TREASURY INSPECTOR GENERAL FOR TAX ADMINISTRATION

Management Controls Should Be Strengthened to Improve Hardware Asset Inventory Reliability

July 13, 2018

Reference Number: 2018-20-041

This report has cleared the Treasury Inspector General for Tax Administration disclosure review process and information determined to be restricted from public release has been redacted from this document.

Phone Number / 202-622-6500
E-mail Address / TIGTACommunications@tigta.treas.gov
Website / http://www.treasury.gov/tigta

To report fraud, waste, or abuse, call our toll-free hotline at:

1-800-366-4484

By Web:

www.treasury.gov/tigta/

Or Write:

Treasury Inspector General for Tax Administration
P.O. Box 589
Ben Franklin Station
Washington, D.C. 20044-0589

Information you provide is confidential and you may remain anonymous.

MANAGEMENT CONTROLS SHOULD BE STRENGTHENED TO IMPROVE HARDWARE ASSET INVENTORY RELIABILITY

Highlights

Final Report issued on July 13, 2018

Highlights of Reference Number: 2018-20-041 to the Commissioner of Internal Revenue.

IMPACT ON TAXPAYERS

The Service Asset and Configuration Management organization's Hardware Asset Management office is responsible for providing enterprise-wide oversight, coordination, and guidance on hardware asset management. Failure to timely update asset inventory records impedes the IRS's ability to timely detect the loss, theft, or misuse of Government property. Lack of controls over hardware assets increases the risk of unauthorized access to taxpayer or other sensitive information.

WHY TIGTA DID THE AUDIT

This audit was initiated to evaluate the IRS's management controls over its information technology hardware asset inventory.

WHAT TIGTA FOUND

The IRS has taken steps to improve its hardware asset management by revising the *Hardware User Guide* and continuing to look for opportunities to implement technologies and automation into its hardware asset inventory processes. The IRS verified 90.6 percent of its Class A assets (*e.g.*, desktop and laptop computers and servers) and Class B assets (*e.g.*, smartphones). This was short of its Fiscal Year 2017 inventory objective of a 95 percent or better certification rate. Specifically, the IRS verified 226,947 of 250,520 assets.

While the certifying officials returned signed *Certification Letters* acknowledging their commitment to make all attempts to find unverified and missing assets, they only verified an additional 7,095 (23.1 percent) of the 30,668 initially unverified and missing hardware assets during the reconciliation period, leaving a balance of 23,573 unverified and missing assets. During site visits to nine IRS locations, TIGTA was able to verify unverified and missing assets by physically locating or otherwise accounting for 54 (41.5 percent) of 130 hardware assets selected for review.

In addition, the IRS did not ensure that all hardware assets were controlled in the Knowledge Incident/Problem Service Asset Management–Asset Manager (KISAM-AM) module. TIGTA identified that 17 of 102 hardware assets selected for review were not properly controlled.

Furthermore, certifying officials did not always ensure that the necessary steps were conducted to locate missing hardware assets prior to reporting them as lost. TIGTA located three of 40 hardware assets selected for review that the IRS had reported as lost. In addition, the IRS has found an additional 95 of 2,429 hardware assets that it had previously reported as lost to TIGTA's Office of Investigations.

WHAT TIGTA RECOMMENDED

TIGTA recommended that the Chief Information Officer review and update the existing *Hardware Asset Management Inventory Certification Plan* and reconciliation process to improve the compliance, accountability, and participation of all asset inventory owners and stakeholders; ensure that newly acquired assets are timely added into the KISAM-AM module by revising the current asset acquisition and receipt process to ensure the timely delivery of required vendor reporting and to improve accountability of personnel responsible for the receipt and acceptance process; and direct certifying officials to ensure that sufficient research is properly conducted to locate missing hardware assets prior to reporting them as lost.

IRS management agreed with all of our recommendations and plans to update the *Hardware Asset Management Inventory Certification Plan* and reconciliation process; ensure that newly acquired assets are timely added into the KISAM-AM module; and direct certifying officials to conduct sufficient asset research.

TREASURY INSPECTOR GENERAL
FOR TAX ADMINISTRATION

DEPARTMENT OF THE TREASURY
WASHINGTON, D.C. 20220

July 13, 2018

MEMORANDUM FOR COMMISSIONER OF INTERNAL REVENUE

FROM: Michael E. McKenney
Deputy Inspector General for Audit

SUBJECT: Final Audit Report – Management Controls Should Be Strengthened to Improve Hardware Asset Inventory Reliability (Audit # 201720030)

This report presents the results of our review to evaluate the Internal Revenue Service's (IRS) management controls over its information technology hardware asset inventory. This audit is included in our Fiscal Year 2018 Annual Audit Plan and addresses the major management challenge of Security Over Taxpayer Data and Protection of IRS Resources.

Management's complete response to the draft report is included as Appendix VII.

Copies of this report are also being sent to the IRS managers affected by the report recommendations. If you have any questions, please contact me or Danny R. Verneuille, Assistant Inspector General for Audit (Security and Information Technology Services).

Table of Contents

Abbreviations

AM	Asset Manager
HAM	Hardware Asset Management
IRS	Internal Revenue Service
KISAM	Knowledge Incident/Problem Service Asset Management
TIGTA	Treasury Inspector General for Tax Administration
UNS	User and Network Services

Background

The User and Network Services (UNS) organization is responsible for managing the Internal Revenue Service's (IRS) information technology hardware assets (hereafter referred to as hardware assets).[1] The UNS organization's mission includes certifying the accuracy of the hardware asset inventory each fiscal year. Although the UNS organization is the business process owner of the hardware asset inventory data, the Office of Chief Counsel, Criminal Investigation, Facilities Management and Security Services, and the other Information Technology component organizations are responsible for verifying and certifying the inventory accuracy of the hardware assets under their respective control. IRS asset owners, stakeholders, and personnel responsible for hardware assets play a critical role in ensuring the hardware asset inventory accuracy.

Within the UNS organization, the Service Asset and Configuration Management organization's Hardware Asset Management (HAM) office is responsible for providing enterprise-wide oversight, coordination, and guidance on hardware asset management. It uses the Knowledge Incident/Problem Service Asset Management-Asset Manager (KISAM-AM) module to track the IRS's hardware asset inventory.

Internal Revenue Manual 2.149, *Information Technology Asset Management*,[2] establishes general policies and procedures for the management and control of IRS hardware assets, but specific guidance is provided in the annual *Hardware Asset Management Inventory Certification Plan* and in the *Asset Management – Hardware User Guide*. The HAM office issues the *Hardware Asset Management Inventory Certification Plan*, and it defines the inventory certification process for IRS hardware assets and provides an overview of the asset management objectives, guidelines, activities, and deadlines necessary to meet the IRS's goals. The *Hardware User Guide* requires all asset inventory certifying officials to follow the certification requirements and meet the deadlines within the annual plan. Ensuring that IRS asset data are complete and up to date in the KISAM-AM module is critical to the accuracy of the IRS's hardware asset inventory and its financial statements. As of October 1, 2017, the KISAM-AM module recorded 250,520 Class A[3] and Class B[4] hardware assets with an approximate purchase price value of $612 million.

[1] See Appendix VI for a glossary of terms.
[2] Internal Revenue Manual 2.149 has subsections that include: 2.149.1, *Asset Management Policy* (Sept. 23, 2015); 2.149.2, *Asset Management Process Description* (October 19, 2015); 2.149.3, *Asset Management Hardware Procedures* (Oct. 19, 2015); and 2.149.4, *Asset Management Software Procedures* (Sept. 28, 2015).
[3] Class A assets are capital high-end assets that include mainframe computers, desktop and laptop computers, servers, routers, firewalls, network printers, *etc*.
[4] Class B assets are personal digital assistants, smartphones, and stick personal computers.

The IRS's annual fiscal year hardware asset inventory certification cycle begins on October 1, ends on September 30, and includes the following two distinct periods:

- **Certification Period** – The certification period occurs from October 1 through June 30 and is used to verify and update hardware assets in the KISAM-AM module. During the certification period, the IRS considers an asset verified and certified for the respective fiscal year when one or more of the KISAM-AM module fields (*e.g.*, 1) Inventory Date, 2) Barcode Scan Date, 3) Last Hardware Scan Date, 4) Last Connected Date, or 5) SelfCert Date) are populated with a date of October 1 of the current fiscal year or later. Asset verification methods include: barcode scanning, self-certification, hardware upgrades, maintenance calls initiated by helpdesk tickets, receipt of new or transferred assets, or electronic verification methods that include the use of automated asset discovery scanning tools[5] or network pings to verify the existence of an asset.
- **Reconciliation Period** – The reconciliation period occurs from July 1 through September 30 and is used to resolve any unverified or missing hardware assets identified during the certification period. Upon conclusion of the certification period, the HAM office sends a hardware asset *Reconciliation Plan* and *Reconciliation Plan Letter* to each certifying organization that summarizes the number of unverified and missing asset records requiring correction or modification in the KISAM-AM module. Each certifying organization must then submit a signed *Certification Letter* back to the HAM office acknowledging the number of unverified and missing asset records in the hardware asset *Reconciliation Plan* and its commitment by the certifying official to make all attempts to locate the unverified and missing assets by September 30.

