TREASURY INSPECTOR GENERAL FOR TAX ADMINISTRATION

Access to Government Facilities and Computers Is Not Always Removed When Employees Separate

June 30, 2016

Reference Number: 2016-10-038

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.

Redaction Legend:
2 = Risk Circumvention of Agency Regulation or Statute

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.

HIGHLIGHTS

ACCESS TO GOVERNMENT FACILITIES AND COMPUTERS IS NOT ALWAYS REMOVED WHEN EMPLOYEES SEPARATE

Highlights

Final Report issued on June 30, 2016

Highlights of Reference Number: 2016-10-038 to the Internal Revenue Service Deputy Commissioner for Operations Support.

IMPACT ON TAXPAYERS

During Fiscal Year 2014, more than 4,100 full-time, permanent employees separated from the IRS, including 186 who separated during a pending disciplinary case (including criminal misconduct). It is important for the IRS to recover security items, such as Government identification, to prevent former employees from unauthorized entry to IRS facilities and workspaces, accessing IRS computers and taxpayer information, or potentially misrepresenting themselves to taxpayers.

WHY TIGTA DID THE AUDIT

The overall objective of this audit was to determine whether IRS management implemented policies and procedures designed to provide reasonable assurance that physical access to Government facilities is secure when employees separate from the IRS.

WHAT TIGTA FOUND

The IRS designed controls to verify that physical access to Government facilities is secured when employees separate. The controls include a computer process to document if security items are recovered from separating employees, including a third-party verification and deactivation of the returned item. However, these controls were not effective to prevent access to Government facilities and computers after employees separated.

Based on a random sample of Fiscal Year 2014 employee separations, TIGTA estimates that the IRS could not verify that all security items were recovered for more than 2,700 (66 percent) of the more than 4,100 employee separations. TIGTA also reviewed a judgmental sample of 10 employees who separated during a pending disciplinary case. The IRS could not verify the recovery of the security items for six of these employees and could not provide evidence that these cases were referred to the TIGTA Office of Investigations as required. When the IRS did not collect security items, some were later used to enter IRS buildings.

In addition, managers did not document all security items that should be recovered and listed some items for recovery that were not assigned to the separating employees. For example, 87 managers from our random sample of separated employees indicated former employees were issued keys; however, only one of these managers listed keys as a recoverable item. In addition, 65 managers indicated that non-enforcement pocket commissions were recovered, although records indicated that these items were never assigned to the employees.

WHAT TIGTA RECOMMENDED

TIGTA recommended that the Chief, Agency-Wide Shared Services, update separating employee clearance guidance; validate and inventory non-enforcement pocket commission assignments to employees; develop an inventory process to include documenting the issuance of manual keys and key cards and changing combination locks; and confirm that computer and building access is deactivated when an employee separates.

In their response, IRS management agreed with all the recommendations. The IRS plans to develop and implement a strategy to review and update current separating employee clearance policies and procedures; complete an inventory verification of non-enforcement pocket commissions; revise and implement key custody policies and procedures; and develop procedures to ensure the deactivation of computer and building access when identification cards are terminated and destroyed.

TREASURY INSPECTOR GENERAL
FOR TAX ADMINISTRATION

DEPARTMENT OF THE TREASURY

WASHINGTON, D.C. 20220

June 30, 2016

MEMORANDUM FOR DEPUTY COMMISSIONER FOR OPERATIONS SUPPORT

FROM: Michael E. McKenney
Deputy Inspector General for Audit

SUBJECT: Final Audit Report – Access to Government Facilities and Computers Is Not Always Removed When Employees Separate
(Audit # 201510018)

This report presents the result of our review to determine whether Internal Revenue Service (IRS) management implemented policies and procedures designed to provide reasonable assurance that physical access to Government facilities is secure when employees separate from the IRS. This review is included in the Treasury Inspector General for Tax Administration's Fiscal Year 2016 Annual Audit Plan and addresses the major management challenge of Security for Taxpayer Data and IRS Employees.

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

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 Gregory D. Kutz, Assistant Inspector General for Audit (Management Services and Exempt Organizations).

Table of Contents

Appendices

Abbreviations

AWSS	Agency-Wide Shared Services
FMSS	Facilities Management and Security Services
FY	Fiscal Year
ID	Identification
IRS	Internal Revenue Service
PDS	Personal Identity Verification Data Synchronization
TIGTA	Treasury Inspector General for Tax Administration

Background

During FY 2014, more than 4,100 full-time, permanent employees separated from the IRS.

