it needs to meet its protective services obligations for USMS-protected persons, including judges. While the USMS has recently undertaken several important initiatives to address shortcomings in its judicial security capabilities, the USMS continues to face several serious challenges in its effort to fulfill its statutory responsibilities in this area. First, the USMS faces significant budget and staffing issues across the organization. Second, competing agency priorities and resource limitations have impeded JSD's ability to fully implement its plan for protective intelligence and threat assessment that could help it successfully detect threats and deter violence against protected judiciary members and their families. Third, the HIDS program does not offer judges home security equipment commonly provided by other home security providers. Finally, we identified areas where USMS policies should be established or revised to improve personal safety and security awareness training provided to protected officials.

(U) The USMS Faces Significant Resource and Staffing Challenges

(U) The USMS determined in December 2020 that it is operating with a significant staffing shortage across its entire organization. The USMS utilizes a District Staffing Model (DSM), based on the prior fiscal year workload data, that uses 177 formulas and more than 200 data elements to calculate the total number of Full Time Equivalent (FTE) staff recommended to accomplish the district's workload if funding constraints were not a consideration.[4] Based upon the DSM, the USMS needs approximately 1,200 additional DUSMs than currently authorized to meet the demands of the districts' workload. An additional 1,200 DUSMs would represent a staffing increase of approximately 31 percent when compared to the USMS's current authorization of 3,885 DUSMs.

(U) The USMS's FY 2021 budget request that it submitted to the Department demonstrates that the organization believes it is similarly understaffed in the area of judicial security. Specifically, the USMS requested support from the Department for an additional 18 positions and $30.4 million for judicial protection —representing increases of 25 percent and 144 percent, respectively, over the prior fiscal year — to bolster the judicial security mission by strengthening OPI and Protective Operations. As noted above, the USMS's FY 2021 budget for judicial and courthouse security was $514 million and included funding for 1,722 staff positions. However, only a fraction of that funding and staff was given to JSD, which received $26.7 million and funding for 206 staff positions in FY 2021. The remainder is used to maintain the security of federal court facilities throughout the country and the security of in-custody defendants during court proceedings.

(U) However, we found that in prior years, the USMS President's Budget requests submitted to the Justice Management Division (JMD) did not reflect the funding and staffing levels that JSD requested to accomplish its mission. For example, in the USMS FY 2020 internal spring call budget justification JSD requested additional funds of approximately $15.5 million and 148 additional FTEs to implement several judicial security program initiatives. According to the USMS's Chief Financial Officer, the agency's FY 2020 President's Budget submission did not include the additional funding and FTEs necessary to implement JSD's

[4] (U) FTE is used to quantify employment as a function of hours worked rather than by the number of individual employees. One FTE is also known as one work year and is equivalent to 2,080 hours of work.

judicial security initiatives. Table 1 shows the initiatives that JSD planned to implement if it had received the funding and FTEs requested in its FY 2020 internal USMS spring call budget submission.

UNCLASSIFIED	
Table 1: JSD Judicial Security Improvement Initiatives	
Program Initiative	**Description**
District Judicial Security Inspectors (JSI)	Hire additional JSIs to develop, administer, and oversee judicial security within a USMS district.
Intelligence Research Specialist Job Analysis	Review and analyze the roles of Intelligence Analysts and Intelligence Research Specialists (IRS) and develop a career management guide and roadmap for those job series.
Threat Management Center (TMC)	Hire additional USMS staff and contractors to increase TMC operations and facilitate organizational changes to the TMC.
OPO Inspectors	Hire and train additional USMS staff to provide districts with support and localized expertise in protective operations.
Light Armored Vehicles (LAVs)	Fund a multi-year cyclical replacement of LAVs used for protective details in the field.
Special Assignments	Properly staff and secure threat based protective details and risk-based judicial security events.
Office of Security Systems Countermeasures	Modernize electronic security equipment in USMS-occupied space and facilities.
District Protective Intelligence Inspectors	Hire additional Protective Intelligence Inspectors responsible for protective investigations and assessments within a USMS district.
Counter Surveillance/ Surveillance Detection (CS/SD)	Hire additional IRS positions to identify hostile surveillance of protected persons and fund other operational CS/SD mission costs.
Data Scientists	Hire additional Data Scientists to analyze data to inform business decisions and risk mitigation measures; and fund hardware, software, training, and travel.
Cyber Investigation Unit	Hire additional specialists to conduct open source intelligence and social media Protective Investigations; and purchase computer equipment to support it.
Behavioral Analysis Unit	Hire additional psychologists and other staff to support the USMS's Behavioral Analysis Unit, implement agency-wide training on JSD mission areas, and fund curriculum development.
OPI Analysis and Production	Hire an OPI technical writer to support intelligence production efforts; and fund OPI software, training, and travel.
Intelligence Liaison Positions	Hire additional USMS staff and contractors to act as liaisons with other federal intelligence entities.

Source: USMS

(U) While the USMS's past President's Budget submissions did not fully fund judicial security, the USMS's spring call budget requests for FY 2021 and FY 2022 included significant funding and staffing increases. As previously stated, in its FY 2021 budget request, the USMS included an additional $30.4 million and 18 FTEs to bolster its judicial security mission. However, this was still 130 FTEs less than JSD identified in FY 2020 as

necessary to implement its security initiatives. Additionally, once the USMS FY 2021 budget was approved, JSD was only given an additional $4.4 million - a fraction of its budget request - and no additional FTEs. In its FY 2022 spring call request, the USMS included an additional $35 million and 104 FTEs to increase protection capacity, enhance threat investigation and mitigation capabilities, and keep pace with the evolving threat landscape. In our judgment, granting these requests may help address the DUSM staffing shortage; however, the USMS should continue pursuing resources to help enable JSD to achieve its judicial security mission objectives.