This review was performed with information obtained from the Information Technology UNS organization in Plantation, Florida, and during site visits to offices in Washington, D.C.; Plantation, Florida; Chamblee, Georgia; Lanham, Maryland; New York, New York; Memphis, Tennessee; Farmers Branch, Texas; Ogden, Utah; and Kearneysville, West Virginia, during the period June 2017 through April 2018. 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. Detailed information on our audit objective, scope, and methodology is presented in Appendix I. Major contributors to the report are listed in Appendix II.

[5] The IRS used Tivoli® to electronically verify its assets during the Fiscal Year 2017 annual inventory certification cycle.

Results of Review

The IRS has taken steps to improve its hardware asset management. On November 14, 2017, the Service Asset and Configuration Management organization revised the *Hardware User Guide*. Revisions included updating assignment groups to better align with the KISAM-AM and KISAM-Service Manager modules; updating the asset and classification types, *e.g.*, Class A and Class B assets, to provide a more comprehensive list of hardware types for each classification; updating the description and definitions of disposal codes to provide further guidance and examples as references; and incorporating new asset management directives to provide context to the requirements of the asset management procedures.

Furthermore, HAM office officials explained that they continue to look for opportunities to implement technologies and automation into their hardware asset inventory processes in order to help reduce the burden and dependence on labor resources. HAM office management stated that they are working on data improvement strategies to more clearly identify the responsible organization for major asset categories within the KISAM-AM module. HAM office management believe that the data improvement strategies along with new automation opportunities will result in improved accountability through perpetual inventory verification and reduced reliance upon labor-intensive inventory activities. For example, an asset inventory automation initiative is underway with the following goals:

- Assess the hardware asset management current state and enterprise business requirements and develop an enterprise-wide asset management target state design and architecture.
- Document business requirements for additional technology improvement opportunities.
- Improve the use of technology to automate hardware asset inventory tasks.
- Automate hardware asset inventory workflow processes with a new barcode scanning solution and radio frequency identification technology, where feasible, to reduce manual tasks.
- Integrate new hardware asset discovery scanning tools with the KISAM-AM module.
- Fully automate and integrate the posting of hardware asset transactional data into the KISAM-AM module.

However, despite these efforts, management controls need to be further strengthened to improve the reliability of the IRS's hardware asset inventory.

Hardware Asset Inventory Certification Objectives Were Not Always Met

Specific guidance on the management and control of IRS hardware assets is provided in two documents. The *Hardware User Guide* requires that all asset owners and personnel tasked with inventory duties and responsibilities follow the certification requirements and meet the overall objectives of the annual *Hardware Asset Management Inventory Certification Plan*, including deadlines and deliverables. In addition, the *Hardware User Guide* provides specifics to further define program objectives described in the IRS's *Fiscal Year 2017 Hardware Asset Management Inventory Certification Plan*, dated February 15, 2017. These objectives include but are not limited to the following:

- Locate and verify the existence of controlled Class A and Class B hardware assets to achieve a 95 percent or greater certification rate. Personnel participating in the asset verification activities should always place a greater focus and priority on locating and discovering assets that are mobile, prone to theft or loss, or not easily or regularly discovered through automated tools.
- Verify and confirm that a KISAM-AM module inventory record is associated with every controlled asset. Asset management processes have been put in place to ensure that asset control begins in the procurement and acquisition phase through individual input and systemically batch adding multiple assets to the KISAM-AM module.
- Complete inventory transactions documented in the KISAM-AM module within 10 workdays of an action. Delayed transactions contribute to errors and inconsistencies within the KISAM-AM module.
- Certify that key KISAM-AM module fields are complete and accurate. The key fields include the Assignment Code, Barcode, Serial Number, Building Code, and User Name or Contact Name.[6] Although only five key fields have been identified, there may be other data fields that are important to the asset management process, and attention to their accuracy should be given during the verification process.
- Identify, resolve, and finalize actions on missing, lost, or stolen assets, and survey the assets out of the inventory. Unverified assets placed in a missing assignment status in the KISAM-AM module should be surveyed from the inventory after all attempts to find and locate the missing assets have been exhausted.

[6] The User Name field lists the employee name and standard employee identifier of the primary user of the assigned hardware asset. Shared hardware assets will not have an entry in the User Name field but rather will have the same employee information in the Contact Name field. Populating the Contact Name field for shared assets is mandatory.

The IRS did not meet its certification goal of 95 percent or better

As of October 1, 2017, the IRS verified 90.6 percent of its Class A and Class B assets, short of its Fiscal Year 2017 inventory objective of a 95 percent or better certification rate. Specifically, the IRS verified 226,947 of its 250,520 assets. Appendix V presents the summary results by hardware type from the IRS's Fiscal Year 2017 asset inventory certification. To provide a historical perspective, we reviewed the hardware asset inventory certification rates for each of the preceding three fiscal years.[7] The IRS certification rate of its Class A and Class B assets ranged from a low of 89.5 percent in Fiscal Year 2016 to a high of 93.5 percent in Fiscal Year 2014, averaging 91.6 percent for the last four fiscal years. Figure 1 presents the summary results from the IRS's Fiscal Years 2014 through 2017 hardware asset inventory certifications.

Figure 1: Summary Results of the IRS's Fiscal Years 2014 Through 2017 Hardware Asset Inventory Certifications

Fiscal Year	Total Assets	Verified Assets	Unverified/ Missing Assets[8]	Percentage Verified
2014	237,557	222,179	15,378	93.5%
2015	220,451	204,600	15,851	92.8%
2016	231,341	207,146	24,195	89.5%
2017	250,520	226,947	23,573	90.6%
Average				**91.6%**

Source: The IRS's Fiscal Years 2014 through 2017 Unverified Asset Data and Summary Reports.

After hardware asset *Reconciliation Plans* and *Reconciliation Plan Letters* were sent out, the certifying officials returned signed *Certification Letters* acknowledging the number of unverified and missing assets and their commitment to make all attempts to find them. To assess the effectiveness of the reconciliation period, we compared the *Unverified Asset Data and Summary Reports*, dated June 30 and October 1, 2017, respectively, to determine the effective rate at which certifying officials were resolving their respective unverified and missing hardware assets. We found that as of October 1, 2017, certifying officials only verified an additional 7,095 (23.1 percent) of the 30,668 initially unverified and missing hardware assets during the reconciliation period, leaving a balance of 23,573 unverified and missing assets.

To gain a better understanding of the reconciliation process, we selected a judgmental sample[9] of 130 (49 unverified, 41 missing, and 40 lost) hardware assets from the KISAM-AM module for nine IRS locations and attempted to find or account for the assets. With the assistance of HAM office personnel, we were able to verify unverified and missing assets. Specifically, we

[7] The IRS did not provide a certification rate objective for Fiscal Years 2014 through 2016.
[8] The unverified hardware assets include in-use, in-stock, and missing assets.
[9] A judgmental sample is a nonprobability sample, the results of which cannot be used to project to the population.

physically located or otherwise accounted for 54 (41.5 percent) of the 130 selected hardware assets,[10] which included the following:

- 37 unverified hardware assets.
- 14 missing hardware assets, two of which were excessed after they were found.[11]
- 3 assets the IRS had categorized as lost, one of which was excessed after it was found.[12]

We also assessed the hardware asset self-certification process. An asset is considered self-certified by any method for which there is direct contact with the asset's user, owner, system administrator, or other contact, including e-mail responses and user responses to the Information Technology organization's Customer Self-Certification website. As part of the self-certification process, users are provided asset information, such as the barcode, asset type, make, and model. The user only needs to certify that this information is accurate. Once the user certifies the information, the SelfCert Date field in the KISAM-AM module is updated.

We selected a judgmental sample of 38 assets that were self-certified during Fiscal Year 2017 to determine whether users certified the correct asset in their possession. After contacting each of the asset owners, we determined that one (2.6 percent) of the 38 assets was not actually in the possession of its assigned user. HAM office management explained that the user self-certified the same asset on three different occasions, but the user stated that he/she was not and has never been in possession of the asset. HAM office management stated that they conducted additional research on the asset but could not locate it or explain the circumstance related to this condition, other than that the asset could have been a shared asset. Further, HAM office management stated that they plan to report this asset as missing.

