Weaknesses in Asset Management Controls Leave Information Technology Assets Vulnerable to Loss

September 16, 2013

Reference Number: 2013-20-089

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

WEAKNESSES IN ASSET MANAGEMENT CONTROLS LEAVE INFORMATION TECHNOLOGY ASSETS VULNERABLE TO LOSS

Highlights

Final Report issued on September 16, 2013

Highlights of Reference Number: 2013-20-089 to the Internal Revenue Service Chief Technology Officer.

IMPACT ON TAXPAYERS

The IRS Information Technology organization controls more than 306,000 information technology assets worth almost $720 million using the Knowledge, Incident/Problem, Service Asset Management (KISAM) system. Our review determined that weaknesses in controls over asset management create an environment in which information technology assets are vulnerable to loss. The risk of loss, theft, or the inadvertent release of sensitive information can decrease the public's confidence in the IRS's ability to monitor and use its resources effectively.

WHY TIGTA DID THE AUDIT

This audit was included in our Fiscal Year 2012 Annual Audit Plan and addresses the major management challenge of Modernization. The overall objectives were to determine whether system user permissions were appropriate to ensure the safeguarding of the information technology asset inventory and to review the effectiveness of the system in maintaining an accurate and complete information technology asset inventory.

WHAT TIGTA FOUND

TIGTA found that information technology asset data successfully migrated from the legacy inventory system to the KISAM–Asset Manager. However, the audit log used to capture events was not being reviewed to ensure that only appropriate accesses were made. In addition, information technology asset data within the KISAM–Asset Manager are inaccurate and incomplete because the IRS is not following its procedures to ensure that all assets are accurately recorded and timely updated in the KISAM–Asset Manager.

TIGTA also found that ineffective inventory controls created an environment where information technology assets are vulnerable to loss. TIGTA selected 146 information technology assets to physically verify and could not locate and verify or find proper supporting documentation for 34 information technology assets worth more than $948,000. In addition, IRS offices improperly completed the annual inventory reconciliation process.

WHAT TIGTA RECOMMENDED

To improve the controls over information technology assets, TIGTA recommended that the Chief Technology Officer ensure that the inventory records are updated to correct the deficiencies identified in our review; the reconciliation process is effectively completed and offices provide supporting documentation for quality review; and dollar threshold criteria are included in the Asset Management Inventory Certification Plan for certifying information technology assets with a high-dollar value that affect financial statement reporting. TIGTA also made several recommendations that will help the IRS Information Technology organization ensure that the data captured in its inventory management system are complete and accurate and that its assets are adequately safeguarded against theft or loss.

In their response to the report, IRS management agreed with all eight recommendations. IRS management agreed to deliver KISAM Asset Manager Tool enhancements for performing asset verification and correct data deficiencies identified by TIGTA; develop a missing asset aging report to facilitate researching and resolving assets in a missing status; and update the Fiscal Year 2014 Inventory Certification Plan to include the verification of the Serial Number field and assets with an acquisition value of $50,000 or greater.

TREASURY INSPECTOR GENERAL
FOR TAX ADMINISTRATION

DEPARTMENT OF THE TREASURY
WASHINGTON, D.C. 20220

September 16, 2013

MEMORANDUM FOR CHIEF TECHNOLOGY OFFICER

FROM: Michael E. McKenney
Acting Deputy Inspector General for Audit

SUBJECT: Final Audit Report – Weaknesses in Asset Management Controls Leave Information Technology Assets Vulnerable to Loss (Audit # 201220016)

This report presents the results of our review of the Knowledge, Incident/Problem, Service Asset Management system. The overall objectives of this review were to determine whether system user permissions were appropriate to ensure the safeguarding of the information technology asset inventory and to review the effectiveness of the system in maintaining an accurate and complete information technology asset inventory. This audit was included in the Treasury Inspector General for Tax Administration's Fiscal Year 2012 Annual Audit Plan and addresses the major management challenge of Modernization.

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

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

Table of Contents

Abbreviations

AM	Asset Manager
IRM	Internal Revenue Manual
IRS	Internal Revenue Service
IT	Information Technology
ITAMS	Information Technology Asset Management System
KISAM	Knowledge, Incident/Problem, Service Asset Management
SACM	Service Asset and Configuration Management
UNS	User and Network Services

Background

The User and Network Services (UNS) organization has responsibility, ownership, management, and control of information technology equipment in the Internal Revenue Service (IRS). The UNS organization's mission includes certifying the information technology inventory on an annual basis and directing Customer Service Support Centers[1] to ensure that the information technology inventory is accurate. Within the UNS organization, the Service Asset and Configuration Management (SACM) organization's Hardware Asset Management office is responsible for providing oversight, coordination, and guidance on information technology equipment management enterprisewide using the Knowledge, Incident/Problem, Service Asset Management (KISAM) system as the management tool. Specifically, the Hardware Asset Management office responsibilities include:

- Developing asset management policies.
- Performing analysis of the Asset Manager (AM) module within the KISAM system and identifying anomalous records.
- Developing and improving processes for asset management and control.
- Monitoring and facilitating execution of the inventory reconciliation and exception plan.
- Working closely with asset owners enterprisewide.

In addition, the organizational placement of the Hardware Asset Management office is intended to maintain its independence from each UNS organization area and external UNS organization entities.[2]

In August and September 2011, the UNS organization replaced the Information Technology Asset Management System (ITAMS) with the KISAM system. The Information Technology (IT) organization's Fiscal Year 2011 fourth Quarter Business Performance Review explained that the previous system became outdated and heavily customized, and it no longer provided sufficient automation to manage the day-to-day operations. As a result, the IRS implemented the KISAM system to improve managing daily operations associated with activities such as asset management. In addition, the IRS is in the process of implementing the Information Technology Infrastructure Library® process methodology to align information technology services with the

[1] See Appendix V for a glossary of terms.
[2] External UNS organization entities consist of Chief Counsel, Enterprise Networks, Enterprise Operations, Information Resources Accessibility Program, Criminal Investigation, and Real Estate and Facilities Management. Criminal Investigation, Chief Counsel, and Real Estate and Facilities Management are permitted to perform inventory tasks such as purchasing and disposing of information technology assets assigned to them.

current and future needs of the organization. The IRS reported that the IT organization had achieved Information Technology Infrastructure Library Maturity Level 3 in October 2012.

The IRS implemented the KISAM system in two releases: the Service Manager module and the AM module. The UNS organization uses the Service Manager module as the problem management reporting tool for all IRS-developed applications and shares information with the Enterprise Service Desk. The UNS organization recognizes the KISAM-AM as the sole authoritative source and official inventory record for all information technology assets within the IRS [with the exception of information technology software–related assets (to include software and software licenses)].

