



Audit of the United States Marshals Service's Home Intrusion Detection System Program



AUDIT DIVISION

24-099

SEPTEMBER 2024

REDACTED FOR PUBLIC RELEASE

The full version of this report contains information that the U.S. Marshals Service considered to be law enforcement sensitive and therefore could not be publicly released. To create the public version of the report, the Office of the Inspector General redacted (blacked out) portions of the full report.



EXECUTIVE SUMMARY

Audit of the United States Marshals Service's Home Intrusion Detection System Program

(U) Objective

(U) Our audit objective was to assess the United States Marshals Service's (USMS) programs and practices concerning the protection of federal judges at their places of residence, with a focus on the Home Intrusion Detection System (HIDS) program. Our audit scope generally covered the USMS's residential judicial security activities from August 2021 through December 2023.

(U) Results in Brief

(U) The safety of the federal judiciary is fundamental to the proper functioning of the justice system. Often, and sometimes tragically, threats to that safety extend beyond the courthouse walls. In 2005, the USMS established the HIDS program to provide home security systems to federal judges. In a 2021 audit, we found that only 60 percent of federal judges participated in the HIDS program. In 2022, the USMS restructured its HIDS program, from a USMS-procured vendor program to a reimbursement-based program with the goal of increasing participation.

(U) In this audit, we found that the USMS has seen a 13 percent increase in HIDS enrollment under the new program. However, about 28 percent of federal judges still do not participate, including over 200 judges who had participated in the prior HIDS program but do not participate now. We also found that, contrary to our prior recommendation, the USMS did not survey federal judges prior to restructuring the program in 2022. However, the USMS recently completed a satisfaction survey of judges in April 2024. We believe seeking this input and taking other steps—such as identifying judges' unique home security needs, identifying and removing impediments to judges' HIDS participation, and providing more training to USMS personnel—could help improve the HIDS program.

(U) Recommendations

(U) Our report contains nine recommendations to assist the USMS in its efforts to protect federal judges at their places of residence.

(U) Audit Results

(U) The USMS's Judicial Security Division (JSD), which manages the HIDS program, assesses concerning communications to and explicit threats made against judges and other protected persons to determine the level of danger and the appropriate response. We found that since our 2021 audit, JSD has undertaken efforts to improve performance in this area, including providing resources to the judiciary to reduce the distribution and accessibility of their personal information and updating JSD's Counter-Surveillance/Surveillance Detection (CS/SD) Unit to keep pace with an evolving threat landscape. Our audit identified further enhancements to the USMS residential judicial security programs and practices that will help the USMS ensure the continued safety of protected persons and improve the efficiency, effectiveness, and accountability of the HIDS program.

(U) The USMS Should Obtain Input from Judges to Increase HIDS Enrollment and Maximize the Security of Participants

(U) After restructuring the HIDS program in 2022 to make it more appealing to judges, by January 2024 total enrollments had increased by 13 percent. However, 729 judges still were not enrolled in the program, including 223 judges who had enrolled in the prior HIDS program. We found in this audit that, contrary to an Office of the Inspector General (OIG) recommendation in 2021, the USMS had not solicited input directly from judges when considering how to restructure the HIDS program. We also found, similar to a finding from our 2021 Judicial Security Activities report, that the USMS was unaware of the reasons why judges were not participating in the HIDS program, and only recently attempted to obtain that data.

(U) Under the HIDS program, judges are reimbursed up to \$2,500 every 3 years to cover the costs of installing a home security system and up to \$800 per year for alarm monitoring services. To receive reimbursement, judges

must first register as a vendor with the USMS and then submit a completed reimbursement request form and required supporting documentation. We reviewed 297 reimbursement requests and found that in its approval of approximately 29 percent of them, the USMS did not adhere to HIDS policy with regard to supporting documentation. However, we also concluded that these reimbursement payments were generally supported based on the documentation the USMS received. We therefore believe the USMS should consider judges' input on the reimbursement process and then streamline that process to ensure that unnecessary requirements do not dissuade judges from participating in the program.

(U//LES) In addition, third-party alarm monitoring services are not a requirement of the restructured HIDS program. The USMS recommends and reimburses judges for monitoring services; however, judges have the option of declining this service. We found that the USMS is generally unaware that judges have included monitoring services as part of their HIDS configuration until they submit a request to be reimbursed for it. Additionally, judges who acquire monitoring services are encouraged, but not required, to [REDACTED]

[REDACTED] creates a risk that, when an alarm sounds, there will not be an appropriate law enforcement response when no one is at a residence to call the police or when residents are home but unable to call for assistance. As such, it is critical that the USMS continue to encourage judges to take advantage of its monitoring reimbursement services and [REDACTED]

[REDACTED]—and ensure no barriers exist that prevent or dissuade judges from opting into this important feature of the HIDS program—[REDACTED]

(U) The USMS Should Strengthen HIDS Policies and Procedures to Improve Program Execution

(U) Residential security surveys, conducted by USMS personnel, include an on-site visit to the judge's home to identify security vulnerabilities that could be exploited by an intruder. These surveys were required under the prior HIDS program whenever a judge enrolled but are now optional under the reimbursement program, and they are only conducted if requested by a participating judge. In

our judgment, because residential security surveys educate and assist judges as they plan and acquire their home security systems, rather than requiring a judge to request the survey, the USMS should routinely conduct them when a judge enrolls in the HIDS program, unless the participating judge specifically declines the survey.

(U) We also found that while the HIDS program guidance provides responsible USMS personnel with sufficient information to perform their duties, the HIDS Program Guide does not identify the authorities, necessary qualifications, responsibilities, and required formal training of all individuals responsible for implementing and overseeing the program. These omissions and insufficient training of HIDS personnel could lead to miscommunications, avoidable errors, and delays in HIDS enrollments and reimbursement payments. Implementing more specific guidance could help to ensure HIDS staff are fully equipped and prepared to facilitate all aspects of the program.

(U) Other USMS Actions to Protect Federal Judges Away from the Courthouse

(U) If the USMS determines that a threat to a protected person warrants a more active mitigation response, it deploys personnel to serve on a protective detail as a collateral duty to their usual responsibilities. Within the past year, the USMS's Office of Protective Operations and CS/SD Unit have taken steps to improve the structure, organization, and operation of the protective detail program. We believe these actions should enhance the USMS's ability to mitigate threats to the judiciary and keep pace with the evolving threat landscape.

(U) Additionally, the widespread public availability of a judge's personally identifiable information (PII), such as their home address, presents risks to their safety, as recognized by Congress when it passed the Daniel Aderl Judicial Security and Privacy Act of 2022 to bolster safeguards over federal judges' PII. These risks make it critical that the USMS take steps to help judges protect this sensitive information, and we found that the USMS Judicial Security Inspectors make adequate efforts to educate and inform the judiciary about how to protect their PII.

(U) Table of Contents

| | |
|---|----|
| (U) Introduction..... | 1 |
| (U) Threats Against USMS-Protected Persons..... | 1 |
| (U) Threat Assessments and Protective Investigations..... | 1 |
| (U) Judicial Security Division | 1 |
| (U) Home Intrusion Detection System Program | 2 |
| (U) HIDS Reimbursement Power App..... | 3 |
| (U) OIG Audit Approach..... | 4 |
| (U) Audit Results..... | 5 |
| (U) More Thorough Analyses and Planning Would Have Better Informed USMS Efforts to Restructure the HIDS Program..... | 5 |
| (U) The USMS Should Obtain Input from Judges to Increase HIDS Enrollment and Maximize the Security of Participants | 7 |
| (U) Streamlining the Submission, Review, and Approval of HIDS Reimbursement Requests Could Improve Program Enrollment and Customer Satisfaction | 8 |
| (U) Residential Security Systems With Alarm Monitoring Services Provide an Additional Layer of Security for Enrolled Judges..... | 9 |
| (U) The USMS Should Strengthen HIDS Policies and Procedures to Improve Program Execution | 10 |
| (U) Residential Security Surveys Could Improve HIDS Program Effectiveness and Timeliness | 10 |
| (U) Authorities, Qualifications, and Responsibilities of HIDS Personnel Should Be Better Defined..... | 11 |
| (U) Required HIDS Training Could More Effectively Equip JSD Personnel..... | 11 |
| (U) The USMS Should Document its Approval of Reimbursement Exceptions | 12 |
| (U) The USMS Could Improve its HIDS Reimbursement Appeal Decision Process..... | 12 |
| (U) Other USMS Actions to Protect Federal Judges Away from the Courthouse..... | 14 |
| (U) The USMS is Taking Proactive Steps to Improve Its Protective Detail Capabilities | 14 |
| (U) USMS Makes Adequate Efforts to Educate and Inform Judges About Protecting Their Personally Identifiable Information | 14 |
| (U) Conclusion and Recommendations..... | 16 |
| (U) APPENDIX 1: Objective, Scope, and Methodology | 18 |
| (U) Objective | 18 |
| (U) Scope and Methodology | 18 |
| (U) Statement on Compliance with Generally Accepted Government Auditing Standards | 18 |
| (U) Internal Controls | 18 |
| (U) Sample-Based Testing | 19 |

| | |
|--|----|
| (U) Computer-Processed Data..... | 19 |
| (U) APPENDIX 2: Optional and Ineligible HIDS Equipment..... | 20 |
| (U) APPENDIX 3: The USMS's Response to the Draft Audit Report..... | 21 |
| (U) APPENDIX 4: Office of the Inspector General Analysis and Summary of Actions Necessary to Close the Audit Report..... | 26 |