The IRS did not meet its inventory certification objective because, in part, some certifying officials did not provide direction to their organizational personnel responsible for verifying assets during the reconciliation period. In addition, HAM office management stated that they did not provide the hardware asset *Reconciliation Plan* and *Reconciliation Plan Letter* to the Enterprise Field Operations[13] organization because, in recent years, Enterprise Field Operations organization management had not been responsive in verifying assets under their respective control due to resource constraints. HAM office management stated that it would be difficult to reproduce the number of unverified and missing assets under the oversight or stewardship of the Enterprise Field Operations organization with complete accuracy because there are many asset

[10] We physically located 49 assets and accounted for an additional five other assets by contacting the person listed in the User Name or Contact Name fields from the KISAM-AM module record. Hardware assets include servers, a router, laptop and desktop computers, network printers, *etc*.
[11] The remaining 12 missing hardware assets not excessed had a total purchase price of $95,149.
[12] The remaining two lost hardware assets not excessed had a total purchase price of $61,243.
[13] The Enterprise Field Operations organization is part of the UNS organization.

categories that are shared between organizations, and it would be dependent upon the environment in which the asset is used.

However, with guidance provided by HAM office management, we estimate that the number of unverified and missing assets for the Enterprise Field Operations organization might be as high as 21,690. This would potentially represent 92 percent of the 23,573 total unverified and missing assets for the entire IRS during Fiscal Year 2017. HAM office management emphasized that the inventory certification process is labor intensive and time-consuming, with consideration needed to be given to staffing constraints and competing organizational priorities. In addition, HAM office management explained that some stakeholders do not always take full responsibility and accountability for their unverified and missing assets because there are no consequences for not adhering to the hardware asset management policies. When organizations do not take responsibility for their missing assets, those assets are then reassigned to the UNS organization for verification, placing additional burden on its limited resources.

To evaluate the benefit of having more resources to conduct asset verifications during the reconciliation period, we assessed the number of IRS personnel assigned from an Enterprise Operations workgroup and the Service Asset and Configuration Management group assisting in the asset verification at sites that were selected as part of our review. There did not appear to be a significant correlation between the number of personnel conducting asset verifications during the reconciliation period and the success rate in finding unverified and missing hardware assets. Figure 2 presents the results of our analysis.

Figure 2: Verification Rates and Resource Usage During the Fiscal Year 2017 Reconciliation Period by Location

Location	Number of Personnel Conducting the Asset Verification	Number of Unverified/Missing Assets at the Beginning of the Reconciliation Period	Number of Assets Verified During the Reconciliation Period	Percentage Verified
Ogden, Utah	5	2,317	1,834	79.2%
Kearneysville, West Virginia	4	2,017	821	40.7%
Memphis, Tennessee	4	2,037	531	26.1%
Washington, D.C.	4	1,104	104	9.4%
Lanham, Maryland	6	4,377	351	8.0%
Remaining Locations[14]	2 or fewer	1,128	111	9.8%

Source: Treasury Inspector General for Tax Administration's (TIGTA) analysis of the IRS's staffing and Unverified Asset Data and Summary Reports, dated June 30 and October 1, 2017, respectively.

[14] The remaining locations include Plantation, Florida; Chamblee, Georgia; New York, New York; and Farmers Branch, Texas.

Not all hardware assets were timely documented or controlled in the KISAM-AM module

The IRS did not always meet its Fiscal Year 2017 inventory objective to ensure that hardware asset information was timely documented or inventory records were properly created in the KISAM-AM module. The majority of hardware assets purchased by the IRS are systemically added in batches to the KISAM-AM module using vendor provided *Asset Management* reports prior to the assets' delivery. We selected a judgmental sample of 30 hardware assets from 10 *Asset Management* reports containing 4,408 assets from a total population of 529 *Asset Management* reports containing 23,853 assets that were systemically batch added to the KISAM-AM module during Fiscal Year 2017. We analyzed IRS-provided documentation and determined that 12 (40 percent) of the 30 selected hardware assets from five *Asset Management* reports were not updated in the KISAM-AM module within 10 workdays of receipt as required. The assets not timely added into the KISAM-AM module ranged from an additional one to 85 workdays late, averaging 38 workdays. The 12 assets included six servers, three laptop computers, two high-end multifunction printers, and a portable printer.

We also selected a judgmental sample of 102 verified and unverified assets during our site visits to determine whether the assets were properly controlled in the KISAM-AM module. Our analysis determined that 17 (16.7 percent) assets did not have a corresponding KISAM-AM module record and were not controlled in the system as required. The 17 assets included 12 servers on a pallet, one switch, one disk array, one network printer, and two additional servers.[15] The 12 servers on a pallet each have two 300-gigabyte drives and are located in the Memphis Enterprise Computing Center. There were no barcodes on any of these servers, and they were not adequately controlled in the KISAM-AM module as required. After we notified HAM office management of the situation, they explained that there were no data on the drives and that the servers were subsequently barcoded and the drives removed.

At the time of our reporting and after much further IRS research, HAM office management provided documentation that the 12 servers were actually controlled in the KISAM-AM module using the service tag numbers rather than the serial number, which is the practice for recording such assets from this vendor. Based upon the documentation provided, we determined that five of the servers were incorrectly reported as lost,[16] and the remaining seven servers appear to have been verified prior to the Fiscal Year 2017 inventory certification. The assignment statuses for all 12 servers have been updated in the KISAM-AM module and the servers placed into stock.

Further, HAM office management explained that the issue of hardware assets not being timely documented in the KISAM-AM module existed because the assets were received prior to the IRS receiving the vendor *Asset Management* reports, which were not timely provided by the vendors.

[15] The 12 servers had a total purchase price of $23,940, and the switch, disk array, network printer, and two additional servers had a total purchase price of $54,972.
[16] The five servers incorrectly reported as lost had a total purchase price of $9,975.

In addition, personnel from the IRS offices receiving the hardware assets failed to inform HAM office personnel to update the records in the KISAM-AM module when the assets were actually received. For the uncontrolled hardware assets not captured in the KISAM-AM module, HAM office management stated that the receipt and acceptance processes were not consistently followed in all receiving offices, and personnel who received the assets allowed them to be placed into operation without first ensuring that the assets were properly barcoded.

Key KISAM-AM module fields were not always complete, accurate, and reliable

IRS hardware asset inventory certifying officials did not always meet the Fiscal Year 2017 inventory objective to ensure that key KISAM-AM module fields were complete, accurate, and reliable. Of 232 hardware assets,[17] we reviewed 151 that were found or selected during our site visits[18] to determine whether four of the five key fields in the KISAM-AM module were accurate. We analyzed a total of 604[19] KISAM-AM module fields by comparing the key field information captured at each of our site visits to the KISAM-AM module data provided by the HAM office. Our analysis identified that one or more of the four key KISAM-AM module fields were inaccurate for 53 (35.1 percent) of the 151 hardware assets reviewed. Further, of the 604 KISAM-AM module fields analyzed, we identified 109 (18 percent) total errors. Figure 3 presents the number of assets with errors by key KISAM-AM module fields and IRS locations.

[17] Our sample included 130 hardware assets judgmentally selected from the KISAM-AM module and 102 hardware assets judgmentally selected from our site visits.
[18] The 151 hardware assets that were found included 49 assets of the 130 assets selected from the KISAM-AM module and 102 of the assets selected from our site visits. We did not include five additional assets that were accounted for because the key KISAM-AM module fields were provided for the user to verify.
[19] Four key KISAM-AM module fields multiplied by 151 hardware assets reviewed.

Figure 3: Number of Assets With Errors by Key KISAM-AM Module Fields and IRS Locations

IRS Location	Number of Assets Reviewed	Number of Assets With Errors	Number of Key Fields Reviewed	Number of Errors by Key KISAM-AM Module Field				
				Assignment Code Field	Barcode Field	Serial Number Field	Building Code Field	Total Number of Errors
Washington, D.C.[20]	14	2	56	2	1	1	1	5
Plantation, Florida	15	4	60	4	0	0	0	4
Chamblee, Georgia[21]	18	5	72	5	0	1	1	7
Lanham, Maryland[22]	15	8	60	7	4	2	3	16
New York, New York[23]	16	5	64	5	1	2	1	9
Memphis, Tennessee[24]	27	15	108	14	12	12	13	51
Farmers Branch, Texas	16	4	64	4	0	0	0	4
Ogden, Utah	14	2	56	0	0	2	0	2
Kearneysville, West Virginia[25]	16	8	64	8	1	1	1	11
Total	**151**	**53**	**604**	**49**	**19**	**21**	**20**	**109**

Source: TIGTA's analysis of the IRS's KISAM-AM module inventory based on our site visits.

We were unable to determine the accuracy of the remaining key KISAM-AM module field (either the User Name or Contact Name field) because the employees listed were not always present during our site visits and/or we were unable to definitively determine whether the asset was assigned to a single user or if the asset was shared. As a result, we measured the IRS's efforts to ensure that required information was entered into either of these two fields in the KISAM-AM module by analyzing the IRS-provided KISAM-AM module data extract of all Class A and Class B assets, dated October 1, 2017.