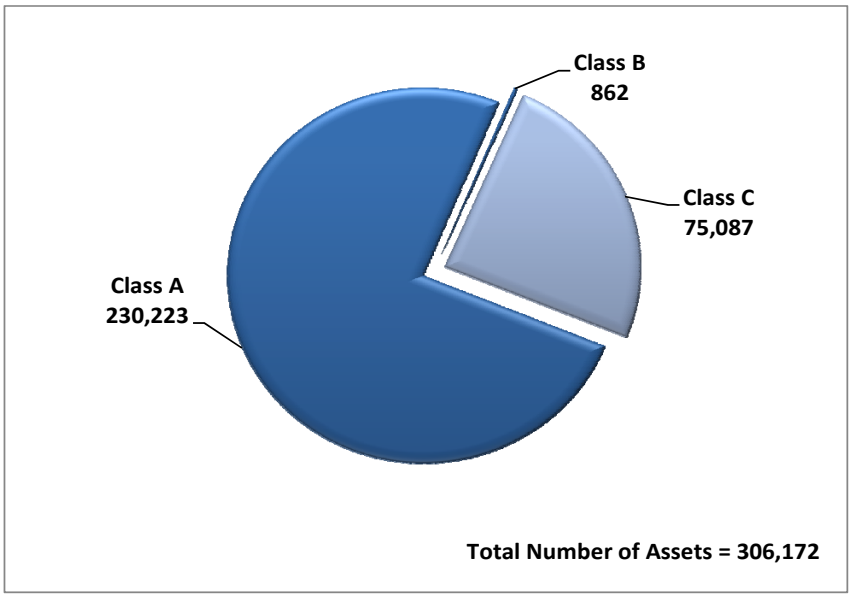
The UNS organization controls information technology assets based on specific classifications.

- Class A – system critical, highly "pilferable," and require significant security considerations or have a high-dollar value. These assets are verified and certified annually. Examples include desktop and laptop computers, high-end scanners, network printers, servers, and routers.
- Class B – exclusively Personal Digital Assistants or Smartphones. These assets are managed electronically and are certified annually.[3]
- Class C – controlled assets with less dollar value than Class A assets that are recorded for important business and operating purposes. Class C assets have an inventory record in the KISAM-AM; however, direction on certification and verification is determined by the Hardware Asset Management office and the annual Asset Management Inventory Certification Plan. Examples include fax machines, low-end scanners, and desktop printers.
- Class D – "consumables" that are not tracked in the KISAM-AM because they are relatively inexpensive items that are replaced rather than repaired. Examples include mice, keyboards, disk drives, and monitors.

Figures 1 and 2 illustrate the total number and dollar value of information technology assets recorded in the KISAM-AM as of August 2012.[4]

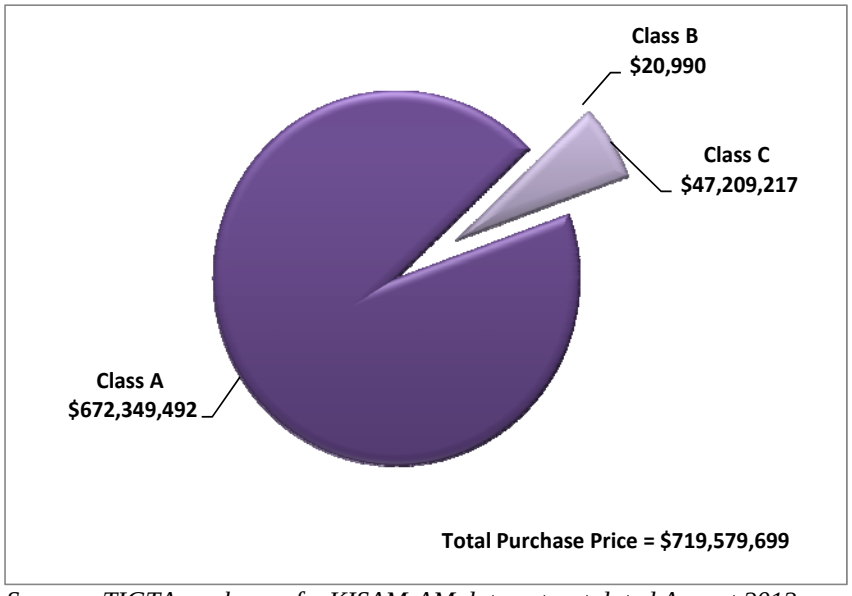
[3] Due to a recent review, we did not include Class B assets in our scope. Treasury Inspector General for Tax Administration, Ref. No. 2013-10-010, *Inadequate Aircard and BlackBerry® Smartphone Assignment and Monitoring Processes Result in Millions of Dollars in Unnecessary Access Fees* (Jan. 2013).
[4] The dollar value was obtained by using the acquisition cost reported in the KISAM-AM. TIGTA did not perform any independent tests to ensure the accuracy of the cost information reported in the KISAM-AM.

Figure 1: Total Number of Information Technology Assets[5]



Source: TIGTA analyses of a KISAM-AM data extract dated August 2012.

Figure 2: Total Dollar Value of Information Technology Assets



Source: TIGTA analyses of a KISAM-AM data extract dated August 2012.

[5] There were 529,419 records in the KISAM-AM data extract; however, only 306,172 are information technology inventory asset records. The remaining 223,247 records are non–information technology asset records.

The UNS organization issues the Annual Asset Management Inventory Certification Plan (hereafter referred to as the Certification Plan) to facilitate the annual reconciliation and verification of assets to the KISAM-AM. Certification Plan goals include locating and verifying the existence of all controlled Class A and Class B assets, leveraging opportunities to verify Class C assets, verifying and confirming that a KISAM-AM inventory record is associated with every controlled asset in the IRS, and certifying the accuracy of key KISAM-AM data fields. The Certification Plan also acknowledges that increasing and maintaining the accuracy and completeness of all information technology assets in the KISAM-AM is critical in assessing and monitoring asset inventory as well as meeting the current and future needs of the organization.

The annual certification cycle for asset verification activities occurs from October 1 through June 30 each fiscal year. During this time, all IT organizations work with the SACM organization to validate and certify a complete and thorough inventory. At the close of the certification period, the Hardware Asset Management office provides certifying organizations (*e.g.*, the Field Directors for each UNS organization Customer Service Support Center) with detailed information about asset records under their control. The information consists of Anomaly Reports, a Certification Letter, and a Reconciliation Plan Letter. All organizations must return the Certification and the Reconciliation Plan Letters, both signed by the official representing the organization. The signed Certification Letter states that an inventory of all assets requiring certification has been completed according to the Certification Plan. The signed Reconciliation Plan Letter includes a commitment to address and correct by fiscal year end any anomalous asset records and error conditions, including unverified Class A and Class B assets, reported in the Reconciliation Plan Letter. The reconciliation period begins July 1 and concludes by September 30 each fiscal year.