(U) The USMS Needs to Improve its Proactive Threat Detection Capabilities

(U) We found that the USMS's threat detection capabilities are insufficient to proactively monitor the current threat landscape, which has largely moved to online and social media settings. Additionally, we found that the DUSMs responsible for conducting district-level threat investigation and mitigation perform this function as a collateral duty, and therefore are only part-time resources dedicated to this responsibility. OPI is aware of these shortcomings and has developed and begun implementing several initiatives to improve the USMS's protective intelligence capabilities.[5]

(U) In 2018, OPI published its USMS Protective Intelligence Enterprise Strategic Plan FYs 2019-2022, which identified challenges facing the organization and goals for OPI's protective responsibilities.[6] The Strategic Plan acknowledged that the USMS was overextended with current protective intelligence and threat investigations and unable to handle the growing workload, as OPI experienced an 89 percent increase in security incidents, inappropriate communications, and threats made to USMS-protected persons from FY 2016 to FY 2019. The Strategic Plan further stated that threat actors' abilities outpace the USMS's threat detection capabilities, which forces the agency into a reactionary posture that relies on threats being reported to OPI by the recipient, creating vulnerabilities that put USMS-protected persons at risk. OPI determined that the primary driver of its reactionary posture stems from the fact that DUSMs performing the DTI function do so as a collateral duty, and therefore are dedicated to it only on a part-time basis.

(U) OPI determined that it must pursue advanced technologies and practices that improve its protective investigation capabilities. The Strategic Plan identified the following three goals to address its shortcomings:

- (U) Goal 1: Detect, deter, and disrupt threats to USMS protected persons and enhance their security.
- (U) Goal 2: Institutionalize an investigative culture within the USMS enterprise.
- (U) Goal 3: Modernize the USMS workforce and the policies and procedures that guide the agency.

[5] (U) In contrast with the USMS's protective capabilities, the Federal Bureau of Investigation's Protective Operations Unit, which is responsible for protecting the Attorney General, the FBI Director, and the FBI Deputy Director, has substantial protective capabilities and resources at its disposal.

[6] (U) OPI is currently revising and refreshing its strategic plan objectives to reflect recent programmatic changes. It expects to submit a draft plan for review and approval in June of 2021.

(U) Each goal is comprised of 10 corresponding objectives, all of which include project milestones or deliverables that allow OPI to track its progress toward achieving the objective. Project milestones range from simple tasks like obtaining project plan approvals and developing policy and procedural documents, to more complex and resource-heavy deliverables such as hiring and training staff or achieving a fully operational intelligence unit. In total, the Strategic Plan included 179 project milestones or deliverables. All 30 objectives, including our assessment of OPI's progress toward achieving the objective, are shown in Appendix 2.

(U) We assessed OPI's progress towards completing the 30 objectives identified in its Strategic Plan and determined that, in the 3 years since publishing the plan, OPI has completed 4 objectives, made progress on 20 objectives, and made no progress toward 6 objectives. Ten of the 26 remaining objectives require additional funding before they can be completed. We also assessed OPI's progress toward achieving the 179 project milestones and found that it has completed 59 milestones and made progress on 26 additional milestones. OPI has not made progress toward the remaining 94 milestones representing 53 percent of all project milestones. Table 2 shows the completion status of all OPI strategic plan objectives and project milestones as of January 2021.

UNCLASSIFIED

Table 2: Status of OPI Strategic Plan Objectives and Milestones as of January 2021

Status	Objectives	Project Milestones/Deliverables
Completed	4	59
In Progress	20	26
No Progress	6	94
Total	**30**	**179**

Source: OIG

(U) In our judgment, the USMS Protective Intelligence Enterprise Strategic Plan FYs 2019-2022 demonstrates that the USMS is aware of its shortcomings related to protective intelligence and investigation and has identified the actions necessary to improve its operational capabilities in this area. However, the current amount of USMS resources allocated to these improvements has hampered OPI's ability to complete its Strategic Plan objectives. For example, not only does OPI need additional resources to establish its Open Source Intelligence Unit to collect and analyze online threats, but it also needs funding to equip districts with managed attribution internet access that conceals the identities of OPI personnel and their affiliation with the USMS. Without these capabilities the safety and security of USMS-protected persons could be at increased risk from undetected threats.

(U) OPI Protective Intelligence Enterprise Reformation Plan

(U) Along with its Strategic Plan, OPI created an internal Protective Intelligence Enterprise Reformation Plan in early 2018 to inform USMS management of the resources it needs to address current judicial security shortcomings and detail how OPI planned to reform its operations. The Reformation Plan identified the need for an additional $18.6 million in funding and 340 additional personnel, representing increases of

approximately 1,329 and 140 percent of FY 2020 OPI funding and staff levels, respectively, to transition OPI's threat identification capabilities from its current reactionary posture into a proactive one. In an interview with the OPI Chief, he stated that many of the threats that appear on the internet go undiscovered because OPI does not have the resources to uncover them. Through implementing the Reformation Plan, OPI seeks to establish new headquarters, circuit, and district-based functions designed to improve the USMS's proactive threat identification, assessment, and mitigation capabilities. As previously mentioned, this includes the establishment of an Open Source Intelligence Unit that will enable the USMS to proactively monitor online content and identify threats that may have previously gone undetected. To begin implementing the Reformation Plan, the USMS requested approximately $10 million in supplemental funding for the Open Source Intelligence Unit but did not include funds for the remaining items and personnel requested in the Reformation Plan. In our judgment, the enhanced capabilities provided through full implementation of the Reformation Plan, with proper management and oversight, will improve the USMS's ability to ensure the safety of individuals under its protection. Therefore, we recommend the USMS review OPI's Protective Intelligence Enterprise Reformation Plan and determine and pursue the actions necessary to achieve desired threat identification, assessment, and mitigation capabilities.