[20] One of the assets had errors in all four fields because the asset was not controlled in the KISAM-AM module.
[21] One of the assets had errors in the Assignment Code, Serial Number, and Building Code fields.
[22] Two of the assets had errors in the Assignment Code and Barcode fields. In addition, two other assets had errors in all four fields because the asset was not controlled in the KISAM-AM module.
[23] One of the assets had errors in the Assignment Code and Serial Number fields. In addition, another asset had errors in all four fields because the asset was not controlled in the KISAM-AM module.
[24] Twelve assets had errors in all four fields because the assets were not controlled in the KISAM-AM module.
[25] One of the assets had errors in all four fields because the asset was not controlled in the KISAM-AM module.

We found that both the User Name and Contact Name fields did not include required information for 6,493 (4.5 percent) of the 144,296 hardware assets that had an assignment status of in use.[26] Further analysis of the KISAM-AM module data extract determined that for in-use hardware assets assigned to a primary user, the User Name field did not include required information for 100 (0.13 percent) of the 75,409 assets.[27] For shared in-use hardware assets, as indicated by the Shared Indicator field in the KISAM-AM module, the Contact Name field did not include required information for 6,457 (9.4 percent) of the 68,887 assets. HAM office management stated they have a process in place and provided an example of a weekly report that they use to identify, monitor, and resolve blank User Name fields for in-use hardware assets assigned to a primary user. However, the IRS did not mention any process for resolving blank Contact Name fields of shared in-use hardware assets.

Both fields would provide valuable information to help certifying officials locate and verify their potentially missing assets. The IRS's own analysis determined that 40 to 50 percent of missing assets can be located by calling or e-mailing the person listed in the Contact Name field. In addition, we analyzed the KISAM-AM module data extract to determine whether the other four key fields (Assignment Code, Barcode, Serial Number, and Building Code) were populated with information as required. We found that all four key fields were properly populated and complete.

In addition, our analysis identified that the Location field in the KISAM-AM module was inaccurate for many of the 232 hardware assets in our judgmental sample selected for our site visits. While the Location field is not one of the five key KISAM-AM module fields requiring IRS personnel responsible for hardware assets to annually certify as accurate, we believe it is a data field important to the hardware asset management process. The Location field provides the specific site of an asset, *e.g.*, floor number, room number, cubicle number, that can be used to locate unverified and missing assets.

Using this information, we were able to find eight (six missing and two lost) of the 13 hardware assets previously reported as missing or lost in the locations listed in the KISAM-AM module record.[28] The eight assets included a server, a laptop computer, two desktop computers, a disk array, a switch, a network printer, and video equipment. For example, we found a desktop computer reported as missing that was unplugged and not connected to the IRS network in the IRS's Joint Operations Center at the Memphis Enterprise Computing Center as listed in the KISAM-AM module record. The Joint Operations Center room appears to be no longer in use.

[26] The User Name or Contact Name fields are required to be populated only for in-use assets and not for in-stock or missing assets.
[27] Of the 100 hardware assets not populated with the User Name, the IRS incorrectly populated the Contact Name field instead of the User Name field for 64 of the assets.
[28] The 13 hardware assets included 10 missing and three lost hardware assets. We did not include four additional missing assets that were accounted for because we contacted the person listed in the User Name or Contact Name fields and did not verify the Location field from the KISAM-AM module record.

In another example, we found a switch reported as missing that was plugged into the IRS network and in use in the computer room as listed in the KISAM-AM module record.

This information is more important for hardware assets that are shared assets. For hardware assets that are reported as missing or lost and assigned to a primary user, the IRS can contact the primary user who is more likely to have custody of and be able to account for the asset. However, our analysis identified that the Location field was inaccurate for 146 (62.9 percent) of the 232 selected hardware assets we reviewed. Further analysis of the KISAM-AM module data extract determined that the Location field was not populated for seven (7 percent) of the 100 KISAM-AM module records that were not populated with a user name for hardware assets assigned to a primary user and 903 (14 percent) of the 6,457 KISAM-AM module records that were not populated with a contact name for shared hardware assets, as indicated by the Share Indicator field in the KISAM-AM module.

HAM office management again cited that the labor-intensive certification process coupled with limited resources and no consequences for individuals not adhering to hardware asset management polices resulted in this condition. In addition, management said that the Contact Name field is not being populated because no one wants to be responsible for a shared asset that everyone uses. Realizing this concern, HAM office management has proposed assigning a responsible organization to each shared asset in the KISAM-AM module. However, due to competing organizational priorities, management has not yet initiated a coordinated effort to implement this plan. In the interim, some of the IRS organizations managing infrastructure equipment, *e.g.*, servers, have taken the initiative to add the responsible organization assignment group for shared assets in the KISAM-AM module.

Sufficient research was not conducted to locate missing hardware assets prior to reporting them as lost

The *Hardware User Guide* states that when a hardware asset has been categorized as missing, 10 research steps must be completed and documented in its KISAM-AM module record prior to surveying the asset and reporting it as lost to the IRS's Computer Security Incident Response Center and TIGTA's Office of Investigations. These 10 research steps include the following:

1. Record any contact and location information under the general tab in the KISAM-AM module record.
2. Check the Tivoli scan indicator and scan date. This will provide when the hardware asset was last scanned.
3. Check the history tab in the KISAM-AM module record for actions taken on the hardware asset.
4. Make a physical search for the hardware asset based on location and contact information.
5. Make a telephone call to the person listed in the User Name or Contact Name field.

6. Contact the last person who updated the record. This information can be found under the history tab in the KISAM-AM module record.
7. Use Microsoft Outlook to e-mail the contact and to determine the working status of the employee.
8. If a reply is not received within a reasonable amount of time, try contacting the manager of the employee.
9. Check Information Technology Service Management for other users to contact.
10. Ping the hardware asset by computer name or device identification if the asset is a desktop or laptop computer.

While the IRS has processes in place to survey lost or stolen hardware assets out of its inventory, certifying officials do not always ensure that the necessary steps are conducted to locate missing hardware assets prior to reporting them as lost. We judgmentally selected 40 hardware assets that the IRS had reported as lost in the KISAM-AM module during Fiscal Years 2014 through 2017 to determine if IRS actions were appropriate. We located three of the reported lost assets, two of which were found in the location listed in the KISAM-AM module record. These three assets included a server, a network printer, and an automated tape library.

For example, we found the server in the computer room as listed in the KISAM-AM module record, plugged in to the IRS network, and in use. The IRS explained that the server may have not been verified due to a bad network endpoint and the discovery scanning tool, *e.g.*, Tivoli, was not able to detect it. In another example, we found the network printer in the general work area as listed in the KISAM-AM module record and in use. For the remaining asset, we found the automated tape library in a storage room that was formerly used as the tape library, but the location in the KISAM-AM module record listed it in a computer room. HAM office management stated that they updated the KISAM-AM module records for all three assets as verified and in use for the network printer, in storage for the automated tape library, and scheduled to be excessed for the server. Certifying officials did not ensure that the personnel responsible for hardware asset verification followed established guidance to conduct sufficient research, as evidenced by TIGTA locating two of three assets in the locations in which they were listed in the KISAM-AM module.

In addition, we reviewed the 40 selected hardware assets to determine whether they were properly surveyed. We determined that HAM office personnel properly surveyed 37 of the 40 lost assets using Form 1933, *Report of Survey*, and appropriately reported them to the IRS's Computer Security Incident Response Center and to TIGTA's Office of Investigations.

Furthermore, the IRS continues to find hardware assets it had previously reported as lost. As a result of a prior audit,[29] TIGTA's Office of Investigations worked with the IRS to coordinate the reporting of large volumes of hardware assets that were being reported as an "administrative loss." The IRS believed that the hardware assets were lost due to a lack of properly completed documentation for the transfer and/or disposal of the assets rather than theft. The IRS also believed that the hardware assets were aged; many had not been inventoried for a number of years and had little to no current value. From this effort, the IRS reported 2,429 hardware assets as lost to TIGTA's Office of Investigations. From the time of its reporting, the IRS has found 95 of these assets and placed 85 of them back into operations or into stock. The IRS plans to retire and excess the remaining 10 hardware assets.

Managing and maintaining the integrity of the KISAM-AM module asset hardware inventory requires the complete and timely updating of asset records. Incomplete or inaccurate asset records hinder management's ability to make sound operating decisions and manage operations. In addition, failure to timely update asset inventory records impedes the IRS's ability to timely detect the loss, theft, or misuse of Government property. Lack of controls over hardware assets increases the potential risk of unauthorized access to taxpayer or other sensitive information. If unverified and missing hardware assets are allowed to remain in the KISAM-AM module, this could result in the IRS overstating its financial statements by reporting amounts for assets that are no longer in its possession. Conversely, hardware assets without a KISAM-AM module record, or incorrectly reported as missing, lost, or stolen that are still in the IRS's possession, could result in the IRS understating the value of its assets on its financial statements.

Based upon the results of our review, we determined that the IRS understated its financial statements by $221,339 for 24 of the 34 hardware assets in our sample previously reported as missing or lost that were subsequently found by TIGTA during this review after being written off of the IRS's financial statements or hardware assets that were not controlled in the KISAM-AM module and not included in the IRS's financial statements.[30] Furthermore, the IRS's Computer Security Incident Response Center and TIGTA's Office of Investigations resources are unnecessarily expended recording and tracking hardware assets erroneously reported as lost or stolen that are subsequently found still in the IRS's possession.