The Hardware Asset Management office leverages a combination of electronic and physical verification methods to verify assets. Shifting from a periodic physical wall-to-wall inventory, the SACM organization continues to promote and implement a perpetual inventory process by capturing changes to asset inventory in real-time. The SACM organization uses two electronic tools for verification of assets: a barcode scan and an automated or manual update through a network scanning tool such as Tivoli. The SACM organization also uses three physical verification methods: customer self-certification, a physical touch of the asset (*i.e.*, asset move, add, change, maintenance, or physical inventory), and a documented customer interaction, such as a service ticket. To verify an asset, certain KISAM-AM date fields need to be populated with a date of October 1 or later in the appropriate fiscal year. Once a date field has been updated, the asset is considered verified.

This review was performed at the UNS organization offices at the Brookhaven Campus (which includes the Depot) in Brookhaven, New York, and the New Carrollton Federal Building in Lanham, Maryland, during the period October 2012 through June 2013. 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 objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives. Detailed information on our audit objectives, scope, and methodology is presented in Appendix I. Major contributors to the report are listed in Appendix II.

Results of Review

Asset Data Successfully Migrated Between Inventory Systems; However, Access Controls Need Improvement

From July 14 through August 25, 2011, the KISAM Project Management office worked on migrating and validating data from the ITAMS to the KISAM-AM. To ensure a successful transition, the SACM organization issued guidance communicating a suspension of certain asset management activities, *e.g.*, processing asset disposals during the transition period. The SACM organization provided us with the criteria used to identify each subset of asset data in the ITAMS prior to the migration and the corresponding record counts for the same subset of data in the KISAM-AM. The SACM organization also provided explanations when differences between the reported datasets occurred. For example, the August 2011 ITAMS data extract showed that there were 230,727 assets with an assignment status of "in use" at the time of migration. According to the SACM organization, the KISAM-AM data reported 221,213[6] assets with an assignment status of "in use;" management explained that the almost 10,000 asset difference was due to 4,855 BlackBerrys that did not migrate until after the KISAM-AM was implemented and 4,660 assets assigned to the Volunteer Income Tax Assistance program that changed to an "in stock" assignment status.

Using the August 2011 ITAMS and the October 2011 KISAM-AM data, we followed the migration steps and compared the two data sets to ensure that all inventory records migrated. Our initial analyses showed that the total number of records migrated did not match the figures provided by SACM organization management, differing by only 38 records. However, upon reviewing our identified discrepancies, SACM organization management provided support to show these 38 assets were in the KISAM-AM under a different barcode number. Each of these records had a barcode replaced, resulting either from a worn barcode or replacement asset.

We also conducted tests to ensure that sufficient system controls were in place to protect access to the KISAM system data. Our tests determined that the KISAM application, database, and operating system complied with password management requirements outlined in Internal Revenue Manual (IRM) 10.8.1, *Password (Authentication) Management*. However, our review of the switch user log (audit log) identified three individuals who accessed the KISAM system database using a system account and without a need to know. These three individuals are not database administrators and should not have access to the database system account or the password for the account. This suggests a security weakness exists within the KISAM system

[6] One asset migrated to the KISAM-AM "in use" assignment status from an ITAMS "in stock" assignment status (230,727 – 4,855 – 4,660 + 1 = 221,213).

infrastructure, and at this time we cannot be assured that the data within the KISAM system are protected from accidental or malicious altering.

IRM 10.8.3, *Audit Logging Security Standards*, establishes agencywide policy for the collection and processing of computer-generated event logs, also called audit logs. Audit capabilities apply to all aspects of a system, including operating systems, database systems, and applications. The IRM further prescribes that the audit trails be used by security specialists within the IRS to help accomplish several security-related objectives, such as individual accountability.

During our meeting to discuss the results of this audit, IRS management indicated that due to resource availability they made a risk-based decision to allow database administrators to perform tasks using the database system account by invoking the switch user command. IRS management advised us that the switch user audit logs were reviewed by security analysts within the Cybersecurity organization. When we followed up to request documentation to support these claims, IRS management provided a document explaining that the switch user command had been in place for many years and preceded the risk-based decision document requirement. We also discussed the audit log review process with representatives from the Enterprise Security Audit Trails group (within IRS's Cybersecurity organization), who explained that a process is in place to review these logs; however, it has yet to be implemented for the KISAM system application and its infrastructure.

Although the switch user login events are recorded in an audit log, no one is currently reviewing the log to ensure that only appropriate accesses are made. This is because the Enterprise Security Audit Trails group is currently working on developing reports to facilitate reviewing the audit log events. Until this occurs, we believe that the IRS needs to develop an interim, mitigating control to review the audit logs.

Recommendation

The Chief Technology Officer should:

***Recommendation 1*:** Ensure that the switch user log for the KISAM system is reviewed while the Enterprise Security Audit Trails group works on developing and implementing the full functionality of its automated tools.

> ***Management's Response*:** IRS management agreed with the recommendation and will ensure that the switch user log for the KISAM system is reviewed while the Enterprise Security Audit Trails group works on developing and implementing the full functionality of its automated tools.

Asset Data in the Knowledge, Incident/Problem, Service Asset Management System Are Inaccurate and Incomplete

Although the SACM organization established procedures to ensure the accuracy of its information technology asset records within the KISAM-AM, procedures are not being followed. As a result, the KISAM-AM contains incomplete and inaccurate information. Specifically, we identified inaccurate information in the KISAM-AM relating to the information technology assets we physically verified. We also found that some items selected for verification from the "floor" were not recorded in the KISAM-AM and some inventory updates were not timely made. These conditions occurred because of a reduction in staff resulting from the prior End-User Equipment and Services reorganization.[7] An inaccurate and incomplete inventory system decreases data integrity and exposes the IRS to the loss or theft of its assets.

Some assets could not be located and some assets that could be physically verified had inaccurate data recorded in the KISAM-AM

Of the 242 assets in our judgmental sample,[8] we physically located and verified 186 assets. We could not locate 30 assets, and 26 assets were in "missing" or "retired" status. There were 61 assets with inaccurate data in fields that should be reviewed for accuracy during the annual inventory, as shown below:

- 31 assets with inaccurate entries in the Assignment field (*e.g.*, four items were classified in the KISAM-AM in a "missing" status, yet we located the assets during our site visits).
- 16 assets with inaccurate entries in more than one required field.
- 8 assets with incorrect entries in the User Name field.
- 6 assets with inaccurate entries in the Building Code field.