(U) Introduction

(U) The United States Marshals Service (USMS) has been responsible for protecting the federal judicial process as the enforcement arm of the federal courts since 1789. The USMS protects each of the 94 judicial districts and 13 federal appellate courts by ensuring the safe and secure conduct of judicial proceedings, and by protecting federal judges, jurors, U.S. Attorneys, and other members of the federal judiciary while performing their duties.¹ In Fiscal Year (FY) 2022, the USMS was responsible for protecting approximately 2,700 federal judges. According to USMS data, the safety of federal judges has historically been at greater risk when they are away from the courthouse, and there have been seven attacks on federal judges in their homes since 1979. According to the USMS, protecting court officials is a responsibility that it strives to accomplish by anticipating and deterring threats to the judiciary, and by continuously developing and employing innovative protective tactics.

(U) Threats Against USMS-Protected Persons

(U) The USMS assesses explicit threats and concerning communications against the judiciary to determine the level of danger and the appropriate response. In USMS annual reporting, the USMS states that it has opened over 1,000 investigations into threats and potential threats to protected persons in each of the last 4 fiscal years—FY 2020 to FY 2023. According to the USMS, today's threat landscape, which largely has moved to online and social media platforms, is more complex than ever before, with particularly high-threat environments resulting from terrorism and organized crime. To combat this, USMS judicial security personnel provide protection in all phases of court proceedings, at judicial conferences, and on an ad hoc basis in response to specific threat situations. The USMS relies primarily on the Home Intrusion Detection System (HIDS) program, described below, to provide security at judges' places of residence when more direct USMS protection is not warranted.

(U) Threat Assessments and Protective Investigations

(U) Immediately upon receipt, the USMS assesses all threats, concerning communications, incidents, or suspicious activity to determine the credibility and seriousness of the threat. If the USMS has reasonable indication that a crime has occurred, will occur, or may occur, a protective investigation is opened. The purpose of the protective investigation is to mitigate the threat by determining the subject's true intent, motive, and ability to harm or pose a threat to the protected person. Protective investigations are assigned a level of risk based on the likelihood of injury or death to the protected person. The USMS uses the information gathered by the investigator to develop a threat mitigation plan with the goal of implementing protective measures to reduce the risk to the protected person. These measures may include, but are not limited to, personal security awareness briefings and residential security surveys, which may lead to recommending the installation of alarm systems, enhanced patrols, and protective details.

(U) Judicial Security Division

(U) The USMS Judicial Security Division (JSD) is chiefly responsible for accomplishing the agency's protective mandate by anticipating and deterring threats to the judiciary and employing appropriate protective tactics

¹ (U) USMS protection may also be extended to the immediate family members of protected persons. The Supreme Court of the United States Police Department (SCPD) is responsible for the security of Supreme Court justices. However, upon request of the SCPD the USMS may assist in providing protection to the justices.

in response to those threats. JSD also reimburses more than 1,600 judges to install and monitor security systems in their personal residences. JSD is comprised of 11 program offices with areas of responsibility that include threat management, protective intelligence and operations, the HIDS program, court security, and financial management.

(U) Home Intrusion Detection System Program

(U) The USMS established the HIDS program in December 2005 following the fatal attack by a litigant at the home of a U.S. District Court Judge in Chicago, after which Congress charged the USMS with providing home security systems to increase federal judges' security when they are away from the secure courthouse environment. From 2006 to 2021, the USMS relied on one vendor to provide equipment installation and alarm monitoring services to participating judges. In June 2021, the OIG released a report on its audit of the USMS's judicial security activities, which found that the equipment and services offered by the HIDS program did not include certain important protections commonly available from other home security systems, such as surveillance cameras.² The audit also found that only 60 percent of eligible judges were participating in the program.

(U) As a result of the OIG's audit and other concerns expressed by the Administrative Office of the U.S. Courts (AOUSC), in February 2022 the USMS restructured the HIDS program from a USMS-procured vendor program to a reimbursement-based program. The USMS believed that a reimbursable program would give judges the opportunity to obtain a modern security system that meets USMS protection standards, while also providing judges with the flexibility to tailor the system to their individual security needs and select any alarm-monitoring provider that meets certification requirements.

(U) The current HIDS program reimburses enrolled judges for home security equipment and installation costs up to \$2,500 every 3 years. Judges may also be reimbursed an additional \$800 per year for alarm monitoring costs and other covered services. To qualify for reimbursement, participating judges must have the required equipment described in Table 1 installed at their residence.³ Additional system components or services that exceed the established reimbursement limits may be procured at the judge's own expense. Judges also have the option of appealing for an exception if they believe it necessary to install equipment that exceeds the \$2,500 reimbursement limit. See Appendix 2 for a list of optional equipment eligible for reimbursement under the HIDS program, as well as a list of equipment that is ineligible for reimbursement.

² (U) DOJ OIG, *Audit of the United States Marshals Service Judicial Security Activities*, Audit Report 21-083 (June 2021), <https://oig.justice.gov/reports/audit-us-marshals-service-judicial-security-activities>.

³ (U) The HIDS Program Office may approve exceptions to the minimum equipment requirements if a specific circumstance warrants a deviation.

(U) Table 1

(U) Required and Recommended HIDS Equipment that Qualifies for Reimbursement

| (U) Required Equipment | | (U) Description | |
|---------------------------|------------|-----------------|-------------------------|
| (U//LES) | [REDACTED] | (U//LES) | [REDACTED] |
| (U//LES) | [REDACTED] | (U//LES) | [REDACTED] |
| (U//LES) | [REDACTED] | (U//LES) | [REDACTED] |
| (U) Recommended Equipment | | (U) Description | |
| (U//LES) | [REDACTED] | (U//LES) | [REDACTED] |
| (U//LES) | [REDACTED] | (U//LES) | [REDACTED] |
| (U//LES) | [REDACTED] | (U//LES) | [REDACTED] |
| (U//LES) | [REDACTED] | (U//LES) | [REDACTED] ⁴ |

(U) Source: USMS

(U) HIDS Reimbursement Power App

(U) As part of the HIDS restructuring effort, the USMS developed a web-based platform, known as the HIDS Reimbursement Power App (HIDS App), as a way of streamlining and automating HIDS program data collection. The HIDS Program Office uses the HIDS App to enroll judges in the program, and to review, approve, and document HIDS reimbursement requests. Data input into the HIDS App is also used to generate an interactive dashboard with a visual depiction of program progress and financial transaction data. For enrollment verification and tracking purposes, the USMS creates a profile in the HIDS App for all judges eligible to participate in the program, regardless of whether they choose to enroll. At present, the HIDS App is used only by USMS employees and is not used by participants to submit reimbursement requests or for other purposes.

⁴ (U//LES) Subsequent to our analyses, the USMS updated the HIDS Program Guide in April 2024 [REDACTED] if the system included all required equipment and the total installation cost did not exceed the \$2,500 reimbursement limit.

(U) OIG Audit Approach

(U) The objective of our audit was to assess the USMS's programs and practices concerning the protection of federal judges at their places of residence, with a focus on the HIDS program. The scope of our audit generally covered the USMS's residential judicial security activities from August 2021 through December 2023. To accomplish our objective, we reviewed policies and procedures guiding the restructured HIDS program, compliance with policies and procedures, and the USMS's approach to providing protective details and conducting counter-surveillance operations.

(U) We interviewed officials from JSD to gain an understanding of the USMS's planning, analysis, and research efforts that contributed to the decision to restructure the HIDS program. We spoke with officials from JSD's Office of Protective Operations and the HIDS Program Office regarding their understanding and implementation of USMS guidance pertinent to their areas of responsibility. Additionally, we distributed a questionnaire to Judicial Security Inspectors (JSI) in 25 of 94 judicial districts throughout the country to obtain their perspective on the HIDS program. We also examined a sample of HIDS reimbursement requests for system installation and monthly monitoring services and several appeals submitted by judges requesting reimbursement amounts over the approved program limits. Finally, we examined the USMS's efforts to educate and inform judges on ways to limit the accessibility and distribution of or otherwise safeguard their personal information. Appendix 1 contains further details on our audit objective, scope, and methodology.