[29] TIGTA, Ref. No. 2014-20-021, *Used Information Technology Assets Are Being Properly Donated; However, Disposition Procedures Need to Be Improved* (Apr. 2014).

[30] The 24 hardware assets consist of 12 missing assets, two lost assets, and 10 assets not controlled in the KISAM-AM module. For the remaining 10 of the 34 hardware assets, seven uncontrolled servers were subsequently identified to have asset records in the KISAM-AM module and therefore did not affect the IRS's financial statements. Further, two missing and one lost hardware assets were excessed after being found and therefore did not affect the IRS's financial statements.

Recommendations

The Chief Information Officer should:

Recommendation 1**:** Review and update the existing *Hardware Asset Management Inventory Certification Plan* and reconciliation process to improve compliance, accountability, and participation of all asset inventory owners and stakeholders and to improve the accuracy of information of key KISAM-AM module fields during the annual certification process.

> ***Management's Response:*** The IRS agreed with this recommendation. The IRS will update the annual *Hardware Asset Management Inventory Certification Plan* and reconciliation process to improve asset inventory owner and stakeholder participation and compliance and to improve the accuracy of the key Hewlett Packard Asset Manager (KISAM-AM) data fields.
>
> ***Office of Audit Comment:*** Although the IRS agreed with this recommendation, the annual *Hardware Asset Management Inventory Certification Plan* and reconciliation process should also be updated to improve accountability. As stated in the report, some stakeholders did not always take full responsibility and accountability for their unverified and missing assets because there are no consequences for not adhering to hardware asset management policies.

Recommendation 2: Ensure that newly acquired assets are timely added into the KISAM-AM module by revising the current asset acquisition and receipt process to ensure the timely delivery of required vendor reporting and to improve accountability of personnel responsible for the receipt and acceptance process.

> ***Management's Response:*** The IRS agreed with this recommendation. The IRS will revise its hardware asset acquisition procedures to specify timely vendor requirements for providing Asset Management Reporting services. To improve accountability, the IRS will revise its procedures to integrate Hewlett Packard Service Manager (KISAM–Service Manager) in the asset receipt and acceptance process. Completion of this corrective action is contingent upon funding for implementing enhancements to Hewlett Packard Asset Manager (KISAM-AM) and Hewlett Packard Service Manager (KISAM–Service Manager).

Recommendation 3: Direct responsible personnel to research and update the KISAM-AM module records for all in-use assets to ensure that all identified blank User Name and/or Contact Name fields are populated accordingly.

> ***Management's Response:*** The IRS agreed with this recommendation. In addition to the existing process to research and update Hewlett Packard Asset Manager (KISAM-AM) to populate null user name information for nonshared, in-use assets, the IRS will develop and implement a repeatable process to update Hewlett Packard Asset Manager (KISAM-AM) with responsible ownership information for in-use information

technology hardware assets. Hewlett Packard Asset Manager (KISAM-AM) and Hewlett Packard Service Manager (KISAM–Service Manager) enhancements are contingent upon funding availability.

Recommendation 4: Improve the accuracy of the Location field in the KISAM-AM module for shared assets by capturing the specificity of the location for future hardware asset inventory certifications and transactions.

Management's Response: The IRS agreed with this recommendation. The IRS will develop and implement a repeatable process to capture the Hewlett Packard Asset Manager (KISAM-AM) location field information for shared, in-use information technology hardware assets during reportable inventory transactions and events. Hewlett Packard Asset Manager (KISAM-AM) and Hewlett Packard Service Manager (KISAM–Service Manager) enhancements are contingent upon funding availability.

Office of Audit Comment: Although the IRS agreed with this recommendation, the plan to develop and implement a repeatable process to capture the Location field information for shared hardware assets should also include both in-use and in-storage assets. The Location field information provides the location where the hardware asset was last verified and is important in the hardware asset management process as demonstrated by the audit team using the information to locate eight of 13 hardware assets previously reported as missing or lost.

Recommendation 5: Direct certifying officials to ensure that sufficient research is properly conducted to locate missing hardware assets prior to reporting them as lost.

Management's Response: The IRS agreed with this recommendation. The IRS will update its procedures to implement a managerial review and approval process to verify that sufficient research is conducted to locate missing assets prior to processing them as lost.

Hardware Asset Management Guidance Needs Improvement

The Government Accountability Office's *Standards for Internal Control in the Federal Government*[31] provides that management define objectives in specific terms so that they are understood at all levels of the entity. This involves clearly defining what is to be achieved, who is to achieve it, how it will be achieved, and the time frames for achievement. Management defines objectives in alignment with the organization's mission, strategic plan, and performance goals.

[31] Government Accountability Office, GAO-14-704G, *Standards for Internal Control in the Federal Government* (September 2014).

In addition, the IRS's *Computer Security Incident Reporting Procedures*, version 1.3, dated November 2015, requires that all identified cybersecurity incidents, *e.g.*, lost hardware assets, shall be reported directly to the IRS's Computer Security Incident Response Center. In turn, Department of the Treasury Chief Information Officer Memorandum 15-05, Update to Treasury Directive Publication 85-01, *Treasury Information Technology Security Program, Appendix A: Minimum Standard Parameters and Treasury Controls*, requires that bureaus shall report confirmed cybersecurity incidents to the Government Security Operations Center through the Department of the Treasury's Computer Security Incident Response Center within one business day.

The IRS's Asset Management Policy Directive 064, *Asset Management Policy to Identify Uncertified Class A and Class B Assets as Missing Assets in KISAM Asset Manager*, dated September 13, 2016, and the *Hardware User Guide* provide additional criteria that require Class A and Class B assets not verified and certified in accordance with the annual *Hardware Asset Management Inventory Certification Plan* for greater than two inventory cycles be categorized as missing in the KISAM-AM module. In addition, as previously discussed, the IRS has specific guidance on research steps to be conducted for locating missing assets before the asset is surveyed and reported as lost to the appropriate organizations. While this guidance provides specific research steps, it does not specify the time period by which these research steps need to be completed.

The IRS has made strides in reducing its inventory of missing, lost, and stolen hardware assets. In October 2016, the IRS identified 10,149 Class A and Class B unverified assets that met the missing criteria established in Asset Management Policy Directive 064. The IRS has worked to locate these missing hardware assets or took the necessary steps to survey them out of its inventory as excessed or lost. By March 14, 2018, the IRS's efforts reduced the total number of missing hardware assets by 3,597,[32] of which 2,317 assets were found and placed back into operations or into stock, and the remaining 1,280 assets were surveyed by either excessing or reporting them as lost. Our analysis further determined that 509 of the hardware assets reported as lost may potentially contain Personally Identifiable Information.[33]

However, we are concerned with the length of time from when the remaining missing hardware assets were last verified and continued to stay in the KISAM-AM module inventory. The length of time for missing hardware assets to be reported as lost from when they were last verified ranged from 1,262 to 6,070 calendar days, averaging 1,813 calendar days or nearly five years. HAM office management stated that a time period to report a hardware asset as lost has not been

[32] The HAM office was unable to provide the status for one of the 10,149 hardware assets because it required additional in-depth research. In addition, the IRS's efforts located another six hardware assets, but the assets subsequently went missing again. The six hardware assets are not reflected in the IRS's effort to reduce the number of missing assets by 3,597.

[33] Hardware assets that may potentially contain Personally Identifiable Information include: desktop and laptop computers; servers; micro–personal digital assistants; and disk arrays.

specified in its guidance because at the time of Asset Management Policy Directive 064 implementation, it was difficult to gauge the time frame or level of effort necessary to conduct appropriate research for more than 10,000 missing assets, in addition to considering resource constraints and other competing priorities. Leaving hardware assets in missing status for such long periods of time hinders the IRS's Computer Security Incident Response Center from timely reporting the loss to the Government Security Operations Center through the Department of the Treasury's Computer Security Incident Response Center, as well as impedes TIGTA's Office of Investigations' ability to appropriately investigate the incident if a potential theft is involved.

Recommendations

The Chief Information Officer should:

Recommendation 6**:** Identify high-risk hardware asset categories that may potentially contain Personally Identifiable Information, update guidance to further define that high-risk assets not verified for one inventory cycle be immediately categorized as missing in the KISAM-AM module, and specify a time frame to complete the 10 research steps for locating missing assets.

> ***Management's Response:*** The IRS agreed with this recommendation. The IRS will update its procedures to identify and define high-risk asset categories and specify a time frame for processing the unverified high-risk asset categories as missing and for conducting research to process the assets as lost.
>
> ***Office of Audit Comment:*** Although the IRS agreed with this recommendation, its corrective action does not specifically address the recommendation that high-risk hardware assets that may potentially contain Personally Identifiable Information not verified for one inventory cycle be immediately categorized as missing in the KISAM-AM module. As stated in the report, we are concerned with the length of time from when missing hardware assets were last verified and continued to stay in the KISAM-AM module inventory. Delays in categorizing high-risk hardware assets not verified within one inventory cycle as missing prevents the IRS from taking the necessary steps to locate or to make a timely determination that these missing assets are lost.