(U) District Threat Investigators

(U) DTIs are a component of the current OPI structure as well as the new structure outlined in the Protective Intelligence Enterprise Reformation Plan. OPI determined that DTIs are the most important positions in its protective intelligence operation, but, as previously mentioned, the DTI assignment is a collateral duty. In addition, OPI stated that DUSMs often rotate in and out of the DTI role, and that their skills necessary to perform the job require regular refresher training. According to the OPI Chief, the fact that DUSMs performing the DTI function do so as a collateral duty, on a part-time and rotational basis, presents increased risk to USMS protected persons, as the workload demands the position be full time.

(U) To exacerbate matters, an OPI official stated that the previous DTI training curriculum proved to be inadequate as DTIs were frequently unable to operate autonomously after completing the 1-week training course. According to a JSD official, due to a lack of designated funding for DTI training and the need to overhaul the training curriculum, only 24 DTIs received training in the past 3 years. However, they now offer two DTI training courses – a basic course and an advanced course – that allows more DTIs to receive training each year. According to OPI, given that the DTI is a collateral duty position, performed on a part-time basis with rotating participation, it would be impossible to conduct regular initial and refresher training for all DTIs under its current resource allocation. Therefore, we recommend that the USMS assess the status and training requirements of the DTI position to determine if it meets the needs of the judicial security program and make any necessary adjustments to ensure an adequate number of DTIs are dedicated on a full-time basis to this function, are appropriately trained and are operational.

(U) Protective Intelligence Policy

(U) During our review of USMS policies and procedures related to judicial security, we found that the USMS lacks consistency in its policies and standard operating procedures related to protective intelligence. Current USMS policy related to this area has been revised several times over the years and consequently, certain aspects of the policy are contradictory or outdated. To ensure all USMS judicial security personnel operate in a similar manner, we recommend that the USMS update the policies and standard operating procedures guiding its protective intelligence and threat assessment to ensure they align with approved practices. Further, we determined through our review of the policies that the USMS does not have

documented policies or procedures for proactively identifying threats, which is a focus of the OPI's Protective Intelligence Enterprise Reformation Plan. Therefore, we recommend that the USMS establish policy guiding its proactive threat identification practices.

(U) The USMS's Home Intrusion Detection System Does Not Include Certain Important Security Protections

(U//~~LES~~) The HIDS program was initiated in December 2005 and provides certain intrusion detection equipment, maintenance, and monitoring services [redacted] of participating federal judges. This voluntary program is offered to all active federal judges; however, as of September 2020, [redacted] percent of federal judges have opted into the program. However, the equipment and services offered by the HIDS program do not include certain important protections [redacted]

(U//~~LES~~) The current HIDS contract was awarded in June 2015 to perform installation, maintenance, and monitoring of HIDS alarm systems over a period of 5 years.[7] As of September 2020, [redacted] systems are active under the HIDS program. Each residence is equipped with components selected from a standard list. The basic system configuration covers [redacted]

- [redacted]
- [redacted]
- [redacted]
- [redacted]
- [redacted]
- [redacted]

(U//~~LES~~) Judges also have the option, at their own expense, of installing a HIDS system [redacted], and adding additional equipment [redacted]. We believe the USMS should assess whether the security risks to federal judges warrant extending home security protection [redacted], as we understand is offered to other senior Department officials.

(U//~~LES~~) We spoke with the federal judge who chairs the U.S. Court's Committee on Judicial Security, who expressed concerns with the HIDS program equipment, stating that the annual funding given to the USMS is adequate for installing new systems, but is not enough to cover regular maintenance or technology

[7] (U) The current HIDS contract, originally set to expire on September 30, 2020, was extended until March 31, 2021.

upgrades. We examined commonly available features of other home security systems. We found that most other home security systems provide similar equipment, but also offer additional capabilities [redacted]. We noted that features offered by the HIDS program are generally designed to alert designated individuals, as well as local law enforcement, that an [redacted], the judge's home. However, judicial threats can also involve an individual simply walking up to the judge's front door and ringing the doorbell, as was the case in the July 2020 attack at the home of a federal judge by an assailant disguised as a delivery person. The current HIDS equipment offerings [redacted]. Table 3 shows a comparison of the features available under the HIDS program and features of other commonly available systems.

(U//~~LES~~) Table 3: Home Security System Features

[redacted]	[redacted]	[redacted]
(U//~~LES~~) [redacted]	[redacted]	[redacted]
(U//~~LES~~) [redacted]	[redacted]	[redacted]
(U//~~LES~~) [redacted]	[redacted]	[redacted]
(U//~~LES~~) [redacted]	[redacted]	[redacted]
(U//~~LES~~) [redacted]	[redacted]	[redacted]
(U//~~LES~~) [redacted]	[redacted]	[redacted]
(U//~~LES~~) [redacted]	[redacted]	[redacted]
(U//~~LES~~) [redacted]	[redacted]	[redacted]
(U//~~LES~~) [redacted]	[redacted]	[redacted]
(U//~~LES~~) [redacted]	[redacted]	[redacted]
(U//~~LES~~) [redacted]	[redacted]	[redacted]
(U//~~LES~~) [redacted]	[redacted]	[redacted]

Source: USMS and OIG

(U) We are further concerned that the limited equipment options that the HIDS program offers to its users could dissuade judges from opting into the program if they deem it inadequate, or cause them to choose an alternative security system that suits their needs better, but does not involve the USMS.

(U//~~LES~~) We found that of the approximately 2,700 federal judges, [redacted] were participating in the HIDS program. Additionally, the monthly usage information that we obtained for all active HIDS users between January 2018 and September 2020 showed that, on average, [redacted] percent of participating judges armed their alarm system in any given month. Additionally, between [redacted] percent of users did not arm their alarm system at all over that same timeframe. The HIDS Program Manager was unable to explain why all

participating judges do not regularly arm their systems, stating that the systems are installed for the judges to use at their discretion. However, he did speculate that judges opt out of the HIDS program because they prefer to pay for their own security system, believe they have better alternatives available to them, or simply are not satisfied with what the HIDS system has to offer.