During Fiscal Year (FY) 2014, the Internal Revenue Service (IRS) had more than 90,000 employees,[1] of which more than 4,100 were full-time, permanent employees who separated through retirement, resignation, death, *etc*. This includes 186 employees who separated during a pending disciplinary case (including criminal misconduct). Various security-related items[2] issued to employees that provide access to buildings and workspace, and items that are used for identification purposes, must be recovered from employees prior to the effective date of separation.

The Facilities Management and Security Services (FMSS)[3] office is responsible for delivering nationwide facilities and security services for the IRS. It provides and secures the physical locations where IRS employees conduct the day-to-day work of tax administration to meet the needs of American taxpayers. The IRS Enterprise Physical Access Control System[4] is the system that provides primary access control to IRS buildings and offices.

In FY 2006, the IRS began using the HR Connect Separating Employee Clearance Module[5] (hereafter referred to as the clearance module) to certify that assigned inventories of security items are recovered when employees separate from the IRS or to notate why an item is unrecoverable. The Separating Employee Clearance process is initiated when the employee, manager, or Human Resources Specialist submits a Personnel Action Request[6] involving the separation of an employee, which generates a clearance module record upon approval. Managers are responsible for entering into the clearance module security-related items that departing employees should return and indicating when, where, and how the items will be returned. The

[1] Human Resources Reporting Center Population Report for FY 2014, including seasonal employees.
[2] Security items include Smart identification cards, non-enforcement pocket commissions, and keys.
[3] The FMSS is part of the Agency-Wide Shared Services office.
[4] The primary system used for access control to IRS facilities. The system uses the Hirsch Identive Velocity™ suite of commercial off-the-shelf application database software. Examples of other systems used include the General Electric Picture Perfect Access Control™ software and other systems when the IRS is co-located in General Services Administration managed buildings.
[5] The Separating Employee Clearance Module is part of the Department of the Treasury's HR Connect system. HR Connect provides managers with the ability to access basic data for employees they supervise, initiate awards and other personnel actions, manage positions by reviewing detailed information about authorized staffing, and initiate recruitment actions.
[6] Personnel Action Requests are used to initiate and document employee events such as job reclassification, promotions, name changes, and retirements.

approved record will move to a third-party work list for confirmation that the items were recovered.

There is an additional security risk when an employee separates under adverse conditions. These situations require managers to follow additional procedures to verify that security items are retrieved from the separated employee. When an employee is terminated for an adverse reason, managers are required to notify the local FMSS office immediately to deactivate building access and to provide immediate alert status to security guards. Once the manager updates the clearance module record with estimated return information, or that a security item is unrecoverable, the process for retrieving the security items may vary. If the manager cannot recover a separating employee's identification card, a report should be submitted explaining the circumstances of the non-recovery. The report is sent to the local servicing security office and, when appropriate (*e.g.*, forced termination), a copy is sent to the Situation Awareness Management Center and the Treasury Inspector General for Tax Administration's (TIGTA) Office of Investigations.

This review was performed at the Agency-Wide Shared Services (AWSS) Office of Employee Support Services in Cincinnati, Ohio, and the AWSS FMSS offices in Washington, D.C.; Atlanta, Georgia; Kansas City, Missouri; and Nashville and Memphis, Tennessee, during the period June 2015 through February 2016. 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.

Results of Review

The IRS designed controls to verify that physical access to Government facilities is secured when employees separate. The controls include a computer process to document security items that should be recovered from separating employees, including a third-party verification and deactivation of the returned item, if required.[7] In addition, IRS management is required to retain documentation supporting the recovery of security items.

The IRS does not offer a comprehensive Separating Employee Clearance training course addressing the requirements for obtaining security items from separating employees for new or experienced managers. However, we found information resources were available. For example, a clearance module overview is available through a payroll newsletter and leaders' alerts, which are posted to the IRS intranet site. The Separating Employee Clearance help desk also hosts a monthly teleconference in which managers can ask questions about the process and discuss the Separating Employee Clearance manager's handbook, which is available on the Employee Resources Center.

Despite these efforts, we found that controls to provide reasonable assurance that access to Government facilities and computers are protected after employees separate were either not functioning as intended or not always followed in FY 2014. It is important for the IRS to recover security items, such as Government identification, to prevent former employees from unauthorized entry to IRS facilities and workspaces, accessing IRS computers and taxpayer information, or potentially misrepresenting themselves to taxpayers.