Figure 3 lists the minimum required data fields that must be kept current and accurate for each asset record within the KISAM-AM per IRM 2.14.1, *Asset Management, Information Technology Asset Management*. The figure also provides a definition for each field and identifies whether the SACM organization requires the field to be verified during the annual inventory.

[7] On April 22, 2012, the End-User Equipment and Services organization merged with the Enterprise Networks organization to form the User and Network Services organization.
[8] A judgmental sample is a nonstatistical sample, the results of which cannot be used to project to the population.

Figure 3: Minimum Required KISAM-AM Data Fields to Be Kept Current and Accurate and the Field Definitions

KISAM-AM Field Name	Verified During Inventory	Definition
Assignment	Yes	Provides the status of an asset at any given time.
Barcode	Yes	A permanent sticker with a unique series of lines printed on it, which is attached to an information technology asset for quick identification by a scanner.
Serial Number	No	A unique, identifying number or group of numbers and letters assigned to an individual asset.
Building Code	Yes	Identifies the building and address of the asset location.
Cost Center	No	Identifies the organization (*e.g.*, Enterprise Operations) primarily responsible for the asset. The data are auto-populated from another source.
System Name	No	Used to improve tracking and management of "in stock" equipment. Also used to identify special equipment used within the IRS (*e.g.*, Common Premise Capability equipment used to support Voice Over Internet Protocol).
Computer Name	No	Populated for computers only. Provides information about the computer and is used to help with electronic touches via Tivoli.
Contact Name[9]	No	Records the primary user of IRS-owned assets. Assets that are not assigned to a primary user are identified as "shared" assets.

Source: TIGTA analysis of IRM 2.14.1 and Fiscal Year 2012 Asset Management Inventory Certification Plan.

We also identified an additional 22 assets in our sample with inaccurate data recorded in the KISAM-AM Serial Number field. A further analysis of the KISAM-AM data identified 1,123 asset records with the same entries in the Serial Number field (*e.g.*, 0000000 or 1234) and 22 asset records where the Serial Number field contained an invalid character. According to the IRM, the Serial Number field consists of alphanumeric characters and can include dashes, which are the only special character allowed. Further, the Serial Number field is protected and cannot be changed after initial entry unless a service desk ticket is submitted.

Although the SACM organization does not currently require independent verification of the Serial Number field, we believe this should be added to the Certification Plan requirements, especially because there are several other information technology asset management processes

[9] The Contact Name data field is different from the User Name data field in the KISAM-AM. While the IRM requires the Contact Name field to be kept current and accurate, the Certification Plan requires verification of the User Name field.

(*e.g.*, asset disposal and purchase of maintenance) that require both the barcode and serial number to identify each asset. Further, the SACM organization acknowledges in the IRM that efforts to locate assets by serial number sometimes fail due to inconsistencies in the data.

We also analyzed two other required data fields in the KISAM-AM and identified the following:

- 20,546 asset records with blank Cost Center fields (the Cost Center field should be auto-populated).
- 38,774 assets in an "in stock" status had an invalid entry in the System Name field.

According to the IRM, standard recording of assets in an "in stock" assignment status assists with the proper identification, monitoring, and control of the assets. Using the System Name field in the KISAM-AM allows offices to more efficiently manage their equipment assigned with an "in stock" status. Acceptable entries in the System Name field include "general refreshment," "depot local," "depot project," and "national depot." Analysis of the KISAM-AM data showed that 34,488 of the assets with an "in stock" status used the default entry of "admin" for the System Name field. Additionally, approximately 80 percent (27,515 of 34,488) of these asset records with the default entry of "admin" also had entries in the Organization Code field. The IRM states that the Organization Code field can be used for whatever the IT organization staff deems necessary to manage assets, with the exception of assets in an "in stock" status.

Required asset information was not timely updated in the KISAM-AM

Our review also identified 21 of 242 assets for which information about the asset was not timely updated in the KISAM-AM. For example, we identified five assets assigned to a user who retired in 2011; however, the August 2012 KISAM-AM data still showed the assets assigned to the former employee. According to IRM 2.14.1, all updates to asset data must be completed within 10 days. Additionally, the UNS organization information technology specialists will use the electronic move, add, and change form to document inventory changes in the KISAM-AM within 10 days from the change request. To further enhance the accuracy of the data within the KISAM-AM and ensure that the SACM organization meets its goal of implementing a perpetual inventory system, any changes to information technology assets must be timely updated in the KISAM-AM.

Assets selected for verification from the floor were not recorded in the KISAM-AM

We also judgmentally selected 96 assets from the floor during our verification testing and traced the items to determine if they were recorded and controlled on the KISAM-AM. Thirteen assets totaling approximately $153,869 were not controlled in the KISAM-AM.[10] These items included

[10] The dollar value is underestimated because we did not capture sufficient information for four of the 13 assets from one of the locations visited and could not research the KISAM-AM to obtain an estimated cost for those assets.

a degausser (used to wipe sensitive data from storage media), a computer, and a printer. These items present a greater risk of being lost or stolen because they are not controlled on the inventory system. IRM 2.14.1 provides instructions that if assets are found on the floor during the annual inventory, the KISAM-AM must be updated within 10 days.

Recommendations

The Chief Technology Officer should:

***Recommendation 2*:** Update the Certification Plan to include the requirement to verify the accuracy of the data reported in the Serial Number field.

> ***Management's Response*:** IRS management agreed with the recommendation and will update the Fiscal Year 2014 Certification Plan to include the requirement that the Serial Number field be verified and validated for all assets requiring certification.

***Recommendation 3*:** Ensure that the KISAM-AM information is timely updated and maintained.

> ***Management's Response*:** IRS management partially agreed with the recommendation and will deliver KISAM Asset Manager Tool enhancements for performing asset verification and systemic asset updates for service asset transactions and events documented within Service Manager if and when funding is available.

***Recommendation 4*:** Create additional anomaly reports for the minimum required KISAM-AM data fields to facilitate ensuring that only valid entries are provided.

> ***Management's Response*:** IRS management agreed with the recommendation and will engage asset owners and stakeholders to solicit feedback and requirements for new asset data anomaly reports to facilitate anomaly resolution and verification activities. They also stated that any necessary new reports will be created.