(U) Audit Results

(U) The USMS primarily utilizes two distinct methods for protecting federal judges when they are outside of the courthouse. Protective details are used, as needed, to protect judges against explicit threats to their safety, while the HIDS program is designed to secure judges' residences when more direct USMS protective services are not necessary. Our audit focused on and identified opportunities for the USMS to improve upon the HIDS program. Since restructuring the HIDS program in 2022, we found that the USMS has experienced an increase in total HIDS program enrollments of approximately 13 percent over the prior program. However, the USMS largely does not have insight into the reasons why the remaining 28 percent of judges have elected not to enroll, or why 223 judges who had enrolled in the prior program have elected not to enroll in the restructured program. We also found that the USMS did not survey judges prior to its decision to restructure the HIDS program, and that the new program no longer requires on-site security surveys of a judge's residence by the USMS to identify vulnerabilities. Further, we identified other areas of the restructured HIDS program that could be strengthened to improve the USMS's programs and practices concerning protection of federal judges at their places of residence and ensure the accuracy and timeliness of reimbursement payments to judges. Finally, we found that the USMS is undertaking steps to improve its protective detail operations in response to the increased threat environment, and that its efforts to educate and inform judges on ways to protect their personally identifiable information (PII) are adequate.

(U) More Thorough Analyses and Planning Would Have Better Informed USMS Efforts to Restructure the HIDS Program

(U) After the issuance of the OIG's 2021 report on its audit of USMS Judicial Security Activities, the USMS conducted a Business Process Analysis of the HIDS program to evaluate alternative methods of purchasing and managing home security systems for the federal judiciary that provide the best balance of accessibility, cost, and quality of service while also adhering to USMS security standards. The aim of the Business Process Analysis was to: (1) ensure the USMS is maximizing the likelihood that judges will enroll in the HIDS program and regularly arm their systems; and (2) provide an updated framework for HIDS system compliance and program oversight ensuring that systems provided or acquired through the HIDS program meet the USMS's minimum security standards. The Business Process Analysis focused primarily on the contracts, agreements, and standards underlying the installation, maintenance, and monitoring of security systems at a participating judge's primary residence, and assessed the following:

1. (U) The methods through which the USMS acquires judges' home alarm systems.
2. (U) The level of direct involvement the USMS and the HIDS program have in the selection, installation, maintenance, and operational management and monitoring of home alarm systems.
3. (U) Contractual and technical requirements for security systems provided.
4. (U) The level of flexibility that judges have in selecting private or customizable security systems and how this flexibility impacts the program's ability to fulfill the USMS's protective mandate.
5. (U) HIDS Program Office capabilities and stakeholder concerns related to all approaches being considered, and any implied changes in responsibility among stakeholders.

(U) As part of the Business Process Analysis, the USMS also considered the limitations of the prior HIDS program—a single nationwide contract with one vendor—and it met with the United States Capitol Police and the United States Secret Service to determine how those agencies operate their home intrusion detection programs. Additionally, in August 2021, the USMS issued a Request for Information to industry providers to obtain relevant information about the home security marketplace and industry capability, and to identify interest and availability of respondents to provide HIDS services.

(U) Ultimately, the Business Process Analysis resulted in the identification of seven options for how the USMS could operate the HIDS program. The USMS then used six criteria – vendor options, serviceability, product flexibility, level of USMS oversight, resource burden, and feasibility – to score individual elements of each option and assign an overall rank. The evaluated program approaches and their associated rank are shown in Table 2. After review of the Business Process Analysis, the AOUSC communicated to the USMS its preference for a reimbursement-based HIDS program, which the USMS ranked in the Business Process Analysis as its second and fourth most favorable options. After several months of discussions, the USMS and AOUSC jointly determined that the USMS reimbursement option was the approach most agreeable to both parties.

(U) Table 2

(U) HIDS Program Approach Alternatives and USMS Favorability Ranking

| Approach | Description | Overall Rank |
|----------------------------|---|--------------|
| Multiple Contracts | Vendors bid on each HIDS installation project. HIDS Program Office evaluates proposals and selects awardee. | 1 |
| AOUSC Reimbursement | AOUSC reimburses judges for installation and monitoring costs. | 2 |
| USMS District Administered | Each judicial district manages and pays for HIDS directly. | 3 |
| USMS Reimbursement | The USMS administers reimbursement payments to judges, who are treated as vendors. | 4 |
| AOUSC Allowance | Each judge is given a predetermined amount to devote to security services, as a part of their job. | 5 |
| Circuit Contracts | Contracts with up to 12 HIDS providers administered separately by each of the 12 Circuit Courts. | 6 |
| Nationwide Contract | Maintain the status quo through a single contract with one nationwide HIDS provider. | 7 |

Source: USMS

(U) The USMS stated in its Business Process Analysis that it was working with the judiciary to distribute a survey to all judges to gain additional insight into their experience with the HIDS program. The Business Process Analysis also stated that the results of this survey, along with decisions from USMS and AOUSC leadership, would determine the next steps for the program. However, we found that the USMS ultimately did not survey judges prior to deciding which Business Process Analysis option it should pursue. According

to a JSD official involved in the HIDS restructuring effort, the USMS ran out of time to survey judges as the end of the prior HIDS contract period of performance approached. Instead, JSD and AOUSC worked together to define how the new HIDS program would operate under the USMS reimbursement model. Without the input of judges or the consideration of their individual security needs, desires, and concerns related to the HIDS program, the decision to pursue a reimbursement-based program may have been inadequately informed. The next section of this report discusses the ongoing need for the USMS to obtain input from judges eligible to participate in the HIDS program.

(U) The USMS Should Obtain Input from Judges to Increase HIDS Enrollment and Maximize the Security of Participants

(U) The USMS could do more to enable and encourage judges to enroll in the HIDS program. Currently, the USMS relies primarily on informational handouts and communications from USMS employees in each judicial district to encourage judges to enroll. At the end of December 2023, 1,833 judges – about 72 percent of all eligible judges – were enrolled in the HIDS program. In calendar year 2023, HIDS program enrollments fluctuated and averaged about four new enrollments each week. And, despite efforts to restructure the HIDS program and make it more appealing to judges, total enrollments have increased by only 212 judges (about 13 percent) over enrollment totals from the prior HIDS program, while 223 judges who were enrolled in the prior HIDS program have not yet enrolled in the new program.

(U) The HIDS Program Office uses the HIDS App to track enrollment and reimbursement data for all judges eligible to participate in the program, as well as information received concerning individual judges' enrollment and installation limitations. The HIDS App also includes the capability to formally track data on non-participating judges and the reasons why they have opted out or otherwise not enrolled in the program, but we found that the USMS does not utilize this feature. Instead, the HIDS Program Office obtains this data anecdotally from USMS personnel in judicial district offices. We had a similar finding in our June 2021 audit report, which found that the USMS was only able to speculate why judges were not participating in the program.

(U) The USMS stated in its Business Process Analysis effort that it would survey judges eligible to participate in the program, but ultimately that did not occur until nearly 3 years after the program was restructured. During our audit, the USMS informed us that it had developed and distributed a customer satisfaction survey to obtain input from the judiciary. The USMS, in consultation with the AOUSC, focused the survey on how judges were made aware of the HIDS program, the reasons why judges have or have not enrolled in the program, opinions on the current enrollment and reimbursement processes, preferences in any security systems and services judges have obtained, and specific ways the USMS can improve HIDS customer satisfaction.⁵

(U) In our judgment, input from the judiciary is necessary if the USMS is to maximize HIDS program enrollment and satisfaction, and the USMS should use the judges' input to identify areas of the program that are barriers to enrollment or impediments to the regular use of their HIDS system. Therefore, we

⁵ (U) With 2 weeks remaining until the April 30, 2024, survey deadline, nearly 1,200 judges—over 45 percent of eligible participants—had responded to the satisfaction survey. Based on our summary review of the survey questions and available responses, we believe this feedback will assist USMS in pursuing meaningful improvements to the HIDS program.

recommend that the USMS establish requirements for regularly soliciting input from judges eligible to participate in the HIDS program, evaluating the judges' input, and assessing the feasibility of implementing changes that will increase HIDS program enrollment and help ensure current participants remain enrolled in the program.