(U//~~LES~~) In our judgment, the USMS needs to determine why [redacted] percent of federal judges have opted out of the HIDS program, and why [redacted] judges who have opted into the program do not regularly arm their system. Without this knowledge, the USMS cannot assure that the HIDS program adequately meets the needs of the federal judges it is responsible for protecting. Therefore, we recommend that the USMS solicit input from judges eligible to participate in the HIDS program to determine what home security features they want made available to them [redacted] and determine the feasibility of incorporating those features into the next HIDS contract requirements We also recommend that the USMS explore options for upgrading current and future intrusion detection equipment to address present day security threats, as well as the needs of its users.

(U) The USMS's Personal Security Education Practices Need Improvement

(U) The USMS's procedures for judicial security require the USMS to provide judicial nominees and newly appointed federal judges an orientation to inform them of the roles and responsibilities of the USMS. During the orientation, USMS personnel discuss the roles of the district-level judicial security officers, threats, OPI, the HIDS program, and any other pressing issues or questions the judge may have. USMS personnel also provide judges with several publications and training aids that help ensure their personal safety and security. One such document is USMS Publication 94, Offsite Security, which is a formal JSD publication with comprehensive guidelines for maintaining security awareness while outside of the courthouse. Publication 94 covers topics such as internet and home security, identity theft, commuting routines, travel, and responding to threats. It also explains the USMS's role in providing and ensuring judicial security. In our judgment, the required orientation of new judges and judicial nominees, particularly the inclusion of USMS Publication 94, provides protected persons with comprehensive knowledge and security practices that, if implemented, would aid in ensuring their safety while they are outside of the courthouse. We noted, however, that the USMS's policy does not specify how USMS officials are to document completion of the orientation, or a method to ensure all new judiciary members receive their orientation in a timely manner.

(U) We also found that USMS policy does not specifically require districts to provide refresher training on the topics covered during initial orientation. USMS policy requires districts to provide an annual "briefing" to USMS-protected persons. However, the content of the briefing is not provided or specified but left open to each district's discretion. The policy also requires USMS district management to ensure protected persons are familiar with identifying threats, inappropriate communications, incidents, and suspicious activity and the procedures for reporting them to the USMS. However, the policy does not address other important areas of offsite security, such as those covered in Publication 94. Additionally, while USMS policy requires the notification, subject, and attendance of these briefings to be "documented locally," it does not specify how it should be tracked and retained and does not enable judicial security officials to ensure that USMS-protected persons are regularly receiving this important security information.

(U) We assessed how several USMS districts complied with these requirements by examining training documentation that we received from 78 of the 94 USMS districts. The other 16 districts did not respond to

our request for training documentation. For the 78 districts, we determined whether the districts' most recent training documentation was maintained in accordance with USMS policy. We found that only 25 of the 78 districts fully complied with the requirement to document the notification, subject, and attendance at security briefings, while 53 districts partially complied by documenting at least 1 of the 3 briefing requirements, and 2 districts did not comply with policy because the documentation maintained was either inadequate or nonexistent. Further, we witnessed significant differences among the 78 districts in the frequency, content, administration, and documentation of the required annual briefing. For example, some districts prepared formal presentation slides, while others created an agenda of topics to be discussed but did not develop a formal presentation. Additionally, some districts conducted one-on-one briefings with federal judges while others, on occasion, simply emailed USMS publications and other security-related documents to judges. In our judgment, these variances are a result of the ambiguous requirements for the annual briefing outlined in the USMS's policy.

(U) During our examination of the training documentation, we also identified 1 action taken by 3 of the 78 districts that we consider to be a best practice and that we believe should be implemented throughout the USMS to ensure all USMS-protected person regularly receive critical security information that will help keep them safe: the use of Form USM-50Z, *Protected Persons Profile & Security Brief Tracking Report*, to track completion of annual security briefings to protected persons. According to the instructions on Form USM-50Z, it must be completed annually and updated as necessary in accordance with JSD policy. Despite these instructions, the document is not mentioned in JSD policy, which may be why it is not widely used.

(U) In our judgment, the USMS's policies and procedures for ensuring protected persons are regularly educated on offsite security measures are inadequate. Since each USMS district decides what information to include in its required annual briefings to these individuals, key information may be inadvertently omitted. Therefore, we recommend that the USMS use its Publication 94 to develop a standard agenda of key topics for required annual security briefings to USMS-protected persons and revise its Judicial Security Policy Directive to require that these topics be briefed annually to each individual under its protection. We also recommend that the USMS revise its Judicial Security Policy Directive to require districts to use Form USM-50Z to track completion of required annual security briefings to USMS-protected persons and retain those records, by fiscal year, for a period of at least 3 years.

(U) Conclusion and Recommendations

(U//~~LES~~) USMS officials have identified the need for improvements to its protective intelligence and threat identification capabilities, without which the USMS's ability to ensure the safety of USMS-protected persons may be adversely impacted. However, we found that competing agency priorities have impeded the USMS's ability to fund the judicial security enhancements that it identified. In addition, we found that the HIDS program has not kept pace with modern home security technology, that the rate of participation among judges eligible for home security equipment offered under the HIDS program is [redacted], and that the use of the equipment by participating judges is [redacted]. Because the USMS could not identify the reasons for these [redacted] participating and usage rates, we believe the USMS should solicit input from eligible judges to determine how it can improve participation and usage, and whether including additional commonly available products would better meet the needs of participating federal judges. Finally, the USMS needs to improve the personal security training provided to judiciary members to ensure they are equipped with the proper knowledge of how to maximize their security awareness and help ensure their safety. As a result, we make eight recommendations to improve the USMS's judicial security activities.

(U) We recommend that the USMS:

1. (U) Review OPI's Protective Intelligence Enterprise Reformation Plan and protective intelligence capabilities at other DOJ components such as the FBI and determine and pursue the actions necessary to achieve desired threat identification, assessment, and mitigation capabilities.