Recommendation 7: Direct responsible personnel to prioritize locating high-risk missing assets that may potentially contain Personally Identifiable Information when conducting the 10 research steps and immediately report assets determined as lost to the IRS's Computer Security Incident Response Center and TIGTA's Office of Investigations.

> ***Management's Response:*** The IRS agreed with this recommendation. The IRS will update its procedures to prioritize locating high-risk missing assets and immediately report assets determined as lost to the IRS's Computer Security Incident Response Center and TIGTA's Office of Investigations.

Appendix I

Detailed Objective, Scope, and Methodology

The overall objective of this review was to evaluate the IRS's management controls over its information technology hardware asset inventory.[1] To accomplish our objective, we:

I. Assessed whether the IRS asset management process was sufficient to ensure that a KISAM-AM module data record was timely created and recorded for newly purchased information technology hardware assets.

   A. Selected a judgmental[2] sample of 30 hardware assets from 10 *Asset Management* reports containing 4,408 assets from a total population of 529 *Asset Management* reports containing 23,853 assets that were systemically batch added to the KISAM-AM module during Fiscal Year 2017 and determined whether they were updated in the KISAM-AM module within 10 workdays of receipt.

   B. Evaluated the reliability of the electronic KISAM-AM module reports data received from the IRS to help ensure that the data were reasonably complete and accurate. This was accomplished by verifying the criteria that the IRS used to create the reports, verifying that all fields requested were received, and verifying that the record counts equaled to what was expected.

      Determined that the data were sufficiently reliable for purposes of this audit. In addition, we selected five judgmental samples, which are detailed in the audit tests within Appendix I. We used judgmental sampling because we determined that statistical sampling techniques would have been cost prohibitive and we did not plan to project our results to the entire population.

II. Determined whether the IRS effectively conducted its annual hardware asset management inventory certification in accordance with established policies, procedures, and guidelines.

   A. Verified the accuracy of the hardware asset management inventory certification reports of its Class A and Class B assets.

      1. Identified the percentage of verified hardware assets as calculated by the IRS in its *Fiscal Year 2017 Unverified Asset Data and Summary Report*, as of October 1, 2017.

      2. Obtained from the IRS a complete KISAM-AM module data extract of Class A and B assets as of October 1, 2017, and calculated the percentage of verified hardware

[1] See Appendix VI for a glossary of terms.
[2] A judgmental sample is a nonprobability sample, the results of which cannot be used to project to the population.

assets. We compared our calculated percentage to the IRS's calculated percentage and determined whether the IRS computation was correct.

B. Assessed the completeness and accuracy of the five key KISAM-AM module fields, *e.g.*, Assignment Code, Barcode, Serial Number, Building Code, User Name or Contact Name, as part of the hardware asset certification process.

   1. Analyzed the complete KISAM-AM module data extract obtained in Step II.A.2 and determined whether the key KISAM-AM module fields were complete as required.

   2. Judgmentally selected a sample of 102 hardware assets during our site visits and determined whether the assets were properly controlled in the KISAM-AM module, determined the accuracy of four of the five key fields in each asset's KISAM-AM module record, and systemically measured IRS compliance with populating the remaining key field, User Name or Contact Name, by analyzing the extract of the KISAM-AM module obtained in Step II.A.2.

   3. From the complete KISAM-AM module data extract obtained in Step II.A.2, judgmentally selected a sample of 38 out of 146 Class A hardware assets that were self-certified during Fiscal Year 2017 from eight IRS locations[3] and determined whether users certified the correct asset in their possession.

C. Determined whether the IRS took appropriate actions to resolve outstanding anomalies and data discrepancies.

   1. Determined whether certifying officials took the necessary steps to locate unverified and missing hardware assets.

      a. Determined whether the HAM office distributed the Fiscal Year 2017 hardware asset *Reconciliation Plans* and *Reconciliation Plan Letters* (that summarize key outstanding anomalies and data discrepancies) to all asset owners and offices responsible for the annual inventory verification.

      b. Determined whether the Fiscal Year 2017 *Certification Letters* were submitted by each certifying official acknowledging the number of anomalous records detailed in their respective hardware asset *Reconciliation Plans*, including their commitments to address the anomalies and discrepancies by September 30, 2017.

      c. Assessed the effectiveness of the certifying official efforts in resolving anomalies and discrepancies in the hardware asset records by comparing the number of

[3] We did not include Plantation, Florida, because two of only three Class A hardware assets that were self-certified resulted from the HAM office management conducting a demonstration of the self-certification process to the audit team.

unverified and missing assets between the *Unverified Assets Summary and Data Report*, dated June 30 and October 1, 2017.

d. Analyzed the complete KISAM-AM module data extract obtained in Step II.A.2 to identify in-stock and in-use hardware assets that have not been verified and certified for greater than two inventory cycles.

e. From the complete KISAM-AM module data extract obtained in Step II.A.2, judgmentally selected a sample of 130 (49 of 5,458 unverified, 41 of 2,963 missing, and 40 of 863 lost) of 9,284 Class A hardware assets from nine IRS locations[4] and attempted to find or account for the assets and determine the accuracy of four of the five key fields in each asset's KISAM-AM module record.

2. Determined whether certifying officials took the necessary steps to locate missing information technology hardware assets and properly documented the loss.

a. Obtained from the IRS a KISAM-AM module data extract as of October 1, 2017, of lost and stolen Class A and B assets with a disposal date from May 1, 2014, and judgmentally selected a sample of 40 out of 863 lost Class A hardware assets from eight IRS locations.[5] We determined whether they were appropriately reported to the IRS's Computer Security Incident Response Center and to TIGTA's Office of Investigations.

b. For the selected sample, we determined whether the IRS accurately completed the Form 1933, *Report of Survey*.

Internal controls methodology

Internal controls relate to management's plans, methods, and procedures used to meet their mission, goals, and objectives. Internal controls include the processes and procedures for planning, organizing, directing, and controlling program operations. They include the systems for measuring, reporting, and monitoring program performance. We determined that the following internal controls were relevant to our audit objective: Internal Revenue Manual 2.149, *Information Technology Asset Management*;[6] the *Asset Management – Hardware User Guide*; the *Fiscal Year 2017 Hardware Asset Management Inventory Certification Plan*; and the Government Accountability Office's *Standards for Internal Control in the Federal Government* as well as policies and procedures related to information technology hardware asset inventory management. We evaluated these controls by interviewing HAM office management concerning

[4] We did not include Plantation, Florida, for our judgmental sample of lost Class A hardware assets because we conducted this site visit as an initial test run prior to obtaining the KISAM-AM module data extract of lost and stolen hardware assets obtained in Step II.C.2.a.
[5] We did not include Plantation, Florida, because we conducted this site visit as an initial test run prior to obtaining the KISAM-AM module data extract of lost and stolen Class A and B hardware assets.
[6] Dated September 23, 2015.

the scope and purpose of the information technology hardware inventory management program. In addition, we reviewed program-related policies and procedures to gain a better understanding of the controls over the hardware asset inventory and the annual certification process.

Appendix II

Major Contributors to This Report

Danny R. Verneuille, Assistant Inspector General for Audit (Security and Information Technology Services)
Bryce Kisler, Director
Louis Lee, Audit Manager
David Allen, Lead Auditor
Jason Rosenberg, Information Technology Specialist

Appendix III

Report Distribution List

Deputy Commissioner for Operations Support
Deputy Commissioner for Services and Enforcement
Chief Information Officer
Deputy Chief Information Officer for Operations
Associate Chief Information Officer, Enterprise Operations
Associate Chief Information Officer, User and Network Services
Director, Office of Audit Coordination

Appendix IV

Outcome Measures

This appendix presents detailed information on the measurable impact that our recommended corrective actions will have on tax administration. These benefits will be incorporated into our Semiannual Report to Congress.

Type and Value of Outcome Measure:

- Reliability of Information – Potential; information in the KISAM-AM[1] module records was not always complete or accurate for 6,649 unique hardware assets (see page 4).

Methodology Used to Measure the Reported Benefit:

Our analysis identified that one or more of the four key KISAM-AM module fields were inaccurate for 53 of the 151 hardware assets reviewed from our judgmental sample[2] of 232 hardware assets. We also measured the IRS's compliance with ensuring that required information was entered into either the User Name or Contact Name field by analyzing an extract of the KISAM-AM module as of October 1, 2017. We found that both fields did not include required information for 6,493 of the 144,296 hardware assets that had an assignment status of in use. Although the Location field is not one of the five key KISAM-AM module fields requiring IRS personnel responsible for hardware assets to annually certify as accurate, we believe it is an important data field to the hardware asset management process.