(U) Streamlining the Submission, Review, and Approval of HIDS Reimbursement Requests Could Improve Program Enrollment and Customer Satisfaction

(U) After paying for HIDS equipment, installation, and alarm monitoring services, judges must register as a vendor with the USMS and then complete a reimbursement request form and provide receipts, invoices, and proof of payment to the HIDS Program Office by emailing the documents to the HIDS mailbox for processing. Judges must also submit proof of payment that shows the amount paid, date of payment, and the vendor's name. The HIDS Program Office then reviews, approves, and routes reimbursement request forms and accompanying support to the USMS's Office of Financial Management for secondary review and final payment processing. Upon approval, all HIDS reimbursement requests must first be signed by an approving official from the HIDS Program Office, and later by a funds certifier in the Office of Financial Management.

(U) From 328 HIDS reimbursement requests approved by the HIDS Program Office between February 2023 and March 2023, we examined a judgmental sample of 297 requests—76 for installation and 221 for monitoring services. We found that the USMS approved 63 (29 percent) of the 221 monitoring requests using supporting documentation provided by the judge under a prior reimbursement request. Specifically, the USMS often was able to use the judges' monitoring contract or an order summary, provided to the USMS when the judges' system was installed, to justify future monthly monitoring payments, even though this practice technically conflicted with the HIDS Program Guide, which requires that each reimbursement request be accompanied by supporting documentation.

(U//~~LES~~) We also found that, in 11 of the 76 installation requests we examined (14 percent), the USMS approved reimbursement for the installation of equipment in excess of the HIDS program's formal limitation of [REDACTED], and that the HIDS Program Office often made such reimbursements without a clear and explicit justification. After we concluded our analyses, the USMS updated the HIDS Program Guide in April 2024 to allow for more than [REDACTED] if the system included all required equipment and the total installation cost did not exceed the \$2,500 reimbursement limit.

(U) In both of these instances—approvals made without technically required documentation, and reimbursements for equipment in excess of the program's formal limitation—the USMS was able to approve appropriate requests from participating judges despite the requests not meeting the technical requirements of the program. As we found no evidence that the requests were inappropriate or unjustified and found no evidence of material overpayment, we concluded that the HIDS Program Guide may contain requirements and limitations that are not reflective of the USMS's actual approval practices, and that this condition could lead to judges spending time gathering unnecessary documentation, judges not installing necessary security equipment, or payment delays. Consequently, we found that the reimbursement submission, review, and approval processes pose challenges to both USMS officials and participating judges and should be improved to ensure that process inefficiencies do not dissuade judges from participating in the program. Therefore, we recommend that the USMS assess the HIDS reimbursement processes and consider feedback received from judges to identify opportunities to streamline the process.

(U) Residential Security Systems with Alarm Monitoring Services Provide an Additional Layer of Security for Enrolled Judges

(U//LES) Under the restructured HIDS program, participants have the option of receiving reimbursement for system monitoring services, which are provided by third parties that remain on alert for alarm activations. When an alarm activation occurs, monitoring service providers take a series of predesignated actions based on the type of alert. Typically, when the system detects an alarm activation, it notifies the monitoring center, which attempts to contact the homeowner first and then will conduct an emergency response if the center is unable to reach the homeowner. If a judge opts not to obtain monitoring services, or the HIDS system they choose [REDACTED]

[REDACTED] This limitation inhibits USMS's ability to effectively achieve the HIDS program's goal to monitor, track, and mitigate residential security issues, and creates the unnecessary risk that, when an alarm sounds, notification to appropriate law enforcement personnel may be delayed or go unreported.

(U) For these reasons, the HIDS Program Guide states that alarm monitoring services provide for greater reliability and a more uniform response to alarm activations, and the USMS recommends to judges that they procure monitoring services if they are willing. According to a USMS official, most enrolled judges have obtained monitoring services. However, the HIDS Program Office only tracks this information through reimbursement requests and does not readily know which judges have included monitoring services as part of their HIDS configuration.

(U//LES) Additionally, when a judge opts to obtain a monitoring service, the USMS also recommends—but again does not require—that judges [REDACTED]

[REDACTED] This ensures that [REDACTED] Due to the voluntary nature of this process, however, judges may decline [REDACTED]

(U//LES) The absence of third-party monitoring creates a risk that, when an alarm sounds, there will not be an appropriate law enforcement response when no one is at a residence to call the police or when residents are home but unable to call for assistance. As such, while this decision ultimately rests with each judge, we believe it is critical that the USMS continue to encourage judges to take advantage of its monitoring reimbursement services and [REDACTED]

[REDACTED] We also believe the USMS should be more aware of which enrolled judges have not obtained monitoring services and take steps to ensure no barriers exist that prevent or dissuade judges from opting into this important feature of the HIDS program. Therefore, we recommend that the USMS track alarm monitoring participation rates, consider feedback from judges about why they choose not to obtain monitoring services, and make any necessary changes to the HIDS program to maximize the number of judges electing to include alarm monitoring in their HIDS configuration.

(U) The USMS Should Strengthen HIDS Policies and Procedures to Improve Program Execution

(U) JSD has developed a comprehensive HIDS Program Guide that contains a detailed overview of the program and establishes operating procedures and security parameters. JSD has also produced a handbook for JSIs designed to equip them with information they need to assist judges in their judicial district with all aspects of the HIDS program. While we found that the HIDS Program Guide and JSI Handbook provide responsible personnel with sufficient information to enable them to implement the HIDS program effectively, we also identified several areas where both the HIDS program and the overarching policies that guide it could be improved to further mitigate risk and strengthen program execution.

(U) Residential Security Surveys Could Improve HIDS Program Effectiveness and Timeliness

(U) The HIDS Program Guide identifies the importance of residential security surveys, along with HIDS coverage, to help minimize risk to the safety of federal judges. A residential security survey is conducted by the judicial district JSI and involves an on-site visit to the judge's home to identify security vulnerabilities that could be exploited by an intruder. This important step in the judicial security process has the potential to not only inform the judge but enable them to address those vulnerabilities through adequate HIDS coverage. Under the previous HIDS program, JSIs were required to conduct security surveys when a judge enrolled in the HIDS program.⁶ Additionally, the USMS had previously established policy for conducting, documenting, and approving residential security surveys.

(U) However, we found that the current HIDS program no longer requires JSIs to conduct security surveys. Instead, these surveys are only conducted at the request of a participating judge. Additionally, when a security survey is conducted, the HIDS Program Guide does not provide guidance on how to perform or document the survey. According to the USMS, these requirements were not incorporated into the restructured reimbursement HIDS Program Guide because, in moving to a reimbursement model, the USMS sought to give judges more responsibility and flexibility in selecting the configuration of their HIDS system, including deciding what level of USMS involvement they preferred in the system design process.

(U) In our judgment, consistent completion of residential security surveys, when acceptable to the participating judge, would aid both the HIDS Program Office and program participants in several ways: it would help ensure judges are aware of the security vulnerabilities unique to their residence; it would provide a useful and informative tool that judges can use to plan for and acquire a HIDS system that meets minimum program requirements; and it would streamline and improve the timeliness of HIDS reimbursement and appeal processes by providing assurance to approving authorities that the reimbursement request is for a system that meets a judge's legitimate security needs.

(U) Residential security surveys are a protective measure that should be a critical first step whenever a judge enrolls in the HIDS program and is willing to accept such a survey. Therefore, we recommend the USMS require district JSIs to conduct residential security surveys of the home of all HIDS participants upon their enrollment in the program, unless the participant specifically declines. We also recommend that the

⁶ (U) Residential security surveys were referred to as Pre-Installation Plan surveys under the prior HIDS program.

USMS update the HIDS Program Guide with established procedures on how to properly conduct, document, and use residential security surveys to inform pertinent processes within the HIDS program.

(U) Authorities, Qualifications, and Responsibilities of HIDS Personnel Should Be Better Defined

(U) Identifying, defining, assigning, and documenting the responsibilities of key roles within an organization are critical components of effective internal control and help ensure the organization meets its objectives. While the HIDS Program Guide has established and defined the role of the JSI in assisting judges with HIDS program matters, it does not identify the authorities, necessary qualifications, and responsibilities of the USMS officials responsible for implementing and overseeing the program. Specifically, we found that the HIDS Program Guide does not adequately define the role of: (1) Physical Security Specialists (PSS), (2) HIDS Help Desk operators who help guide judges in their search for a security system, (3) HIDS vendor installation estimate reviewers, and (4) HIDS reimbursement request approval officials. As the daily responsibilities of JSD positions, like the PSS, are determined at the judicial district level, the HIDS Program Office does not see a need to define certain roles in the HIDS Program Guide. However, the HIDS Program Office offers training to these individuals in the event they are tasked with HIDS-related matters.