Ineffective Controls Create an Environment in Which Information Technology Assets Are Vulnerable to Loss

Our review identified several conditions demonstrating the IT organization's inability to maintain effective controls over its information technology assets. For, example, we visited the Brookhaven Campus (which included a Depot location) and the New Carrollton Federal Building and physically located and verified information technology assets controlled in the KISAM-AM (referred to as book-to-floor testing). We judgmentally selected a sample of 146 information technology assets from a population of 47,857 assets recorded in the KISAM-AM. We could not locate and verify or find proper supporting documentation for 34 assets valued at $948,310.

As previously mentioned, we also judgmentally selected a sample of 96 information technology assets located in the offices to verify if these items were controlled in the KISAM-AM (referred to as floor-to-book testing). Our results showed that 12 information technology assets valued at an estimated $28,869 were not controlled in the KISAM-AM.

Offices improperly completed the annual inventory reconciliation process

IRS offices did not always properly conduct the reconciliation of information technology assets because they did not have sufficient resources to properly follow up and resolve those asset records identified by the SACM organization as needing updating or correcting. As of July 2012, the start of the reconciliation period, a total of 17,162 Class A and B assets in the KISAM-AM had not been physically or electronically verified. The two offices selected for our review committed to address and resolve outstanding issues identified during the annual inventory by the end of the fiscal year (*i.e.*, September 30, 2012). When we conducted our on-site testing in November and December 2012, well after the close of the reconciliation period, we could not locate 30 information technology assets, 17 (13 Class A and 4 Class C) of which appeared on the offices' reconciliation plan lists dated July 2012. Sixteen of the 17 assets appeared in the reconciliation plan lists as either "aged in stock" (8), or "unverified" (8), suggesting that at that time they existed within the IRS environment. One of the 17 assets appeared in the reconciliation plan as "aged awaiting receipt." The 17 assets had an acquisition value totaling $800,554 and included a laptop and desktop computer, a server, and a network printer.

IRM 2.14.1 describes reconciliation as the process of matching information gathered at the time of the inventory (*e.g.*, via self-certification, Tivoli scan, barcode scan) with what is recorded in the KISAM-AM. The IRM further states that offices have until the end of the fiscal year to resolve any outstanding errors found during the analysis. The Certification Plan describes anomaly reporting as identifying inconsistencies within the KISAM-AM data (*e.g.*, assets that do not have a verification date) or lifecycle control issues (*e.g.*, assets in a status longer than they should be). Every effort should be made to update the KISAM-AM expeditiously to correct data errors or document asset transactions. The Certification Plan also states that it is imperative that all "unverified" asset records are updated if the asset is located or surveyed off the database if the asset is determined to be unaccounted for or missing. The SACM organization, in conjunction with asset owners and stakeholders, will work to resolve critical asset data anomalies and complete the requirements of the Certification Plan during the reconciliation period.

The Certification Plan describes "aged in stock" assets as those that are out of warranty and too costly to repair. Offices should use information about "aged in stock" assets to reduce the number of assets in that status. Eight of the assets we could not locate during our review appeared on the "aged in stock" list and still showed in an "in stock" status per an updated KISAM-AM extract dated December 2012. Similarly, eight of the assets we could not locate during our review appeared on the unverified assets list, yet updated KISAM-AM data showed these assets as still in the "in stock" or "in use" statuses. For the one asset that appeared on the

"aged awaiting receipt" report, the updated KISAM-AM data showed that the asset had moved to an "in stock" status; however, we could not locate the asset during our visit.

These continued data discrepancies indicate that the IRS offices did not effectively complete the reconciliation process and correct the data errors prior to the end of September 2012. Further, because we could not locate and UNS organization staff could not provide us with documentation to support whether the 17 assets in question were either relocated to another organization/office or disposed, we have no assurance that those assets with storage media (*e.g.*, server, laptop computer, desktop computer) did not contain any sensitive information. SACM organization management needs to take additional steps to ensure that asset owners resolve all outstanding issues during the reconciliation period. Otherwise, information technology assets will continue to be at risk of loss and management will be unable to rely on the data within the KISAM-AM to make business decisions.

Insufficient steps were taken to recover missing assets

Offices are not taking sufficient steps to recover assets placed in a temporary "missing" status because they do not have the resources available to track down the assets and because the reports used by the offices to track down missing assets did not provide disposal information. Sixteen of the 146 assets judgmentally selected from our sample of the KISAM-AM records were categorized in the KISAM-AM in a "missing" status, 13 of which appeared on the offices' reconciliation lists as missing and requiring resolution. During our on-site visits, which occurred after the end of the reconciliation period, we physically located and verified four of the assets and were provided documentation supporting the disposition of another eight assets.[11] The KISAM-AM status for these 12 assets still showed as "missing" several months after the end of the reconciliation period, whereas the assets' statuses should have been updated during the reconciliation period to a status other than "missing."

According to IRM 2.14.1, assets placed in a temporary "missing" status will appear on an anomaly report if those asset records have not been updated after 60 days. Offices are required to reconcile their missing assets by the end of the fiscal year in which the inventory began. The IRM prescribes detailed steps offices should take to help with locating missing assets. These steps include, but are not limited to, checking when the asset was last scanned by Tivoli, physically searching for the asset based on location information recorded in the KISAM-AM, calling the contact person listed in the KISAM-AM, and "pinging" the asset if it is a desktop or laptop computer. After all efforts have been made to locate the missing assets, offices may proceed with paperwork to "survey" or remove the asset record from the active inventory in the KISAM-AM.

[11] For the remaining four assets, the IRS did not provide sufficient documentation to explain why the assets continued to remain in a "missing" status or why they had not been removed from the KISAM-AM.

Our review of the KISAM-AM data for the eight disposed assets determined that each asset record provided an IRS report number identifying the disposal documentation. The IRS report number was not included in the missing asset lists provided to the offices for resolution. Had this information been included, these assets could have been resolved by obtaining the documentation to confirm the disposition of the assets and updating the KISAM-AM to reflect the disposition date. We successfully physically located and verified four assets only after our inquiries led SACM organization personnel to contact the users listed in the KISAM-AM, steps that should have been taken prior to fiscal year end.

We also observed three instances where offices surveyed (or removed from the KISAM-AM active inventory) a combined total of 423 assets during March and June 2012. This occurred prior to receiving a Reconciliation Plan Letter, which is typically distributed on July 13 of each fiscal year. For two of the instances, SACM organization personnel specifically stated that the assets could not be located and were thus surveyed from the KISAM-AM active inventory. The third instance was a follow-up on asset records that migrated from the ITAMS to the KISAM system and could not be found. These assets, with an acquisition cost of more than $1.1 million, included desktop and laptop computers and servers. According to the disposal documentation, the responsible asset owners removed the assets from the KISAM-AM active inventory, stating the assets were "lost" on March 28, 2012, March 29, 2012, and June 25, 2012, respectively. While we understand it may be necessary to survey asset records from the KISAM-AM from time to time, this practice should not become routine. If IRS employees survey missing assets without taking appropriate actions to locate the assets, then the employees will be burdened by additional steps to reinstate these asset records when they do eventually locate the asset.