2. (U) Assess the status and training requirements of the DTI position to determine if it meets the needs of the judicial security program and make any necessary adjustments to ensure an adequate number of DTIs are dedicated on a full-time basis to this function, are appropriately trained, and are operational.

3. (U) Update the policies and standard operating procedures guiding its protective intelligence and threat assessment to ensure they align with approved practices.

4. (U) Establish policy guiding its proactive threat identification practices.

5. (U//~~LES~~) Solicit input from judges eligible to participate in the HIDS program to determine what home security features they want made available to them, [redacted], and determine the feasibility of incorporating those features into the next HIDS contract requirements.

6. (U) Explore options for upgrading current and future intrusion detection equipment to address present day security threats, as well as the needs of its users.

7. (U) Use its Publication 94 to develop a standard agenda of key topics for required annual security briefings to USMS-protected persons and revise its Judicial Security Policy Directive to require that these topics be briefed annually to each individual under its protection.

8. (U) Revise its Judicial Security Policy Directive to require districts to use Form USM-50Z to track completion of required annual security briefings to USMS-protected persons and retain those records, by fiscal year, for a period of at least 3 years.

(U) APPENDIX 1: Objectives, Scope, and Methodology

(U) Objectives

(U) The objectives of the audit were to assess the USMS's: (1) judicial security intelligence gathering and threat assessment capabilities, (2) judicial security resources and staffing, (3) HIDS program, and (4) personal security training provided to judicial officials.

(U) Scope and Methodology

(U) Our audit covers the USMS's judicial security activities, including threat assessment and mitigation, protective intelligence and investigations, offsite security, the HIDS program, staff and resource allocations, and personal security training provided to USMS-protected persons from FY 2015 through FY 2021. To accomplish our objectives, we interviewed personnel responsible for certain aspects of the USMS's judicial security, including OPI, the Office of Security Systems, the Office of Financial Management, and the NCJS. We also interviewed the Chair of the U.S. Court's Committee on Judicial Security, and the Federal Bureau of Investigation's Protective Operations Unit Chief. Additionally, we evaluated USMS policies and procedures guiding its judicial security activities to ensure they were current, comprehensive, and cohesive. Our primary references were Sections 10.1 through 10.12 of the USMS's Policy Directive, the JSD Standard Operating Procedures for OPI, OPO, NCJS, and the HIDS Program.

(U) We examined several USMS publications, forms, and informational bulletins related to judicial security such as Publication 94, Offsite Security; Publication 202, Guide to Protective Investigations and Threat Management; Form USM-50, Judicial Personnel Profile; and Form USM-50Z, Protected Persons Profile and Security Brief Tracking Report. We also assessed the USMS's Protective Intelligence Enterprise Strategic Plan for FY 2019 through FY 2022 to identify the agency's progress in meeting its protective intelligence goals. In addition, we evaluated USMS funding and staffing levels to determine if they have impacted the success of JSD's judicial security responsibilities. Finally, we examined district-level training documentation on judicial security briefings and security awareness.

(U) Statement on Compliance with Generally Accepted Government Auditing Standards

(U) We conducted this performance audit in accordance with generally accepted government auditing standards (GAGAS). Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

(U) Internal Controls

(U) In this audit, we performed testing of internal controls significant within the context of our audit objectives. We did not evaluate the internal controls of the USMS to provide assurance on its internal control structure as a whole. USMS management is responsible for the establishment and maintenance of internal controls in accordance with OMB Circular A-123. Because we do not express an opinion on the

USMS's internal control structure as a whole, we offer this statement solely for the information and use of the USMS.[8]

(U) In planning and performing our audit, we identified the following internal control components and underlying principles as significant to the audit objectives:

(U) Internal Control Components & Principles Significant to the Audit Objectives	
Control Environment Principles	
	(U) Management should establish an organizational structure, assign responsibility, and delegate authority to achieve the entity's objectives.
	(U) Management should demonstrate a commitment to recruit, develop, and retain competent individuals.
Risk Assessment	
	(U) Management should define objectives clearly to enable the identification of risks and define risk tolerances.
	(U) Management should identify, analyze, and respond to risks related to achieving the defined objectives.
	(U) Management should identify, analyze, and respond to significant changes that could impact the internal control system.
Control Activity Principles	
	(U) Management should design control activities to achieve objectives and respond to risks.
	(U) Management should implement control activities through policies.
Information & Communication Principles	
	(U) Management should use quality information to achieve the entity's objectives.
	(U) Management should internally communicate the necessary quality information to achieve the entity's objectives.

(U) We assessed the design, implementation, and operating effectiveness of these internal controls and identified deficiencies that we believe could affect the USMS's ability to effectively and efficiently operate, and to ensure compliance with laws and regulations. However, because our review was limited to internal control components and underlying principles determined to be significant to the audit objectives, it may not have disclosed all deficiencies that may have existed at the time of this audit. The internal control deficiencies we found are discussed in the Audit Results section of this report.

(U) Compliance with Laws and Regulations

(U) In this audit we also tested, as appropriate given our audit objectives and scope, selected transactions, records, procedures, and practices, to obtain reasonable assurance that the USMS's management complied with federal laws and regulations for which noncompliance, in our judgment, could have a material effect on

[8] (U) This restriction is not intended to limit the distribution of this report, which is a matter of public record.

the results of our audit. Our audit included examining, on a test basis, the USMS's compliance with the following law that could have a material effect on the USMS's operations:

- 28 U.S.C. 566 § (e)(1)(A).

(U) This testing included assessing the USMS's judicial security policies and procedures to ensure they aligned with the agency's statutory authority to provide for the personal protection of the federal judiciary. However, nothing came to our attention that caused us to believe that the USMS was not in compliance with the aforementioned law.