Appropriate Actions Were Not Always Taken to Prevent Access to Government Facilities and Computers After Employees Separate

Based on our review of a stratified random sample of clearance module records for FY 2014 employee separations,[8] we estimate that the IRS cannot verify that all security items were recovered for 2,733 (66 percent)[9] of the more than 4,100 employee separations.[10] In

[7] Smart identification cards require deactivation to prevent their future use for access to IRS buildings and computers.
[8] See Appendix I for our sampling methodology.
[9] The point estimate projection is based on a two-sided 95 percent confidence interval. We are 95 percent confident that the point estimate is between 2,302 and 3,165.
[10] There were 165 of 200 employees with at least one (some employees had more than one) security item not verified as recovered. See Appendix V for more detail.

addition, based on our review of this same sample, we estimate that the clearance module records are inaccurate or unreliable for 2,060 employees (50 percent).[11]

We also reviewed a judgmental sample[12] of 10 employees who separated during a pending disciplinary case, two of which separated after criminal charges were filed. The IRS could not verify the recovery of all security items for six of the 10 employees and determined that security items were missing for one of the employees. In addition, the IRS could not provide evidence that these cases were referred to the TIGTA Office of Investigations,[13] as required by the Internal Revenue Manual.

We believe these issues may have occurred because the clearance module does not contain an inventory of security items assigned to employees that should be recovered on departure. Also, 1) managers change roles frequently and are often not in the same position as when security items were issued, 2) the separation process has not been updated in the Internal Revenue Manual, 3) managers may not refer to the payroll newsletters and e-mail alerts, and 4) the timing of the monthly teleconferences may not be convenient when managers need to use the clearance module and other controls.

Details concerning issues we found for smart identification cards (hereafter referred to as Smart ID cards), non-enforcement pocket commissions, and keys and combination locks are described in the following sections of the report. During the audit, we notified IRS executive management of several of the security issues we identified and they immediately began to take corrective action.

Some Smart ID cards were used to access IRS facilities after employees no longer worked for the IRS.

Source: fedidcard.gov

Smart ID cards

A Smart ID card is a personal identity verification credential that is issued to eligible IRS employees and contractors. It is used by IRS employees to access IRS computers and some IRS buildings.

When employees separate from the IRS, if security items such as Smart ID cards are not returned or deactivated in USAccess[14] or

[11] The point estimate projection is based on a two-sided 95 percent confidence interval. We are 95 percent confident that the point estimate is between 1,618 and 2,503. There were 126 of 200 employees with at least one record in the clearance module (for various security items) inconsistent with third-party documentation (some employees had more than one inconsistent security item). The security item clearance module records inconsistent with third-party documentation include the following: eight Smart ID cards; 74 pocket commissions; 23 key cards (all types); and, 89 manual keys.

[12] A judgmental sample is a nonprobability sample, the results of which cannot be used to project to the population.

[13] The TIGTA Office of Investigations had no records of referrals from the IRS for the six cases.

[14] A General Services Administration program that the IRS uses to facilitate Smart ID card issuance, maintenance, and lifecycle management.

the local access control software,[15] the separated employee may still access IRS buildings, offices, or computers.

Based on our random and judgmental samples, we determined that: 1) Smart ID cards are generally marked returned in the clearance module, but we could not verify that Smart ID cards were actually recovered; 2) Smart ID cards are not destroyed timely; 3) *******2******* ***************************2***********************; and 4) some Smart ID cards were used to access IRS facilities after employees had separated.

<u>Smart ID cards are generally marked returned in the clearance module, but we could not verify that ID cards were actually recovered</u>

IRS management relies on the clearance module as a tool to input Smart ID cards that need to be recovered when employees separate and to certify that the Smart ID cards are recovered. Clearance module records show that the IRS recovered 195 Smart ID cards[16] for our random sample of 200 employees who separated from the IRS in FY 2014. For the remaining five Smart ID cards, three were listed as unrecoverable and two had no records in the clearance module.

To verify that Smart ID cards were physically recovered, we compared the information in the clearance module to USAccess. We noted that USAccess had similar information to the clearance module on the recovery of Smart ID cards from our sample.[17] We also noted that many of the Smart ID cards from our sample of separated employees were marked as destroyed in the USAccess system.

IRS security personnel initially stated that they must have physical possession of the Smart ID card and insert it into the Credential Inventory Tool[18] to mark it as destroyed. However, during a subsequent site visit, a security specialist demonstrated her standard operating procedure in which, without inserting a Smart ID card into the Credential Inventory Tool, she directly accessed the USAccess computer system and marked Smart ID cards as “destroyed.” As such, IRS security personnel were incorrect; possession of a Smart ID card and use of the Credential Inventory Tool is not necessary for marking the card as destroyed. In addition,

[15] Smart ID cards are marked “terminated” in USAccess when all certificates have been revoked. They are then marked “destroyed” within USAccess to indicate that the Smart ID card has been physically destroyed. At this point, the recovered Smart ID card should be physically shredded or otherwise destroyed. IRS security specialists should then ensure that building access is removed from the local access control software.