(U) Without properly defined roles and responsibilities, JSD cannot maintain adequate oversight of the HIDS program and ensure those responsible for implementing the program are doing so in accordance with applicable HIDS policies. For example, the HIDS Program Guide states that PSSs should be familiar with the information and procedures in the Program Guide to ensure accurate and consistent information is provided to participating judges. However, the HIDS Program Guide provides no additional information on the specific duties and responsibilities of the PSS position. In comparison, JSD has published a HIDS JSI Handbook that details the expectations of this key role in facilitating the HIDS program, which we believe is helpful to JSIs in the execution of their responsibilities. Therefore, we recommend that the USMS update the HIDS Program Guide to identify and define the authorities, qualifications, roles, and responsibilities of all individuals tasked with facilitating, executing, and overseeing the HIDS program.

(U) Required HIDS Training Could More Effectively Equip JSD Personnel

(U) We found that JSIs—the judicial district-level USMS officials on which the HIDS program most relies to facilitate the program and ensure judges are well informed about the program—are not required to complete formal HIDS training. Generally, on an annual basis, the HIDS Program Office presents a series of HIDS training slides and holds a question-and-answer session to JSD employees as a part of more comprehensive non-mandatory training coordinated and provided by the USMS National Center for Judicial Security. However, the HIDS Program Office does not initiate these training sessions or maintain its own records of completion for training attendees. As the primary USMS liaison at each judicial district for the HIDS program, JSIs are expected, but not required, to complete one of these HIDS training sessions and remain up to date with the program's operational policies, procedures, and materials published by JSD and accessible online. However, the HIDS Program Office does not confirm whether JSIs have completed this training. Furthermore, the HIDS Program Guide does not extend these expectations to other JSD personnel, despite their involvement in facilitating the program.

(U) Because of JSD's reliance on JSIs to share HIDS information, training, program updates, newsletters, and frequently asked questions with their respective district judges, inadequate HIDS training of these key personnel can lead to miscommunications, unnecessary errors or omissions in HIDS paperwork

submissions, and delays in HIDS program enrollments and reimbursement payments. For JSIs and other pertinent JSD personnel to be adequately, consistently, and uniformly knowledgeable and prepared to assist judges in their judicial districts with all aspects of the HIDS program, the USMS should track completion of HIDS training sessions for all JSD personnel. In addition, PSSs should also be required to complete periodic HIDS training. Therefore, we recommend that the USMS update the HIDS Program Guide to require all appropriate JSD personnel to complete periodic HIDS training and track the completion of any HIDS training for all attendees.

(U) The USMS Should Document its Approval of Reimbursement Exceptions

(U) The HIDS Program Office may approve exceptions to the minimum required HIDS equipment if a specific circumstance warrants a deviation. Reviewers are to use their judgment and experience to make approval and denial determinations. However, we found that the USMS did not maintain records supporting these determinations in the reimbursement requests we tested. Without such documentation, we were unable to determine if the approvals and denials were in fact warranted by circumstance. As such, we believe HIDS reimbursement approval authorities should more adequately document the rationale and justification for approving or denying requests (including partial approvals and denials) for reimbursement amounts over the program limits and for equipment that exceeds or falls outside of the allowable equipment requirements. Figure 2 shows the USMS approval section within the HIDS Reimbursement Form that could serve as a logical space to document such justifications. We recommend that the USMS require HIDS reimbursement approval authorities to document in the HIDS Reimbursement Form their justification for approving or denying requests for amounts or equipment that exceed established HIDS program parameters.

(U) Figure 2

(U) HIDS Reimbursement Form – Possible Approval and Denial Justification Space

U.S. MARSHALS SERVICE USE ONLY

HIDS Request ID

USMS Comments

USMS Approving Official Sign Here USMS Authorized Funds Certifying Official Sign Here

(U) Source: USMS

(U) The USMS Could Improve its HIDS Reimbursement Appeal Decision Process

(U) When the HIDS Program Office does not approve exceptions on initial reimbursement requests that exceed the \$2,500 system installation reimbursement limit or allowed technical specifications, a judge can submit an appeal. Examples of these situations may involve a judge claiming that all required HIDS equipment cannot be installed in their residence within the \$2,500 reimbursement limit, or a judge asserting that an exception is necessary to cover atypical security requirements. Appeals are considered by the HIDS

Program Office only if the additional amount requested is for the installation of required or recommended security devices and will not cover optional equipment. Judges initiate the appeal process by completing and submitting a HIDS appeal request form detailing the reason for the appeal and providing supporting documentation. The supporting documentation must contain adequate information from which the deciding official can fully assess the situation, including two vendor estimates, justification for systems or equipment that falls outside of the program parameters, and information describing why the judge believes it is appropriate to receive reimbursement over the limit or for an uncovered component. The appeal documentation provided must be sufficient to allow the deciding official to make a decision based on the approval thresholds shown in Table 3.

(U) Table 3

(U) HIDS Appeal Approval Thresholds for Amounts over \$2,500

| Additional Amount Sought | Approval Threshold | Burden of Proof |
|--------------------------|---|---|
| Up to \$1,000 | Reasonable efforts have been made to procure required system components within the program limits. | Two estimates to establish reasonable efforts were made to obtain system components that align with similar systems in the area. |
| \$1,000 to \$3,000 | Required system components cannot be obtained for less than the requested amount. | The system is designed in the most cost-effective manner and the cost aligns with the lowest comparable vendor estimates in the area. |
| More than \$3,000 | Required system components cannot be obtained for less than the requested amount and an extraordinary security need exists. | An extraordinary security need or current threat exists and concurrence from the Assistant Director of JSD. |

Source: USMS

(U) We examined a judgmental sample of 10 of 21 HIDS installation reimbursement appeals submitted by judges from June through October 2022 and found that the justifications for the appeal decisions were based on sufficient supporting documentation. However, we also found that initial HIDS appeal requests frequently do not include sufficient documentation necessary for USMS officials to make an informed decision, thereby necessitating follow up requests for additional documentation. While the appeal intake system records the day the initial appeal request is received, it does not have a mechanism in place to track when all necessary documentation is received. As a result, the USMS is unable to assess the timeliness of appeal decisions to determine its rate of success in meeting the current USMS policy requirement that appeals determinations be completed within 7 days of receipt and timely providing resolution to appealing judges. Therefore, we recommend the USMS reevaluate its appeal policy and process and implement any necessary changes to ensure the timeliness of appeal decisions, such as tracking the date all documentation is received.

(U) Other USMS Actions to Protect Federal Judges Away from the Courthouse

(U) In addition to the HIDS program, the USMS implements other efforts to protect judges while they are away from the heightened security of the courthouse. These efforts include Deputy U.S. Marshals performing duties related to personal protection, site security, counter-surveillance and surveillance detection, and education for judges on how to protect their PII.

(U) The USMS is Taking Proactive Steps to Improve Its Protective Detail Capabilities

(U) As previously stated, the USMS assesses all threats against judges to determine the credibility and seriousness of the threat and opens a threat investigation if it has reasonable indication that a crime has, will, or may occur. USMS threat investigations are conducted to develop a mitigation plan designed to reduce the risk to the protected person. If a threat investigation results in the deployment of a protective detail, the USMS selects and assigns Deputy U.S. Marshals, drawn from any district or division, to perform the detail. According to JSD, all Deputy U.S. Marshals receive basic protective services training, and the USMS has been able to staff all judicial protective detail missions with an appropriate number of Deputy U.S. Marshals. However, JSD policy indicates that circumstances occasionally require the deployment of Deputy U.S. Marshals with specialized training in counter-surveillance and surveillance detection to supplement the physical protection of judges. According to JSD staff, JSD intends to add Deputy U.S. Marshals to its Counter-Surveillance/Surveillance Detection (CS/SD) Unit to proactively address a general upward trend in threats received. JSD told us this would be a positive step because the unavailability of specialized personnel would adversely impact the security of protected persons.

(U) In addition to its plans to increase the number of personnel participating in the CS/SD Unit, the Assistant Chief Inspector of the Office of Protective Operations is in the process of updating the program's Standard Operating Procedures (SOPs). As of November 2023, these draft SOPs were under Assistant Director review and included more specific information on how the program should operate and established detailed procedures for selecting program participants, deployments, and staff qualifications. We found the USMS is taking proactive steps to improve the structure, organization, and operation of the Office of Protective Operations, including the CS/SD Unit program, that we believe will assist in its efforts to continue mitigating threats to the judiciary and keep pace with a general upward trend in threats.