(U) APPENDIX 2: USMS Protective Intelligence Enterprise Strategic Plan FYs 2019-2022 Objectives

(U) Strategic Plan Objective	Status	Additional Funding Required
(U) Objective 1.1: Partner with the Courts, Cabinet Agencies, and the Department of Justice to identify emerging vulnerabilities and alert protected persons, investigators, and analysts of those vulnerabilities before they can be exploited.	No Progress	
(U) Objective 1.2: Partner with the Courts, Cabinet Agencies, and the Department of Justice to inform protected persons of emerging threats (cyber-attacks, ride sharing, etc.) and educate them in proactive mitigation steps.	No Progress	
(U) Objective 1.3: Integrate open source collection and analysis and social-media exploitation into Protective Investigations	Completed	
(U) Objective 1.4: Gain, maintain and leverage access to inter-agency, commercial, and academic databases and research services.	In Progress	
(U) Objective 1.5: Enhance Enterprise counter-surveillance, surveillance detection and surveillance capability.	In Progress	√
(U) Objective 1.6: Establish Enterprise Intelligence requirements and seek Intelligence and Law Enforcement Community adoption.	In Progress	
(U) Objective 1.7: Transform the Threat Management Center into a Threat Information Sharing and Analysis Center.	In Progress	√
(U) Objective 1.8: Embed OPI Inspectors and Analysts in Regional & State Fusion Centers across the Country.	In Progress	√
(U) Objective 1.9: Develop and institutionalize a Judicial Security Risk Management process.	In Progress	
(U) Objective 1.10: Establish an Enterprise Confidential Human Source program.	No Progress	√
(U) Objective 2.1: Introduce threat investigations into the Deputy U.S. Marshal basic course.	In Progress	
(U) Objective 2.2: Establish a Judicial Security Training Center and conduct joint inspector, investigator, and analyst training.	In Progress	
(U) Objective 2.3: Revamp the Protective Investigations Training Program (PITP), incorporate a scenario-based curriculum, and expand it as necessary.	In Progress	
(U) Objective 2.4: Detail District investigators into OPI for 30 days within 1 year of appointment as an investigator.	Completed	
(U) Objective 2.5: Develop an Advanced PITP and administer it annually.	Completed	
(U) Objective 2.6: Develop a certification/accreditation program in partnership with threat associations.	No Progress	√
(U) Objective 2.7: Develop a continuing education program, encourage, and reimburse membership in professional threat associations, and include participation in annual performance initiatives.	In Progress	

Cont'd

(U) Strategic Plan Objective	Status	Additional Funding Required
(U) Objective 2.8: Reinforce the importance of protective investigations and intelligence to District leadership through new and existing training venues.	In Progress	
(U) Objective 2.9: Conduct annual Circuit and Enterprise conferences, monthly conference calls by Circuit, and produce weekly operational summaries for Enterprise consumption.	Completed	
(U) Objective 2.10: Incorporate protective intelligence performance measures into District leadership's performance plans.	No Progress	
(U) Objective 3.1: Revise protective investigations and intelligence policy and publications to clarify authority, scope, roles, responsibilities, guidelines and incorporate modern investigative and analytical techniques.	In Progress	
(U) Objective 3.2: Establish a secure web portal that allows for Circuit-based requirements management and feedback, improves information sharing, and enables targeted dissemination of intelligence products germane to each Circuit.	In Progress	
(U) Objective 3.3: Establish policy for and resource the Districts with managed attribution internet access to facilitate social media exploitation in the field.	No Progress	√
(U) Objective 3.4: Establish and sustain Circuit-centric "Investigator toolkits".	In Progress	
(U) Objective 3.5: Establish SECRET level communication systems/protocols in each District.	In Progress	√
(U) Objective 3.6: Seek administrative subpoena authority.	In Progress	
(U) Objective 3.7: Establish a USMS Career Path Guide for threat investigators and analysts.	In Progress	√
(U) Objective 3.8: Improve Enterprise planning, programming, budgeting and execution.	In Progress	
(U) Objective 3.9: Invigorate the Judicial Security Division's research, development, testing, and evaluation capability to test, evaluate, acquire, and enable Enterprise access to advanced investigative and analytical tools.	In Progress	√
(U) Objective 3.10: Establish a governance model for USMS Cyber Investigations.	In Progress	√

Source: USMS and OIG

(U) APPENDIX 3: USMS Response to the Draft Report

U.S. Department of Justice

United States Marshals Service

Office of Professional Reponsibility

Washington, DC 20530-0001

May 26, 2021

(U)MEMORANDUM TO: Jason R. Malmstrom
Assistant Inspector General for Audit
Office of the Inspector General

(U)FROM: Heather Walker
Assistant Director

(U)SUBJECT: Response to Draft Audit Report: Audit of the United States Marshals Service's Judicial Security Activities

(U) This is in response to correspondence from the Office of the Inspector General (OIG) requesting comment on the recommendations associated with the subject draft audit report. The United States Marshals Service (USMS) appreciates the opportunity to review the Report and concurs with the recommendations therein. Actions planned by the USMS with respect to OIG's recommendations are outlined in the attached response.

(U) Should you have any questions or concerns regarding this response, please contact Krista Eck, External Audit Liaison, at 202-819-4371.

Attachments

cc: (U) David Sheeren
Regional Audit Manager
Office of the Inspector General

(U) Bradley Weinsheimer
Associate Deputy Attorney General
Department of Justice

(U) Matthew Sheehan
Counsel to the Deputy Attorney General
Department of Justice

(U) Louise Duhamel
Acting Assistant Director, Audit Liaison Group
Internal Review and Evaluation Office
Justice Management Division

(U) John Kilgallon
Chief of Staff
United States Marshals Service

(U) United States Marshals Service Response to the Office of Inspector General Draft Report Audit of the United States Marshals Service's Judicial Security Activities

(U) **Recommendation 1: Review OPI's Protective Intelligence Enterprise Reformation Plan and protective intelligence capabilities at other DOJ components such as the FBI and determine and pursue the actions necessary to achieve desired threat identification, assessment, and mitigation capabilities.**

USMS Response (Concur): The Judicial Security Division (JSD) continues to move forward toward the creation of a full-cycle intelligence capability. In March 2021, JSD reorganized the resources of Office of Protective Intelligence (OPI) by restructuring the Investigation and Assessment Branches and creating a Threat Investigations Unit (TIU). The United States Marshals Service (USMS) will initiate a Mission Center concept similar to those at the Department of Homeland Security and the Federal Bureau of Investigation. These organizational adjustments and planned growth of the Protective Intelligence Enterprise will lead to the USMS achieving desired threat identification, assessment, and mitigation capabilities.