High-valued information technology assets used in financial statement reporting are not subject to annual inventory

Our analysis of KISAM-AM data identified 60 Class C information technology assets worth almost $5.9 million that met the financial statement reporting requirements because 38 of the assets are information technology assets and 22 of the assets are other equipment that met the cost and useful life thresholds for financial statement reporting purposes. However, 45 of these information technology assets were not verified during Fiscal Year 2012. This occurred because the IRS did not incorporate guidance into the Certification Plan to consider the acquisition value of assets during the annual inventory. These assets are of particular concern because they meet the dollar criteria for financial statement reporting purposes.

According to IRM 1.35.6, *Property and Equipment Accounting*, the IRS will capitalize information technology equipment, regardless of price or value, unless it is specifically exempted as expendable equipment. The IRM further provides that equipment designated as other equipment will be capitalized when the requisition funding line is greater than or equal to $50,000 and has a useful life greater than two years. Because these 60 high-value information technology assets affect the IRS's financial statements, every effort should have been made to verify them during the annual inventory and ensure the accuracy of the financial statements.

Recommendations

The Chief Technology Officer should:

Recommendation 5: Ensure that the KISAM-AM records are updated to correct the deficiencies identified in our review and provided to management.

> **Management's Response:** IRS management agreed with the recommendation and will perform data review and analysis to correct deficiencies we identified and update KISAM-AM accordingly with current and complete information.

Recommendation 6: Ensure that the reconciliation process is effectively completed and have offices provide supporting documentation to the SACM organization for quality review.

> **Management's Response:** IRS management agreed with the recommendation and will implement and communicate process controls for follow-up actions with the responsible and accountable asset owners. They will also use an Enterprise Governance Board to monitor compliance.

Recommendation 7: Include additional data in the missing asset anomaly report (*e.g.*, disposal information) to allow offices to resolve these assets.

> **Management's Response:** IRS management agreed with the recommendation and will develop a missing asset aging anomaly report including appropriate data fields to facilitate researching and resolving assets in a missing status.

Recommendation 8: Include dollar threshold criteria in the Certification Plan for certifying information technology assets with a high-dollar value that affect financial statement reporting.

> **Management's Response:** IRS management agreed with the recommendation and will update the FY 2014 and all future Certification Plans to require that assets with an acquisition value of $50,000 or greater be verified and certified.

Appendix I

Detailed Objectives, Scope, and Methodology

Our overall objectives were to determine whether system user permissions were appropriate to ensure the safeguarding of the information technology asset inventory and to review the effectiveness of the system in maintaining an accurate and complete information technology asset inventory. To accomplish our objectives, we:

I. Evaluated the effectiveness of the general information technology access controls and determined whether the KISAM system is properly safeguarded from unauthorized access and changes.

   A. Ensured the passwords for the application, database, and operating system complied with policies outlined in the IRM.

   B. Reviewed information generated from the audit log to ensure that only appropriate individuals accessed the database.

II. Assessed the effectiveness of the inventory management controls to ensure the accuracy and reliability of the KISAM system to safeguard assets from fraud, waste, and abuse.

   A. Analyzed the KISAM-AM data as of August 13, 2012, and identified 306,172 information technology assets with an acquisition cost of approximately $719 million. The IT Headquarters office in New Carrollton, Maryland, and the Depot in Brookhaven, New York, were judgmentally[1] selected based on factors such as having a high Classes A and C asset count and a high total Classes A and C asset value. 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.

   B. Conducted a physical verification of information technology assets, excluding Class B assets,[2] listed in the KISAM-AM and assigned to the two offices in our review.

      1. Analyzed information technology assets and identified assets assigned to the following statuses: "in use," "awaiting receipt," "in stock," and "retired."

[1] A judgmental sample is a nonstatistical sample, the results of which cannot be used to project to the population.
[2] Due to a recent review, we did not include Class B assets in our scope. Treasury Inspector General for Tax Administration, Ref. No. 2013-10-010, *Inadequate Aircard and BlackBerry® Smartphone Assignment and Monitoring Processes Result in Millions of Dollars in Unnecessary Access Fees* (Jan. 2013).

2. Judgmentally selected 146 information technology assets (from a population of 47,857) assigned to the two offices. 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.
3. Physically verified 116 of the 146 information technology assets at the two offices.

C. Judgmentally selected from the "floor" a total of 96 information technology assets from the two offices and determined whether the information technology assets were properly controlled in the KISAM-AM. We used judgmental sampling because we could not determine the population of all information technology assets in these offices.

D. Reviewed the Fiscal Year 2012 inventory verification and reconciliation process for each office.

E. Analyzed the KISAM-AM data to identify data inaccuracies in those fields where the IRM and Certification Plan require accurate information.

III. Evaluated the results from migrating inventory data from the ITAMS to the KISAM system to ensure that 100 percent of the inventory records were accounted for.

A. Obtained an ITAMS data extract and compared it to the KISAM system data to ensure that all the information related to the assets was migrated.

B. Requested a detailed walk-through of the data migration/validation contractor/ developer-prepared deliverables and, where warranted, requested additional supporting documentation.

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 the following internal controls were relevant to our audit objective: UNS organization's policies, procedures, and practices relating to information technology asset management and inventory; policies and procedures relating to access security controls; and asset migration strategy, procedures, and practices. We evaluated these controls by interviewing UNS organization management and IT organization staff, asset users, and access security managers; reviewing relevant documentation; and analyzing the KISAM-AM data.

Appendix II

Major Contributors to This Report

Alan R. Duncan, Assistant Inspector General for Audit (Security and Information Technology Services)
Danny Verneuille, Director
Diana Tengesdal, Audit Manager
Mark Carder, Lead Auditor
Richard Borst, Senior Auditor
Lara Phillippe, Auditor
Kevin Liu, Information Technology Specialist

Appendix III

Report Distribution List

Acting Commissioner
Office of the Commissioner – Attn: Chief of Staff C
Deputy Commissioner for Operations Support OS
Deputy Chief Information Officer for Operations OS:CTO
Associate Chief Information Officer, Enterprise Operations OS:CTO:EO
Associate Chief Information Officer, User and Network Services OS:CTO:UNS
Chief Counsel CC
National Taxpayer Advocate TA
Director, Office of Legislative Affairs CL:LA
Director, Office of Program Evaluation and Risk Analysis RAS:O
Office of Internal Control OS:CFO:CPIC:IC
Audit Liaison: Director, Risk Management Division OS:CTO:SP:RM

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; 60,548 information technology asset records with incorrect or invalid entries in fields that are required to be accurate (see page 8).