(U) USMS Makes Adequate Efforts to Educate and Inform Judges About Protecting Their Personally Identifiable Information

(U) The protection of the judiciary's PII is an important element in helping ensure the safety of federal judges. PII includes sensitive information such as home addresses, which, if publicly available, could present safety risks to federal judges. Protecting judicial PII requires individual judges to take affirmative steps to remove and keep certain information out of the public domain.⁷

⁷ (U) In December 2022, Congress took action to help protect federal judges' PII by passing the Daniel A. Claitor Judicial Security and Privacy Act of 2022 as part of the National Defense Authorization Act for FY 2023. This Act provided additional protection for judges' PII by prohibiting government agencies, data brokers, and other persons and businesses from knowingly buying, selling, and otherwise making publicly available this information, and by allowing judges to request that these entities remove such PII from public view. The Act also authorized the USMS to expand its

Continued

(U) Prior to this audit, the USMS published various informational and training aids to educate judges on ways to protect their PII. Namely, USMS Publication 94, Offsite Security, is a formal JSD publication with comprehensive guidelines on topics such as maintaining internet security, using social media, and preventing identity theft. As a result of our prior audit of USMS Judicial Security Activities, the USMS has incorporated information from Publication 94 into annual judicial district-level security briefings to judges. In addition, the HIDS program enrollment form strongly suggests that judges encrypt the submission of sensitive information emailed to the HIDS Program Office and provides encryption instructions.

(U) According to a JSD official, local laws at the judicial district level dictate what privacy protection information and services are available for USMS personnel to pass on to judges. For example, we found that JSIs in the District of Colorado provided their judges with instructions on how to become a confidential voter, a status that omits an individual's voter registration information from any lists requested by individuals as well as from appearing in third-party website postings of registered voters. Additionally, information was provided to the judiciary in this judicial district on how to enroll in a government-vetted service that proactively searches the Internet and removes online PII of the enrollee.

(U) We found that the USMS recognizes that protecting PII is a continual process and an integral part of protecting the safety of the judiciary. As such, the USMS urges judges to maintain vigilance and practice proactive measures to safeguard their PII by regularly reviewing and attempting to remove personal information from internet sources. The USMS appropriately recommends that judges review their digital footprint every 3 to 6 months. We therefore found that the USMS is making substantial efforts to educate and inform judges on ways to protect their PII.

current judicial security workforce to ensure that it is equipped to anticipate and deter threats to the judiciary. Pub. L. No. 117-263. [James M. Inhofe National Defense Authorization Act for Fiscal Year 2023](https://www.congress.gov/117/plaws/publ263/PLAW-117publ263.pdf).
<https://www.congress.gov/117/plaws/publ263/PLAW-117publ263.pdf>.

(U) Conclusion and Recommendations

(U) With a rise in threats received by judges, and with the advancing complexity of the threat landscape, the USMS faces an evolving challenge to protect the federal judiciary. The agency has been successful in achieving its protective mandate over the past 3 years; however, ensuring the safety of federal judges is an unending pursuit that is particularly challenging when these individuals are outside of the courthouse. With the USMS's use of protective details reserved for the most egregious threats to a judge's safety, the home security provided through the HIDS program becomes paramount in mitigating inherent risk to the safety of judges at their places of residence. As such, it is imperative that the USMS maximize enrollment in the HIDS program and ensure that it is operating effectively.

(U) We found that about 72 percent of eligible judges are currently enrolled in the restructured HIDS program, which is an increase of approximately 13 percent over the prior program. However, the USMS largely does not have insight into the reasons why the remaining 28 percent of judges have elected not to enroll, or why 223 judges who had enrolled in the prior program have elected not to enroll in the restructured program. We also found that while areas of the restructured HIDS program are an improvement over the previous program, the new program has weaknesses of its own, including a lack of USMS involvement in the planning, design, acquisition, and installation of individual judge's systems, and new challenges posed by the reimbursement element of the program. The USMS should pursue continuous improvement of the HIDS program by seeking judicial input on impediments that may dissuade judges from participating—and taking other steps, such as providing more training to USMS personnel—could help the USMS improve the HIDS program. Therefore, we make the following nine recommendations to improve the USMS's programs and practices concerning the protection of federal judges at their places of residence.

(U) We recommend that the USMS:

1. (U) Establish requirements for regularly soliciting input from judges eligible to participate in the HIDS program, evaluating the judges' input, and assessing the feasibility of implementing changes that will increase HIDS program enrollment and help ensure current participants remain enrolled in the program.
2. (U) Assess the HIDS reimbursement process and consider feedback received from judges to identify opportunities to streamline the process.
3. (U) Track alarm monitoring participation rates, consider feedback from judges about why they choose not to obtain monitoring services, and make any necessary changes to the HIDS program to maximize the number of judges electing to include alarm monitoring in their HIDS configuration.
4. (U) Require district JSIs to conduct residential security surveys of the home of all HIDS participants upon their enrollment in the program, unless the participant specifically declines.

5. (U) Update the HIDS Program Guide with established procedures on how to properly conduct, document, and use residential security surveys to inform pertinent processes within the HIDS program.
6. (U) Update the HIDS Program Guide to identify and define the authorities, qualifications, roles, and responsibilities of all individuals tasked with facilitating, executing, and overseeing the HIDS program.
7. (U) Update the HIDS Program Guide to require all appropriate JSD personnel to complete periodic HIDS training and track the completion of any HIDS training for all attendees.
8. (U) Require HIDS reimbursement approval authorities to document in the HIDS Reimbursement Form their justification for approving or denying requests for amounts or equipment that exceed established HIDS program parameters.
9. (U) Reevaluate its appeal policy and process and implement any necessary changes to ensure the timeliness of appeal decisions, such as tracking the date all documentation is received.

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

(U) Objective

(U) The objective of our audit was to assess the United States Marshals Service's (USMS) programs and practices concerning the protection of federal judges at their places of residence, with a focus on the Home Intrusion Detection System (HIDS) program.

(U) Scope and Methodology

(U) The scope of our audit generally covered the USMS's residential judicial security activities from August 2021 through December 2023. To accomplish our objective, we reviewed documentation relevant to Judicial Security Divisions (JSD) protective mandate, including policies and procedures guiding its judicial security operations, the prior HIDS program, the reimbursement-based HIDS program, and the USMS's approach to providing protective details and conducting counter-surveillance operations.

(U) We interviewed officials from JSD responsible for overseeing the HIDS program to gain an understanding of the USMS's planning, analysis, and research efforts that contributed to the decision to restructure the program. We conducted interviews with officials from the HIDS Program Office responsible for establishing and implementing the reimbursement-based HIDS program to evaluate the operation and oversight of the program. We also interviewed the Judicial Security Inspector (JSI) and Physical Security Specialist (PSS) responsible for facilitating the HIDS program in the District of Colorado to determine if the program is operating as expected and to identify areas of needed improvement. To obtain the insight of JSIs in other judicial districts, we distributed a questionnaire to a judgmental sample of 25 JSIs throughout the country and evaluated the responses of 15 respondents and obtained their perspectives on the HIDS program. Furthermore, we examined a sample of 297 HIDS reimbursement requests for system installation and monthly monitoring services, and 10 HIDS appeals submitted by judges to assess the appropriateness, accuracy, and timeliness of reimbursement payments made by the USMS. We spoke with officials from JSD's Office of Protective Operations regarding their understanding and implementation of the USMS guidance pertinent to protective detail operations. Finally, we examined the USMS's efforts to educate and inform judges on actions they can take to safeguard and limit the accessibility and distribution of their PII.

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

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

(U) Internal Controls

(U) In this audit, we performed testing of internal controls significant within the context of our audit objective. 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 several underlying internal control principles within each of the five internal control components that were significant to the audit objective, including the principle that management should design control activities to achieve objectives and respond to risks. We assessed the design and operating effectiveness of these internal controls and identified weaknesses that we believe could affect the USMS's ability to adequately identify and respond to risks facing judges under its protection.

(U) The internal control deficiencies we found are discussed in the Audit Results section of this report. However, because our review was limited to those internal control components and underlying principles that we found significant to the objective of this audit, it may not have disclosed all internal control deficiencies that may have existed at the time of this audit.

(U) Sample-Based Testing

(U) To accomplish our audit objective, we performed sample-based testing to assess the accuracy and appropriateness of reimbursement payments made by the USMS to judges enrolled in the HIDS program. We also used this approach in distributing a questionnaire to select JSIs throughout the United States. In these efforts, we employed a judgmental sampling design to obtain broad exposure to numerous facets of the areas we reviewed. These non-statistical sample designs did not allow projection of the test results to the universe from which the samples were selected.

(U) Computer-Processed Data

(U) During our audit, we obtained HIDS enrollment and reimbursement data from the HIDS Reimbursement Power App (HIDS App) dashboard. Given that the HIDS App data is used for background and informational purposes, we did not test the reliability of this system as a whole, therefore any findings identified involving information from this system were verified with documentation from other sources.