(U) **Recommendation 2: Assess the status and training requirements of the DTI position to determine if it meets the needs of the judicial security program and make any necessary adjustments to ensure an adequate number of DTIs are dedicated on a full-time basis to this function, are appropriately trained, and are operational.**

(U) **USMS Response** (Concur): Historically, all threat investigations were conducted by a Protective Intelligence Investigator (PII) or a District Threat Investigator (DTI). Since the implementation of the Full Performance Level-13 (FPL-13), the full-time PII and collateral duty DTI positions were eliminated. Moving forward, all 1811 Criminal Investigators can conduct protective investigations. The TIU will complete three additional JSD Protective Intelligence Training Courses (PITC) in the remainder of fiscal year (FY) 2021. JSD's short term goal is to have a trained Criminal Investigator in protective investigations for each USMS district by the end of FY 2021. TIU's long term goal is to have at least one PITC trained 1811 Criminal Investigator trained to conduct protective investigations in every office.

(U) **Recommendation 3: Update the policies and standard operating procedures guiding its protective intelligence and threat assessment to ensure they align with approved practices.**

(U) **USMS Response** (Concur): Since the implementation of the FPL-13, the investigative policies of the USMS have been undergoing review. USMS Policy Directive 10.4 provides policy for Protective Investigations and will be updated once other USMS policies on investigations have been updated. When the draft USMS Policy Directive 10.4 is approved, OPI will update the USMS Publication 202, *Guide to Protective Investigations & Threat Management,* to align with the policy. USMS Publication 202, dated July 2016, provides the standard operating procedures for OPI. In the first quarter of FY 2022, OPI will also update and republish the Protective Intelligence Enterprise Strategic Plan for FYs 2022 through 2025.

(U) **Recommendation 4: Establish policy guiding its proactive threat identification practices.**

(U) **USMS Response** (Concur): The OPI created the Open-Source Intelligence (OSINT) Unit in 2016. Due to limited resources the USMS was only able to provide reactive threat identification capabilities based on open threat cases. This unit expanded dramatically in 2021 and by 2022, will provide proactive threat identification capabilities for the federal judiciary. Policy guiding the Agency's proactive threat identification practices of the OSINT Unit and the full-cycle intelligence capability will be drafted when the Protective Intelligence Enterprise Strategic Plan is updated.

(U//~~LES~~) **Recommendation 5: Solicit input from judges eligible to participate in the HIDS program to determine what home security features they want made available to them,** [redacted] **and determine the feasibility of incorporating those features into the next HIDS contract requirements.**

(U) **USMS Response** (Concur): In May 2021, JSD released a survey to the district Judicial Security Inspectors (JSIs) requesting the status of judges involved in the program. For those judges not in the program, the survey also asks to provide reasons why. This data will help the Home Intrustion Detection Systems (HIDS) program gauge interest, provide potential improvements, and improve strategic planning. JSD will continue to work with the Administrative Office of United States Courts, throughout the remainder of FY 2021, to gather additional input from judges eligible to participate in the HIDS program to better serve USMS protected persons.

(U) **Recommendation 6: Explore options for upgrading current and future intrusion detection equipment to address present day security threats, as well as the needs of its users.**

(U//~~LES~~) **USMS Response** (Concur): The USMS is currently undergoing a nationwide re-compete for the HIDS contract. The expected performance date of the new HIDS contract will begin this FY. The new contract will incorporate current technology [redacted] The modernized HIDS contract will include newer technologies which are available in the marketplace today.

(U) The HIDS modernization effort, which will require three years to fully implement, is designed to ensure effective monitoring, timely maintenance, and ongoing equipment upgrades. The HIDS program will continue to update intrusion detection systems with new specifications to implement technological advances as the contract is re-competed.

(U) **Recommendation 7: Use its Publication 94 to develop a standard agenda of key topics for required annual security briefings to USMS-protected persons and revise its Judicial Security Policy Directive to require that these topics be briefed annually to each individual under its protection.**

(U) **USMS Response** (Concur): The USMS is currently reviewing USMS Policy Directive 10.1 to make the necessary changes needed; updates to USMS Policy Directive 10.1 will be sent for approval by the end of the FY. The National Center for Judicial Security is in the process of updating training products which can be used for the annual security training and briefings.

(U) **Recommendation 8: Revise its Judicial Security Policy Directive to require districts to use Form USM-50Z to track completion of required annual security briefings to USMS-protected persons and retain those records, by fiscal year, for a period of at least 3 years.**

(U) **USMS Response** (Concur): The updates to USMS Policy Directive 10.1 will include how to document the annual security training and retention period.

(U) APPENDIX 4: Office of the Inspector General Analysis and Summary of Actions Necessary to Close the Report

(U) The OIG provided a draft of this audit report to the USMS. The USMS's response is incorporated as Appendix 3 of this final report. In response to our draft audit report, the USMS concurred with our recommendations and discussed the actions it will implement in response to our findings. As a result, the audit report is resolved. The following provides the OIG analysis of the responses and summary of actions necessary to close the report.