Our analysis identified that the Location field was inaccurate for 146 of the 232 hardware assets we reviewed. We calculated the total number of hardware assets with inaccuracies as: 53 hardware assets with inaccuracies in one or more of the four key KISAM-AM module fields + 6,493 hardware assets with missing information in the User Name and Contact Name KISAM-AM module fields[3] + 146 hardware assets with missing information in the Location KISAM-AM module field – 43 duplicate hardware assets that were in more than one of the previous categories = 6,649 hardware assets with inaccurate information in the KISAM-AM module.

[1] See Appendix VI for a glossary of terms.
[2] A judgmental sample is a nonprobability sample, the results of which cannot be used to project to the population.
[3] The User Name field lists the employee name and standard employee identifier of the primary user of the assigned hardware asset. Shared hardware assets will not have an entry in the User Name field but rather will have the same employee information in the Contact Name field. Populating the Contact Name field for shared assets is mandatory.

Type and Value of Outcome Measure:

- Protection of Resources – Potential; $221,339 for 24 hardware assets previously reported as missing or lost that were subsequently found after being written off of the IRS's financial statements or hardware assets that were not controlled in the KISAM-AM module and not included in the IRS's financial statements[4] (see page 4).

Methodology Used to Measure the Reported Benefit:

We associated the barcodes of the hardware assets that had previously been reported as missing or lost but subsequently found by TIGTA to the barcodes in the KISAM-AM module data extract, dated October 1, 2017, to identify the purchase price. For the hardware assets not properly controlled in the KISAM-AM module and, therefore, not listed in the data extract, we contacted the HAM office to obtain the purchase price. We located 14 missing hardware assets[5] with a combined purchase price of $95,149 and three lost hardware assets[6] with a combined purchase price of $61,243. In addition, we identified five of the 12 servers on a pallet not controlled in the KISAM-AM module that were incorrectly reported as lost had a combined purchase price of $9,975 and five other hardware assets, *e.g.*, one switch, one disk array, one network printer, and two additional servers, not controlled in the KISAM-AM module had a combined purchase price of $54,972. The total purchase price of the missing or lost hardware assets was $221,339.

[4] The 24 hardware assets consist of 12 missing assets, two lost assets, and 10 assets not controlled in the KISAM-AM module.
[5] Two of the missing hardware assets were excessed after being found, not affecting the financial statements, and therefore were not included in the combined purchase price.
[6] One of the lost hardware assets was excessed after being found, not affecting the financial statements, and therefore was not included in the combined purchase price.

Appendix V

Results of the Fiscal Year 2017 Hardware Asset Inventory Certification

Hardware Type	Total Assets	Verified Assets	Unverified Assets	Percentage Verified
Adaptive Equipment[1]	1,736	802	934	46.2%
Copier Multifunction Device	4,422	4,266	156	96.5%
Desktop Computer	67,170	63,081	4,089	93.9%
Disk Array	2,239	1,870	369	83.5%
High-End Scanner	2,059	1,527	532	74.2%
Laptop Computer	116,594	110,786	5,808	95.0%
Micro–Personal Digital Assistant	16,423	15,004	1,419	91.4%
Network Printer	13,599	8,786	4,813	64.6%
Router	1,574	1,320	254	83.9%
Server	8,072	7,004	1,068	86.8%
Switch	7,115	6,026	1,089	84.7%
32 Other Categories[2]	9,517	6,475	3,042	68.0%
Total	**250,520**	**226,947**	**23,573**	**90.6%**

Source: The IRS's Fiscal Year 2017 Unverified Asset Data and Summary Report, dated October 1, 2017.

[1] See Appendix VI for a glossary of terms.
[2] Information technology hardware assets in this category include encryption devices, video equipment, gateways, high-end multifunctional printers, *etc*.

Appendix VI

Glossary of Terms

Term	Definition
Adaptive Equipment	Encompasses the electronics and information systems used by IRS employees and customers with disabilities, *e.g.*, video magnifier, text typewriter, and braille.
Asset Manager	KISAM module that tracks information technology and non–information technology equipment used throughout the IRS.
Assignment Code	There are five assignments in the KISAM-AM module that identify the status of an asset at any given time: In Use, In Stock, Missing, Retired, and Awaiting Receipt.
Automated Tape Library	A peripheral device in which a large number of cartridges or reels of magnetic tape are stored in cells in a storage matrix. Any chosen cartridge can be transferred mechanically to a tape transport where it can be accessed by the host system, and then returned to the same or another cell.
Barcode	A unique series of alphanumeric characters for each asset record in the KISAM-AM module that are associated with a unique series of varying width lines. The unique series of varying width lines are printed on a tag and affixed to the associated asset for identification by an optical scanner.
Barcode Scanning	A valid method of asset inventory verification using an optical scanning tool to scan the asset's unique barcode.
Batch Add	Allows assets with a shared and common identity to be batched, managed, and added together to the KISAM-AM module.
Building Code	Identifies the building location of an asset.
Certifying Official	The official held accountable and responsible for verifying and certifying assets under his/her respective control and stewardship. The official is responsible for ensuring that proper action is taken to research, resolve, and correct anomalous asset records in the KISAM-AM module.

Term	Definition
Computer Security Incident Response Center	A group of individuals usually consisting of security analysts organized to develop, recommend, and coordinate immediate mitigation actions for containment, eradication, and recovery resulting from computer security incidents.
Desktop Computer	A computer that is designed to stay in a single location, cannot be powered from an internal battery, and therefore must remain connected to a wall outlet.
Digital Assistant	A portable device that functions as a personal information manager and is used for Web browsing, office applications, watching videos, viewing photos, or as a mobile phone.
Disk Array	A hardware element that contains a large group of hard disk drives. It may contain several disk drive trays and has an architecture that improves speed and increases data protection.
Drive	A computer component used to store data and may be a static storage device or may use removable media.
Firewall	A system designed to prevent unauthorized access to or from a private network.
Fiscal Year	Any yearly accounting period, regardless of its relationship to a calendar year. The Federal Government's fiscal year begins October 1 and ends on September 30.
Gateway	Serves as the entry and exit point of a network; all data routed inward or outward must first pass through and communicate with the gateway in order to use routing paths. Generally, a router is configured to work as a gateway device in computer networks.
Government Security Operations Center	Serves as the Department of the Treasury's computer security incident response capability and is responsible for monitoring network traffic.
Information Technology Hardware Asset Inventory	Equipment or property that are part of the information technology infrastructure in use, in storage, or awaiting disposal.
Information Technology Service Management	Responsible for monitoring the interfaces to the KISAM-AM module that includes the daily import of requisition, procurement, and award information.

Term	Definition
Internal Revenue Manual	The IRS's primary source of instructions to its employees related to the administration and operation of the IRS. The manual contains the directions employees need to carry out their operational responsibilities.
Inventory	To take stock of assets. A detailed list of assets.
Knowledge Incident/Problem Service Asset Management	A system that maintains the complete inventory of information technology and non–information technology organizational assets, and computer hardware and software. It is also the reporting tool for problem management with all IRS-developed applications and shares information with the IRS Enterprise Service Desk.
Laptop Computer	A portable computer that can be carried and used in different environments, and has a battery that allows it to operate without being plugged into a power outlet.
Location Field	Identifies the location, *e.g.*, floor number, room number, cubicle number, of an asset.
Mainframe Computer	A term used to distinguish high-end commercial machines, with large-scale computer system architectures, from less powerful units.
Multifunction Printer	A printer designed for multiple purposes beyond printing, such as faxing and copying.
Network	Information system(s) implemented with a collection of interconnected components. Such components may include routers, hubs, cabling, telecommunications controllers, key distribution centers, and technical control devices.
Network Endpoint	A port on an asset that allows a discovery tool to electronically locate and verify an asset.
Personally Identifiable Information	Information that, either alone or in combination with other information, can be used to uniquely identify an individual. Some examples of Personally Identifiable Information are: name, Social Security Number, date of birth, place of birth, address, and biometric record.
Physical Inventory	An inventory conducted as necessary to verify the existence of the asset recorded in the KISAM-AM module and certify the accuracy of certain information maintained on the asset.
Ping	A command run from the operating system prompt used to determine if an asset is connected to the network.