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

(U) APPENDIX 2: Optional and Ineligible HIDS Equipment

| (U) Optional Equipment | | (U) Description | |
|--------------------------|------------|-----------------|------------|
| (U//LES) | [REDACTED] | (U//LES) | [REDACTED] |
| (U//LES) | [REDACTED] | (U//LES) | [REDACTED] |
| (U//LES) | [REDACTED] | (U//LES) | [REDACTED] |
| (U//LES) | [REDACTED] | (U//LES) | [REDACTED] |
| (U) Ineligible Equipment | | (U) Description | |
| (U//LES) | [REDACTED] | (U//LES) | [REDACTED] |
| (U//LES) | [REDACTED] | (U//LES) | [REDACTED] |
| (U//LES) | [REDACTED] | (U//LES) | [REDACTED] |
| (U//LES) | [REDACTED] | | |
| (U//LES) | [REDACTED] | | |
| (U//LES) | [REDACTED] | | |
| (U//LES) | [REDACTED] | | |

Source: USMS

(U) APPENDIX 3: The USMS's Response to the Draft Audit Report~~Unclassified//Law Enforcement Sensitive~~**U.S. Department of Justice**

United States Marshals Service

*Office of Professional Responsibility**Washington, DC 20530-0001*

July 24, 2024

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

FROM: Geoffrey S. Deas JOHNNY
Assistant Director WILLIAMS UNCLASSIFIED//LAW ENFORCEMENT SENSITIVE

SUBJECT: Response to Draft Audit Report: Audit of the United States
Marshals Service's Home Intrusion Detection System

(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 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 External Audit Liaison Krista Eck, Office of Professional Responsibility, at 202-819-4371.

Attachments

cc: Kimberly Rice
Regional Audit Manager
Office of the Inspector General

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

Michelle Hamilton
Acting Chief of Staff
United States Marshals Service

Unclassified//~~Law Enforcement Sensitive~~

**USMS Response to OIG Draft Report
Audit of the United States Marshals Service's Home Intrusion Detection System Program**

(U)Recommendation 1: Establish requirements for regularly soliciting input from judges eligible to participate in the HIDS program, evaluating the judges' input, and assessing the feasibility of implementing changes that will increase HIDS program enrollment and help ensure current participants remain enrolled in the program.

(U)USMS Response (Concur): The USMS is reviewing responses from the Home Intrusion Detection System (HIDS) Judicial survey to assist in developing long-term requirements for soliciting and incorporating input from judges eligible to participate in the HIDS Program. The goal is to group major and recurring issues into themes for a frequently asked questions (FAQ) document. The FAQ will be shared with the Judiciary, USMS Judicial Security Units (JSU), and AOUSC Judicial Security Officers (JSO) and will be made available at applicable events such as conferences and training sessions. The HIDS Program plans to work with the Administrative Office of the United States Courts (AOUSC) to recruit new judges under each Judicial Circuit's purview, as well as work with USMS district JSUs, to promote HIDS enrollment, site surveys, and ongoing judicial satisfaction. The HIDS Program will participate in as many judicial functions as funding will allow to promote in-person outreach with the Judiciary, AOUSC, and JSUs. The HIDS Program has monthly meetings scheduled with the AOUSC to discuss program pros/cons, issues, successes, and ways to ensure participants remain enrolled or new judges are enrolled. The HIDS Program is also communicating with vetted alarm system vendors to ensure they understand program rules and requirements and to assist judges in obtaining HIDS-related documents or services.

(U)Recommendation 2: Assess the HIDS reimbursement process and consider input from judges from the survey in recommendation 1 to identify opportunities to streamline the process.

(U)USMS Response (Concur): See above. The HIDS Satisfaction Survey contains several items that request information on gaps and inconsistencies in the current program as well as suggestions for improvement.

(U)Recommendation 3: Track alarm monitoring participation rates, consider feedback from judges from the survey in recommendation 1 about why they choose not to obtain monitoring services, and make any necessary changes to the HIDS program to maximize the number of judges electing to include alarm monitoring in their HIDS configuration.

(U)USMS Response (Concur): The HIDS Program currently recommends Judges obtain monitoring services for enhanced safety. Monitoring participation rates can be tracked if a Judge has submitted a request for reimbursement. The HIDS Program will continue to promote monitoring through outreach and training opportunities.

Unclassified//~~Law Enforcement Sensitive~~

(U)Recommendation 4: Require district JSIs to conduct residential security surveys of the home of all HIDS participants upon their enrollment in the program, unless the participant specifically declines.

(U)USMS Response (Concur): District Judicial Security Inspectors perform this duty at the start of the enrollment process. JSUs across the country are currently assisting HIDS participants with residential security surveys. The JSU member will assist the vendor with the survey. This text is from the JSD-HIDS, JSI Handbook:

(U)If the judge chooses to have equipment installed by a vendor, the service provider may conduct a survey to determine their recommended configuration of HIDS equipment for the residence.

(U)You may be requested to be present when a vendor comes to survey a home. The presence of a JSI may provide a sense of security and confidence to the judge. It is up to you to determine if you can accommodate this request.

(U)JSUs also offer this service each year as part of the Judicial profile update or at any request of a Judge. JSIs will be encouraged to communicate this assistance to their protectees as well as perform periodic or random drive-by checks of residences to enhance the security posture.

(U)Recommendation 5: Update the HIDS Program Guide with established procedures on how to properly conduct, document, and use residential security surveys to inform pertinent processes within the HIDS program.

(U)USMS Response (Concur): The HIDS Program Guide is being updated with guidelines for conducting residential security surveys and a copy will be provided as soon as available.

(U)The HIDS Program Guide and JSU Guide are living documents and will continue to be updated to enhance the safety of the Judiciary and make improvements to the HIDS Program.

(U)Each JSU has tasks which may be required on a daily, weekly, monthly, annual, or continuous basis. Part of this list of tasks is completion of annual USMS related forms to include:

- Form USM-50, *Judicial Personal Profile*;
- Form USM-50B, *Residential Security Form*;
- Form USM-50R, *Residential Floorplan Information*;
- Form USM-50S, *Security Assessment*;
- Form USM-50U, *Update*;
- Form USM-50J, *Judicial Duress Device Profile*; and
- Form USM-50Z, *Protected Persons Profile & Security Brief Tracking Report*.

(U)These forms will be added to the HIDS Program Guide as forms which can be used to reference, document, and assist in the surveys for the implementation of the HIDS program for a Judge's residence.

Unclassified//~~Law Enforcement Sensitive~~

(U)Recommendation 6: Update the HIDS Program Guide to identify and define the authorities, qualifications, roles, and responsibilities of all individuals tasked with facilitating, executing, and overseeing the HIDS program.

(U)USMS Response (Concur): The HIDS Program Guide is being updated to provide these descriptions and a copy will be provided as soon as available.

(U)JSU Members:

(U)JSU Supervisor: Oversight of the judicial security mission for any district. The supervisor must be able to resolve security issues or problems, schedule installation appointments, possess a knowledge of set standards and requirements for HIDS systems, and conduct training for personnel to ensure they have the most up to date and relevant information.

(U)JSIs: Critical front-line members in the USMS mission of protecting the judiciary. Conducts security surveys of residences or facilities and provides feedback and recommendations to improve the security posture of the facility or residence. JSU primary point of contact for the district judges.

(U)District Physical Security Specialist (DPSS): The DPSS can train the protectees on the use of security systems (e.g., duress alarms, home intrusion detection systems, etc.). Conducts security surveys of residences or facilities and provides feedback and recommendations to improve the security posture of the facility or residence.

(U)JSU members will assist the vendor with the residential survey, ensuring the HIDS Program requirements are met, and answer all questions from the protectee about their HIDS system and reimbursement process.

(U)JSD HIDS Program Office:

(U)The JSD HIDS mission is to provide the Federal Judiciary with advanced security solutions to support their safety away from hardened United States court facilities.

(U)The HIDS Program Office manages, and assists with all areas of the program for the Judiciary and JSU. The Program Office can answer questions related to the program, enrollment, or the reimbursement process, including:

- Reviewing vendor system recommendations and estimates;
- Suggesting additional or alternate vendors in an area;
- Explaining program coverage and eligibility;
- Suggesting cost-lowering adjustments and substitutions that still achieve appropriate security coverage;
- Assisting with enrollment and reimbursement form questions;
- Checking the status of an enrollment or reimbursement submission; and
- Other HIDS Program questions.

Unclassified//~~Law Enforcement Sensitive~~

(U)Recommendation 7: Update the HIDS Program Guide to require all appropriate JSD personnel to complete periodic HIDS training and track the completion of any HIDS training for all attendees.