(U) Recommendation for the USMS:

1. **(U) Review OPI's Protective Intelligence Enterprise Reformation Plan and protective intelligence capabilities at other DOJ components such as the FBI and determine and pursue the actions necessary to achieve desired threat identification, assessment, and mitigation capabilities.**

   (U) Resolved. The USMS concurred with our recommendation. The USMS stated in its response that JSD reorganized OPI resources and created a Threat Investigations Unit. Additionally, the USMS stated that it plans to incorporate mission concepts similar to those at the Department of Homeland Security and the FBI into its own protective intelligence capabilities. The USMS noted that it expects these enhancements to help the agency achieve its desired threat identification, assessment, and mitigation capabilities. As a result, this recommendation is resolved.

   (U) This recommendation can be closed when we receive evidence that the USMS has determined and is sufficiently achieving its desired threat identification, assessment, and mitigation capabilities.

2. **(U) Assess the status and training requirements of the DTI position to determine if it meets the needs of the judicial security program and make any necessary adjustments to ensure an adequate number of DTIs are dedicated on a full-time basis to this function, are appropriately trained, and are operational.**

   (U) Resolved. The USMS concurred with our recommendation. The USMS stated in its response that since the implementation of FPL-13, the collateral-duty DTI positions were eliminated. Moving forward, all Criminal Investigators can conduct protective investigations, with the Threat Investigation Unit conducting additional Protective Intelligence Training Courses (PITC) to achieve JSD's short-term goal of having at least one Criminal Investigator in each district complete the PITC by the end of FY 2021. The USMS eventually plans to have a PITC-trained Criminal Investigator in every USMS office. As a result, this recommendation is resolved.

   (U) This recommendation can be closed when we receive evidence that at least one Criminal Investigator in each USMS district has completed PITC training, and a documented plan and schedule for having a PITC-trained Criminal Investigator in every USMS office.

3. **(U) Update the policies and standard operating procedures guiding its protective intelligence and threat assessment to ensure they align with approved practices.**

   (U) Resolved. The USMS concurred with our recommendation. The USMS stated in its response that its investigative policies have been undergoing review since the implementation of FPL-13. USMS further stated that once these policies have been updated, the USMS plans to update its

Protective Investigations policy (USMS Policy Directive 10.4) and its Guide to Protective Investigations and Threat Management (USMS Publication 202). The USMS stated that it also plans to update its Protective Intelligence Enterprise Strategic Plan for FYs 2022-2025, which it anticipates will be published in the first quarter of FY 2022. As a result, this recommendation is resolved.

(U) This recommendation can be closed when the USMS demonstrates that its updated USMS Policy Directive 10.4, USMS Publication 202, and the Protective Intelligence Enterprise Strategic Plan for FYs 2022-2025, align with approved practices for protective intelligence and threat assessments.

4. **(U) Establish policy guiding its proactive threat identification practices.**

(U) Resolved. The USMS concurred with our recommendation. The USMS stated in its response that its Open Source Intelligence Unit has dramatically expanded its threat identification capabilities in recent years and intends to draft policy guiding the agency's proactive threat identification practices when the Protective Intelligence Enterprise Strategic Plan is updated. As a result, this recommendation is resolved.

(U) This recommendation can be closed when we receive the approved policy for the USMS's proactive threat identification practices.

5. **(U//~~LES~~) Solicit input from judges eligible to participate in the HIDS program to determine what home security features they want made available to them [redacted] and determine the feasibility of incorporating those features into the next HIDS contract requirements.**

(U) Resolved. The USMS concurred with our recommendation. The USMS stated in its response that JSD released a survey in May 2021 to its district Judicial Security Inspectors requesting the status of judges involved in the HIDS program, including an explanation of why judges have opted not to participate in the program. The USMS believes that this data will help the HIDS program gauge interest, provide potential improvements, and improve strategic planning. The USMS also stated that JSD will continue to work with the Administrative Office of the United States Courts throughout the remainder of FY 2021 to gather additional input from judges eligible to participate in the HIDS program. As a result, this recommendation is resolved.

(U) This recommendation can be closed when we receive evidence that the USMS has obtained input from judges eligible to participate in the HIDS program on what security features they want made available to them and used that input to determine the feasibility of incorporating those features into the next HIDS contract, as well as improve strategic planning for the HIDS program.

6. **(U) Explore options for upgrading current and future intrusion detection equipment to address present day security threats, as well as the needs of its users.**

(U//~~LES~~) Resolved. The USMS concurred with our recommendation. The USMS stated in its response that it is currently re-competing its HIDS contract, which is expected to begin in FY 2021. The new contract will incorporate newer technologies, which are available in the marketplace today, [redacted]. As a result, this recommendation is resolved.

(U) This recommendation can be closed when we receive evidence that the new HIDS contract

provides newer technologies and equipment to address present day security threats and the needs of its users.

7. **(U) Use its Publication 94 to develop a standard agenda of key topics for required annual security briefings to USMS-protected persons and revise its Judicial Security Policy Directive to require that these topics be briefed annually to each individual under its protection.**

   (U) Resolved. The USMS concurred with our recommendation. The USMS stated in its response that it is currently reviewing its Judicial Security policy (USMS Policy Directive 10.1) and plans to submit necessary revisions for approval by the end of FY 2021. Additionally, the NCJS is updating training products, which can be used for annual security trainings and briefings. As a result, this recommendation is resolved.

   (U) This recommendation can be closed when we receive evidence that the updated NCJS training products incorporate information from Publication 94 and the updated and approved USMS Policy Directive 10.1 requiring that, on an annual basis, USMS-protected persons are briefed on the NCJS training products.

8. **(U) Revise its Judicial Security Policy Directive to require districts to use Form USM-50Z to track completion of required annual security briefings to USMS-protected persons and retain those records, by fiscal year, for a period of at least 3 years.**

   (U) Resolved. The USMS concurred with our recommendation. The USMS stated in its response that the updated USMS Policy Directive 10.1 will include requirements for how annual security training should be documented and establish a retention period for training documentation. As a result, this recommendation is resolved.

   (U) This recommendation can be closed when we receive the updated and approved USMS Policy Directive 10.1 appropriately establishing requirements for documentation and retention of annual security briefings to USMS-protected persons.