Methodology Used to Measure the Reported Benefit:

- We judgmentally selected 146 information technology assets from the KISAM-AM to physically verify and 96 information technology assets from the "floor" to determine if they were properly controlled in the KISAM-AM. Sixty-one of these items had inaccurate data in fields that should be reviewed for accuracy.
- We analyzed the KISAM-AM and our judgmental sample identified 1,167 (1,123 + 22 + 22) asset records with inaccurate or invalid entries in the Serial Number field. Our analysis also identified 59,320 (20,546 + 38,774) asset records with either a blank entry in the Cost Center field or an invalid entry in the System Name field.

Type and Value of Outcome Measure:

- Protection of Resources – Potential; 46 information technology assets costing $977,179[1] could not be located or positively identified or were not controlled in the KISAM-AM (see page 11).

Methodology Used to Measure the Reported Benefit:

- We judgmentally selected 146 information technology asset records from the KISAM-AM to physically verify. We could not locate or find support for 34 assets. These items had an acquisition cost of $948,310.

[1] The value of information technology assets reported in this section of the report was derived by using the data which appeared in the Purchase Price field within the KISAM-AM. According to the IRS, the KISAM-AM does not calculate the current market value of its assets. As a result, these reported dollar amounts could be inflated.

- We judgmentally selected 96 information technology assets to determine if the items were properly controlled in the KISAM-AM. We identified 12 assets that were not controlled in the KISAM-AM. These assets had a total estimated acquisition cost of $28,869.

***Type and Value of Outcome Measure*:**

- Protection of Resources – Potential; 60 Class C information technology asset records with an acquisition cost totaling $5,880,619 that were not verified (see page 11).

***Methodology Used to Measure the Reported Benefit*:**

We analyzed the KISAM-AM and identified 60 Class C assets that met the financial statement reporting requirements but were not verified because the Certification Plan does not include guidance that considers the acquisition value of assets. Information technology assets are capitalized regardless of price or value, and equipment designated as other equipment will be capitalized when the requisition funding line is greater than or equal to $50,000 and has a useful life greater than two years. The 60 Class C assets met the capitalization requirements.

Appendix V

Glossary of Terms

Term	Definition
Anomaly Report	Produced annually and provided by the Hardware Asset Management office to identify inconsistencies or potential inaccuracies in the KISAM-AM database.
Asset Management Inventory Certification Plan	Annual document sent to individuals responsible for managing and verifying information technology assets. This document provides timelines and detailed guidance for completing the inventory and reconciliation process.
Asset Manager	KISAM module that tracks information technology and non–information technology equipment used throughout the IRS.
Awaiting Receipt	The KISAM-AM asset assignment status of pending acceptance (to be received) and usually in transit status.
Campus	The data processing arm of the IRS. The campuses process paper and electronic submissions, correct errors, and forward data to the Computing Centers for analysis and posting to taxpayer accounts.
Certification Letter	A letter sent to each certifying organization populated with information corresponding to assets controlled by the certifying area. Each organization certifies on or about the end of July that an inventory of all assets requiring certification has been completed.
Certifying Organization	Organizations responsible for completing a Certification Letter and Reconciliation Plan Letter.
Customer Service Support Center	Consists of Service Desk and Deskside groups, which provide prompt and professional resolution of IRS end-user incidents and problems.
Database Administrator	An individual that performs all activities related to maintaining a correctly performing and secure database environment. Responsibilities include design, implementation, and maintenance of the database system.

Term	Definition
Depot	There are four Functional Equipment Depots: Brookhaven [formerly Volunteer Income Tax Assistance Program], Austin, Ogden, and Memphis. Equipment Depots perform inventory tasks and track assets that are either distributed and deployed in various locations or remotely located, requiring regular communication with end users and the Hardware Asset Management office.
Enterprise Service Desk	Responsible for receiving incident reports, defining the incident category, determining the priority for all incident reports received, and overseeing the resolution process.
In Stock	KISAM-AM asset assignment status of unplugged and reserved for future use.
In Use	KISAM-AM asset assignment status of currently being used and is plugged in. The asset is in use, installed, and operational.
Information Technology Infrastructure Library	Provides a practical, no-nonsense framework for identifying, planning, delivering and supporting information technology services to the business. It advocates that information technology services must be aligned to the needs of the business. It provides guidance to organizations on how to use information technology as a tool to facilitate business change, transformation, and growth. Maturity levels refer to an information technology organization's ability to perform. An organization passes through five evolutionary levels as it becomes more competent: Level 1: Initial – Focuses on technology and technology excellence/experts. Level 2: Repeatable – Focuses on products/services and operational processes (*e.g.*, Service Support). Level 3: Defined – Focuses on the customer and proper service level management. Level 4: Managed – Focuses on business/information technology alignment. Level 5: Optimized – Focuses on value and the seamless integration of information technology into the business and strategy making.
Missing	KISAM-AM asset assignment status of lost, stolen, or temporarily missing assets until a determination is made.

Term	Definition
Pinging	Running the "ping" command from the operating system prompt to determine if an asset is connected to the network.
Reconciliation Plan Letter	Letter sent to each certifying organization containing anomalous asset records requiring correction and modification to the KISAM-AM. The letter includes a commitment by the certifying official to ensure that all outstanding items are addressed by the end of September.
Retired	KISAM-AM asset assignment status of removed from active inventory and no longer used. This assignment is used in conjunction with disposal codes.
Tivoli	Application that performs system and network management, and exports hardware inventory information to the KISAM-AM on a weekly basis.

Appendix VI

Management's Response to the Draft Report

CHIEF TECHNOLOGY OFFICER

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

August 22, 2013

MEMORANDUM FOR DEPUTY INSPECTOR GENERAL FOR AUDIT

FROM: Terence V. Milholland
Chief Technology Officer

SUBJECT: Draft Audit Report – TIGTA Draft Report - Weaknesses in Asset Management Controls Leave Information Technology Assets Vulnerable to Loss (Audit #201220016)

Thank you for the opportunity to review the draft audit report and to discuss the report observations with the audit team. I was encouraged by your acknowledgement of the IRS' achievement of Information Technology Infrastructure Library (ITIL) maturity Level 3 and the successful migration of information technology asset data from the legacy inventory system to KISAM-Asset Manager.