(U)USMS Response (Concur): The HIDS Program Guide is being updated with training requirements and a copy will be provided as soon as it is available. The HIDS training is included in JSU component on boarding and sustainment trainings and is tracked by the National Center for Judicial Security and the USMS Training Division. The HIDS Program Office has access to roster information as requested.

(U)Recommendation 8: Require HIDS reimbursement approval authorities to document on the HIDS Reimbursement Form their justification for approving or denying requests for funds or equipment that exceed established HIDS program parameters.

(U)USMS Response (Concur): The USMS tracks justifications in the HIDS Power App in a section designated for free text notes. The USMS does not recommend tracking the justification for approvals or denials in the PDF form since these are locked after being signed by the judges and would unnecessarily extend the signatures and approval process, which is a topic of complaint identified in the survey.

(U)Recommendation 9: Reevaluate its appeal policy and process and implement any necessary changes to ensure the timeliness of appeal decisions, such as tracking the date all documentation is received.

(U)USMS Response (Concur): The HIDS currently ingests appeals on the day received and the HIDS Power App tracks that date automatically when saved. When new documentation is received and uploaded to the Power App, the app automatically adds the additional date and time when the material is uploaded. The HIDS Program will also ensure notes are made in the running text blocks within the appeal file.

(U) APPENDIX 4: Office of the Inspector General Analysis and Summary of Actions Necessary to Close the Audit 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 response and summary of actions necessary to close the report.

(U) Recommendations for the USMS:

1. (U) Establish requirements for regularly soliciting input from judges eligible to participate in the HIDS program, evaluating the judges' input, and assessing the feasibility of implementing changes that will increase HIDS program enrollment and help ensure current participants remain enrolled in the program.

(U) Resolved. The USMS concurred with our recommendation; as a result, this recommendation is resolved. The USMS stated in its response that it is reviewing responses from the HIDS judicial survey to assist in developing long-term requirements for soliciting and incorporating input from judges eligible to participate in the program with the goal of grouping major and recurring issues into themes for a frequently asked questions (FAQ) document. The FAQ will be shared with the judiciary, USMS Judicial Security Units, and AOUSC Judicial Security Officers and will be made available at applicable events such as conferences and training sessions. The HIDS Program Office plans to work with the AOUSC and its district personnel to recruit new judges, promote enrollment, site surveys, and evaluate judicial satisfaction. The HIDS Program Office also plans to participate in as many judicial functions as possible to promote in-person outreach with all stakeholders. Additionally, the HIDS Program Office has monthly meetings scheduled with the AOUSC to discuss the HIDS program's issues, successes, and ways to ensure participants remain enrolled or new judges are enrolled. Finally, the USMS stated that the HIDS Program Office is also communicating with vetted alarm system vendors to ensure they understand program rules and requirements and to assist judges in obtaining HIDS-related documents or services.

(U) This recommendation can be closed when we receive evidence establishing requirements for regularly soliciting input from judges eligible to participate in the HIDS program, evaluating the judges' input, and assessing of the feasibility of implementing changes that will increase HIDS program enrollment and help ensure current participants remain enrolled in the program.

2. (U) Assess the HIDS reimbursement process and consider feedback received from judges to identify opportunities to streamline the process.

(U) Resolved. The USMS concurred with our recommendation; as a result, this recommendation is resolved. The USMS stated in its response that the HIDS Satisfaction Survey, the results of which it is currently reviewing, contained several items that request information on gaps and inconsistencies in the current program as well as suggestions for improvement.

(U) This recommendation can be closed when we receive evidence that the USMS has assessed the reimbursement process and HIDS Satisfaction Survey results to identify opportunities to streamline the process and developed a plan to implement any improvements.

3. (U) **Track alarm monitoring participation rates, consider feedback from judges about why they choose not to obtain monitoring services, and make any necessary changes to the HIDS program to maximize the number of judges electing to include alarm monitoring in their HIDS configuration.**

(U) Resolved. The USMS concurred with our recommendation; as a result, this recommendation is resolved. The USMS stated in its response that the HIDS program currently recommends that judges obtain monitoring services for enhanced safety. Monitoring participation rates can be tracked if a judge has submitted a request for reimbursement. The HIDS program will continue to promote monitoring through outreach and training opportunities.

(U) This recommendation can be closed when we receive evidence that the USMS has begun tracking alarm monitoring participation rates, collecting feedback from judges, and addressing areas of improvement within its control to maximize the number of judges electing to include alarm monitoring in their HIDS configuration.

4. (U) **Require district JSIs to conduct residential security surveys of the home of all HIDS participants upon their enrollment in the program, unless the participant specifically declines.**

(U) Resolved. The USMS concurred with our recommendation; as a result, this recommendation is resolved. The USMS stated in its response that district JSIs perform this duty at the start of the enrollment process and Judicial Security Units (JSU) across the country participate in residential security surveys by assisting the vendor with the survey. Additionally, JSUs offer this service each year as part of the Judicial profile update or at the request of a judge. JSIs will be encouraged to communicate this assistance to their protectees as well as perform periodic or random drive-by checks of residences to enhance the security posture. However, the USMS did not provide evidence demonstrating that these surveys are being conducted as described.

(U) This recommendation can be closed when we receive documentation requiring district JSIs to conduct residential security surveys of the home of all HIDS participants upon their enrollment in the program, unless the participant specifically declines.

5. (U) **Update the HIDS Program Guide with established procedures on how to properly conduct, document, and use residential security surveys to inform pertinent processes within the HIDS program.**

(U) Resolved. The USMS concurred with our recommendation; as a result, this recommendation is resolved. The USMS stated in its response that it is updating the HIDS Program Guide with guidelines for conducting residential security surveys. The update will include several forms that can be used to reference, document, and assist in the surveys for the implementation of the HIDS program for a judge's residence.

(U) This recommendation can be closed when we receive the updated HIDS Program Guide establishing procedures on how to properly conduct, document, and use residential security surveys to inform pertinent processes within the HIDS program.

6. (U) Update the HIDS Program Guide to identify and define the authorities, qualifications, roles, and responsibilities of all individuals tasked with facilitating, executing, and overseeing the HIDS program.

(U) Resolved. The USMS concurred with our recommendation; as a result, this recommendation is resolved. The USMS stated in its response that it is updating the HIDS Program Guide to provide descriptions of various roles of JSU members and the JSD HIDS Program Office.

(U) This recommendation can be closed when we receive an updated HIDS Program Guide identifying and defining the authorities, qualifications, roles, and responsibilities of all individuals tasked with facilitating, executing, and overseeing the HIDS program.

7. (U) Update the HIDS Program Guide to require all appropriate JSD personnel to complete periodic HIDS training and track the completion of any HIDS training for all attendees.

(U) Resolved. The USMS concurred with our recommendation; as a result, this recommendation is resolved. The USMS stated in its response that it is updating the HIDS Program Guide to include training requirements.

(U) This recommendation can be closed when we receive an updated HIDS Program Guide with established HIDS training requirements for all appropriate JSD personnel, including how the USMS will track training attendance and ensure it is completed periodically.

8. (U) Require HIDS reimbursement approval authorities to document in the HIDS Reimbursement Form their justification for approving or denying requests for amounts or equipment that exceed established HIDS program parameters.

(U) Resolved. The USMS concurred with our recommendation; as a result, this recommendation is resolved. The USMS stated in its response that it tracks approval justifications in the HIDS Power App in a section designated for free text notes. The USMS does not recommend tracking the justification for approvals or denials in the HIDS reimbursement request PDF form since they are locked after being signed by the judges. However, the USMS did not provide evidence demonstrating how the HIDS App adequately documents approval and denial justifications.

(U) This recommendation can be closed when we receive evidence that HIDS approval and denial justifications for requested amounts or equipment that exceed established HIDS program parameters are appropriately documented.

9. (U) Reevaluate its appeal policy and process and implement any necessary changes to ensure the timeliness of appeal decisions, such as tracking the date all documentation is received.

(U) Resolved. The USMS concurred with our recommendation; as a result, this recommendation is resolved. The USMS stated in its response that the HIDS App automatically tracks the date that appeals are received when they are saved in the system. Additionally, when new documentation is received and uploaded to the HIDS App, it automatically adds the additional date and time the material is uploaded. The USMS stated that the HIDS program will ensure notes are made in the running text blocks within the appeal file. However, the USMS did not provide evidence demonstrating how the HIDS App automatically tracks the dates and times when additional documentation is received, or how this information is used to ensure the timeliness of appeal decisions.

(U) This recommendation can be closed when we receive evidence that the USMS has reevaluated its appeal policy and process and implemented any necessary changes to ensure the timeliness of appeal decisions, such as tracking the date all documentation is received.