Term	Definition
Portable Printer	A small and lightweight printer designed for portability. It performs at low volume and speed output, and often runs on an alternate battery supply.
Radio Frequency Identification Technology	The wireless non-contact use of radio frequency fields to transfer data. It is used to automatically identify and track tags attached to objects.
Record	An asset record in the KISAM-AM module that includes fields such as Assignment Code, Barcode, Serial Number, Building Code, User Name, Contact Name, Purchase Price, Inventory Date, Model, Manufacturer, and other information used to identify the asset.
Requirement	A formalization of a need and the statement of a capability or condition that a system, subsystem, or system component must have or meet to satisfy a contract, standard, or specification.
Router	A hardware device that routes data from a local area network to another network connection.
Serial Number	A unique combination of alpha characters and numeric digits affixed to an asset.
Server	A physical computer, *e.g.*, a computer hardware system, dedicated to running one or more services (as a host) to serve the needs of the users of other computers on the network. Depending on the computing service that it offers, it could be a database server, file server, mail server, print server, web server, gaming server, or some other kind of server.
Service Manager	An IRS application for reporting and managing problems with all applications developed by the IRS.
Smartphone	A mobile telephone with highly advanced features that typically has a high-resolution touch screen display, wireless connectivity, Web browsing capabilities, and the ability to accept sophisticated applications.
Stick Personal Computer	A type of device that puts all the performance of a personal computer into a small drive that looks similar to a slightly larger version of standard flash drives and universal serial bus storage drives.
Switch	A small hardware device that joins multiple computers together with one local area network.

Appendix VII

Management's Response to the Draft Report

CHIEF INFORMATION OFFICER

DEPARTMENT OF THE TREASURY
INTERNAL REVENUE SERVICE
WASHINGTON, D.C. 20224

JUN 18 2018

MEMORANDUM FOR DEPUTY INSPECTOR GENERAL FOR AUDIT

FROM: S. Gina Garza
Chief Information Officer

SUBJECT: Draft Audit Report – Management Controls Should Be Strengthened to Improve Hardware Asset Inventory Reliability (Audit # 201720030) (e-trak # 2018-03320)

Thank you for the opportunity to comment on the draft audit report. We appreciate the collaboration between the audit team and the Internal Revenue Service (IRS) personnel in identifying opportunities for improvement. Also, we appreciate TIGTA's acknowledgement of the IRS's ongoing efforts to strengthen asset and inventory controls.

The IRS manages a comprehensive and robust hardware asset management program and is committed to continually improving hardware asset inventory reliability. Further, the IRS is already taking steps to address TIGTA's recommendations to improve the Annual Certification and Reconciliation process, and to strengthen management controls of hardware asset inventory. We strive to reduce the dependence on manual processes and leverage opportunities to insert automation into the hardware and asset inventory processes.

Should you have any questions, please contact me at (202) 317-5000 or a member of your staff may contact Carmelita White, Senior Manager, Program Oversight at (240) 613-2191.

Attachment

Attachment

Draft Audit Report – Management Controls Should Be Strengthened to Improve Hardware Asset Inventory Reliability (Audit # 201720030) (e-trak # 2018-03320)

RECOMMENDATION 1: Review and update the existing Hardware Asset Management Inventory Certification Plan and reconciliation process to improve compliance, accountability, and participation of all asset inventory owners and stakeholders, and to improve the accuracy of information of key KISAM-AM fields during the annual certification process.

CORRECTIVE ACTION 1: We agree with this recommendation. We will update the annual Hardware Asset Management Inventory Certification Plan and Reconciliation Process to improve asset inventory owner and stakeholder participation and compliance, and to improve the accuracy of the key HP Asset Manager – Knowledge Incident/Problem Service Asset Management–Asset Manager (KISAM-AM) data fields.

IMPLEMENTATION DATE: October 15, 2019

RESPONSIBLE ORGANIZATION: Associate Chief Information Officer, User and Network Services

CORRECTIVE ACTION MONITORING PLAN: We enter accepted Corrective Actions into the Joint Audit Management Enterprise System (JAMES) and monitor them monthly until completion.

RECOMMENDATION 2: Ensure that newly acquired assets are timely added into the KISAM-AM module by revising the current asset acquisition and receipt process to ensure the timely delivery of required vendor reporting, and to improve accountability of personnel responsible for the receipt and acceptance process.

CORRECTIVE ACTION 2: We agree with this recommendation. We will revise our hardware asset acquisition procedures to specify timely vendor requirements for providing Asset Management Reporting services. To improve accountability, we will revise our procedures to integrate HP Service Manager – Knowledge Incident/Problem Service Asset Management–Service Manager (KISAM-SM) in the asset receipt and acceptance process. Completion of this corrective action is contingent upon funding for implementing enhancements to HP Asset Manager (KISAM-AM) and HP Service Manager (KISAM-SM).

IMPLEMENTATION DATE: April 15, 2019

RESPONSIBLE ORGANIZATION: Associate Chief Information Officer, User and Network Services

CORRECTIVE ACTION MONITORING PLAN: We enter accepted Corrective Actions into the Joint Audit Management Enterprise System (JAMES) and monitor them monthly until completion.

Attachment

Draft Audit Report – Management Controls Should Be Strengthened to Improve Hardware Asset Inventory Reliability (Audit # 201720030) (e-trak # 2018-03320)

RECOMMENDATION 3: Direct responsible personnel to research and update the KISAM-AM records for all in-use assets to ensure that all identified blank User Name and/or Contact Name fields are populated accordingly.

CORRECTIVE ACTION 3: We agree with this recommendation. In addition to the existing process to research and update HP Asset Manager (KISAM-AM) to populate null user name information for non-shared, in-use assets, we will develop and implement a repeatable process to update HP Asset Manager (KISAM-AM) with responsible ownership information for in-use IT hardware assets. HP Asset Manager (KISAM-AM) and HP Service Manager (KISAM-SM) enhancements are contingent upon funding availability.

IMPLEMENTATION DATE: February 15, 2020

RESPONSIBLE ORGANIZATION: Associate Chief Information Officer, User and Network Services

CORRECTIVE ACTION MONITORING PLAN: We enter accepted Corrective Actions into the Joint Audit Management Enterprise System (JAMES) and monitor them monthly until completion.

RECOMMENDATION 4: Improve the accuracy of the Location field in the KISAM-AM module for shared assets by capturing the specificity of the location for future hardware asset inventory certifications and transactions.

CORRECTIVE ACTION 4: We agree with this recommendation. We will develop and implement a repeatable process to capture the HP Asset Manager (KISAM-AM) location field information for shared, in-use IT hardware assets during reportable inventory transactions and events. HP Asset Manager (KISAM-AM) and HP Service Manager (KISAM-SM) enhancements are contingent upon funding availability.

IMPLEMENTATION DATE: February 15, 2020

RESPONSIBLE ORGANIZATION: Associate Chief Information Officer, User and Network Services

CORRECTIVE ACTION MONITORING PLAN: We enter accepted Corrective Actions into the Joint Audit Management Enterprise System (JAMES) and monitor them monthly until completion.

Attachment
Draft Audit Report – Management Controls Should Be Strengthened to Improve Hardware Asset Inventory Reliability (Audit # 201720030) (e-trak # 2018-03320)

RECOMMENDATION 5: Direct certifying officials to ensure that sufficient research is properly conducted to locate missing hardware assets prior to reporting them as lost.

CORRECTIVE ACTION 5: We agree with this recommendation. We will update our procedures to implement a managerial review and approval process to verify that sufficient research is conducted to locate missing assets prior to processing them as lost.

IMPLEMENTATION DATE: June 15, 2019

RESPONSIBLE ORGANIZATION: Associate Chief Information Officer, User and Network Services

CORRECTIVE ACTION MONITORING PLAN: We enter accepted Corrective Actions into the Joint Audit Management Enterprise System (JAMES) and monitor them monthly until completion.

RECOMMENDATION 6: Identify high risk hardware asset categories that may potentially contain Personally Identifiable Information, and update guidance to further define that high-risk assets not verified for one inventory cycle be immediately categorized as missing in the KISAM-AM module, and specify a time frame to complete the 10 research steps for locating missing assets.

CORRECTIVE ACTION 6: We agree with this recommendation. We will update our procedures to identify and define high-risk asset categories and specify a time frame for processing the unverified high-risk asset categories as missing, and for conducting research to process the assets as lost.

IMPLEMENTATION DATE: February 15, 2020

RESPONSIBLE ORGANIZATION: Associate Chief Information Officer, User and Network Services

CORRECTIVE ACTION MONITORING PLAN: We enter accepted Corrective Actions into the Joint Audit Management Enterprise System (JAMES) and monitor them monthly until completion.

Attachment

Draft Audit Report – Management Controls Should Be Strengthened to Improve Hardware Asset Inventory Reliability (Audit # 201720030) (e-trak # 2018-03320)

RECOMMENDATION 7: Direct responsible personnel to prioritize locating high-risk missing assets that may potentially contain Personally Identifiable Information when conducting the 10 research steps and immediately report assets determined as lost to the IRS's Computer Security Incident Response Center and TIGTA's Office of Investigations.

CORRECTIVE ACTION 7: We agree with this recommendation. We will update our procedures to prioritize locating high-risk missing assets, and immediately report assets determined as lost to the IRS's Computer Security Incident Response Center and TIGTA's Office of Investigations.

IMPLEMENTATION DATE: February 15, 2020

RESPONSIBLE ORGANIZATION: Associate Chief Information Officer, User and Network Services

CORRECTIVE ACTION MONITORING PLAN: We enter accepted Corrective Actions into the Joint Audit Management Enterprise System (JAMES) and monitor them monthly until completion.