In response to your recommendation we have attached our corrective action plan. We are committed to implementing these improvements, however we want to note that implementation of some actions are dependent on budget availability. Also, while the IRS is in agreement with the eight recommendations provided by TIGTA, we take exception to the outcome measures outlined in the draft report. KISAM-AM is the sole authoritative source and official inventory repository for all Information Technology assets; it is not the authoritative source for financial data. As such, KISAM does not calculate the current market value of assets. Additionally, while IRM 2.14.1 requires that the Cost Center code be kept accurate, there are specific business rules that may cause the cost center to be null. The IRS will drive continual improvements and risk mitigation in these areas by reducing reliance on manual inventory processes and using automated tools.

We value your continued support and the assistance your organization provides. If you have any questions, please contact me at (202) 622-6800 or a member of your staff may contact Lisa Starr, Senior Manager, Program Oversight at (202) 283-3607.

Attachment

Attachment
Draft Audit Report – Weaknesses in Asset Management Controls Leave Information Technology Assets Vulnerable to Loss (Audit # 201220016)

RECOMMENDATION #1: Ensure that the switch user log for the KISAM system is reviewed while the Enterprise Security Audit Trails group works on developing and implementing the full functionality of its automated tools.

CORRECTIVE ACTION #1: IRS agrees with this recommendation. We shall ensure that the switch user log for the KISAM system is reviewed while the Enterprise Security Audit Trails group works on developing and implementing the full functionality of its automated tools.

IMPLEMENTATION DATE: June 25, 2014

RESPONSIBLE OFFICIAL: Associate Chief Information Officer, Cybersecurity

CORRECTIVE ACTION MONITORING PLAN: We enter accepted corrective actions into the Joint Audit Management Enterprise System (JAMES) and monitor them on a monthly basis until completion.

RECOMMENDATION #2: Update the Certification Plan to include the requirement to verify the accuracy of the data reported in the Serial Number field.

CORRECTIVE ACTION #2: IRS agrees with this recommendation. We will update the FY2014 Certification Plan to include the requirement that the Serial Number field be verified and validated for all assets requiring certification.

IMPLEMENTATION DATE: May 25, 2014

RESPONSIBLE OFFICIAL: Associate Chief Information Officer, User & Network Services

CORRECTIVE ACTION MONITORING PLAN: We enter accepted corrective actions into the Joint Audit Management Enterprise System (JAMES) and monitor them on a monthly basis until completion.

RECOMMENDATION #3: Ensure that the KISAM-AM information is timely updated and maintained.

CORRECTIVE ACTION #3: IRS partially agrees with this recommendation. IRS will deliver KISAM Asset Manager Tool enhancements for performing asset verification, and systemic asset updates for service asset transactions and events documented within Service Manager if and when funding is available.

IMPLEMENTATION DATE: September 25, 2015

RESPONSIBLE OFFICIAL: Associate Chief Information Officer, User & Network Services

Attachment
Draft Audit Report – Weaknesses in Asset Management Controls Leave Information Technology Assets Vulnerable to Loss (Audit # 201220016)

CORRECTIVE ACTION MONITORING PLAN: We enter accepted corrective actions into the Joint Audit Management Enterprise System (JAMES) and monitor them on a monthly basis until completion.

RECOMMENDATION #4: Create additional anomaly reports for the minimum required KISAM-AM data fields to facilitate ensuring only valid entries are provided.

CORRECTIVE ACTION #4: IRS agrees with this recommendation. We will engage asset owners and stakeholders to solicit feedback and requirements for new asset data anomaly reports to facilitate anomaly resolution and verification activities. Any necessary new reports will be created.

IMPLEMENTATION DATE: September 25, 2014

RESPONSIBLE OFFICIAL: Associate Chief Information Officer, User & Network Services

CORRECTIVE ACTION MONITORING PLAN: We enter accepted corrective actions into the Joint Audit Management Enterprise System (JAMES) and monitor them on a monthly basis until completion.

RECOMMENDATION #5: Ensure that the KISAM-AM records are updated to correct the deficiencies identified in our review and provided to management.

CORRECTIVE ACTION #5: IRS agrees with this recommendation. We will perform data review and analysis to correct deficiencies identified by TIGTA and will update KISAM AM accordingly with current and complete information.

IMPLEMENTATION DATE: June 25, 2014

RESPONSIBLE OFFICIAL: Associate Chief Information Officer, User & Network Services

CORRECTIVE ACTION MONITORING PLAN: We enter accepted corrective actions into the Joint Audit Management Enterprise System (JAMES) and monitor them on a monthly basis until completion.

RECOMMENDATION #6: Ensure that the reconciliation process is effectively completed and have offices provide supporting documentation to the SACM organization for quality review.

CORRECTIVE ACTION #6: IRS agrees with this recommendation. We will implement and communicate process controls for follow-up actions with the responsible and accountable asset owners. We will utilize an Enterprise Governance Board to monitor compliance.

Attachment
Draft Audit Report – Weaknesses in Asset Management Controls Leave Information Technology Assets Vulnerable to Loss (Audit # 201220016)

IMPLEMENTATION DATE: September 25, 2014

RESPONSIBLE OFFICIAL: Associate Chief Information Officer, User & Network Services

CORRECTIVE ACTION MONITORING PLAN: We enter accepted corrective actions into the Joint Audit Management Enterprise System (JAMES) and monitor them on a monthly basis until completion.

RECOMMENDATION #7: Include additional data in the missing asset anomaly report (e.g., disposal information) to allow offices to resolve these assets.

CORRECTIVE ACTION #7: IRS agrees with this recommendation. We will develop a MISSING asset aging anomaly report including appropriate data fields to facilitate researching and resolving assets in a MISSING status.

IMPLEMENTATION DATE: January 25, 2014

RESPONSIBLE OFFICIAL: Associate Chief Information Officer, User & Network Services

CORRECTIVE ACTION MONITORING PLAN: We enter accepted corrective actions into the Joint Audit Management Enterprise System (JAMES) and monitor them on a monthly basis until completion.

RECOMMENDATION #8: Include dollar threshold criteria in the Certification Plan for certifying information technology assets with a high-dollar value that impact financial statement reporting.

CORRECTIVE ACTION #8: IRS agrees with this recommendation. We will update the FY14 and all future Inventory Certification plans to require that assets with an acquisition value of $50,000 or greater be verified and certified.

IMPLEMENTATION DATE: May 25,2014

RESPONSIBLE OFFICIAL: Associate Chief Information Officer, User & Network Services

CORRECTIVE ACTION MONITORING PLAN: We enter accepted corrective actions into the Joint Audit Management Enterprise System (JAMES) and monitor them on a monthly basis until completion.