[16] We determined through review of supporting documentation that three of the 195 Smart ID cards were listed as returned when they were not.

[17] USAccess records for our random sample of 200 separated employees indicated 196 Smart ID cards were returned, instead of the 195 accounted for in the clearance module.

[18] An accessory to USAccess that provides the ability to check in credentials when they are received on site from either the Card Production Facility or from another site and allows a Credential Ready for Pickup email to be sent to the applicant. The portal also allows role holders to mark credentials as destroyed in the system.

two Smart ID cards that were marked as terminated or destroyed in the USAccess system were later used to access the IRS Headquarters building.[19] Therefore, we question whether all Smart ID cards were physically recovered, as required.

We also selected a judgmental sample of 10 employees who separated under adverse circumstances. We found that the Smart ID card for one of these employees, who had been indicted on criminal charges, had not been recovered. The IRS was unaware the Smart ID card was not recovered because the manager stated he did not receive a notification that a clearance module record had been created for this employee. Additional information could not be provided on attempts to recover the Smart ID card, and the TIGTA Office of Investigations did not have a record that this had been referred for investigation as required by the Internal Revenue Manual.

Smart ID cards are not destroyed timely

According to the USAccess Program Personal Identification Verification Credential Issuer Operations Plan, IRS management must destroy Smart ID cards within 30 days of separation and, according to the Internal Revenue Manual, Smart ID cards must be destroyed within 18 hours of receipt at a local security office. However, we determined that Smart ID cards were not always destroyed timely, as required.

Our random sample of 200 employees who separated from the IRS in FY 2014 had a Smart ID card with the following statuses in USAccess: 152 were destroyed; 45 were terminated; and three records were unavailable at the time of our fieldwork.[20] For the 152 Smart ID cards that were marked as destroyed in our sample of 200 separated employees, we found that Smart ID cards were destroyed an average of 79 days after the employee separated, ranging from the day of separation up to 634 days after the employee separated. We determined 71 were marked as destroyed within 30 days of the separation, 71 were destroyed between 31 and 365 days after the separation, and 10 were destroyed after more than one year. Seven Smart ID cards tested in one office were marked as destroyed more than 400 days after the employees' separation date, and the destruction occurred within one week of our initial contact with this office to schedule a site visit.

USAccess records did not include information for timeliness of destruction for 44 Smart ID cards with a status of "terminated" from our random sample. Although the clearance module listed 43 of the 44 Smart ID cards as returned, we found that 35 Smart ID cards were from an office that bypassed the requirement for destruction in USAccess by inputting the card on a manual

[19] Further details are provided later in this report.
[20] During fieldwork, IRS management informed us that USAccess documentation was not available for three employees; two were unrecoverable; and one Smart ID card was never issued. IRS management provided documentation for one of the three separated employees, but it was incorrect because it was for a different employee with the same name.

spreadsheet to be "terminated" at a later date; seven Smart ID cards in a second office were terminated and no reason was provided for not destroying the ID cards; and manual documentation was provided to support that two Smart ID cards were physically shredded. During the audit, we notified IRS executive management of this issue and as a result, FMSS Associate Directors confirmed on February 17, 2016, that they identified and physically destroyed more than 300 Smart ID cards they had in their possession as of February 9, 2016.

<u>************************************2****************************</u>**
<u>*****2******</u>**

**************************************2***********************************
**************************************2*********************************
**************************************2*******************************
**************************************2*************************************
**************************************2**************************************
**************************************2***********************************
**************************************2*********************************
**************************************2**************************************.
**************************************2**************************************
**************************************2*********************************
**************************************2**************************************
**************************************2***********.

**************************************2****************************,
**************************************2*************************************
**************************************2************************************
**************************************2***********************************
**************************************2***********************.[21]

<u>Some Smart ID cards were used to access IRS facilities after employees had separated</u>

We discovered that two Smart ID cards ********************2*****************
2* were later used to access IRS facilities after employees had separated. We also determined that two additional Smart ID cards ***************2*****************
*********2*********were used to access Government facilities after employees had separated from the IRS.

We reviewed information from the Hirsch Identive Velocity™ system and the General Electric Picture Perfect Access Control™ software to determine the last time Smart ID cards belonging to

[21] The point estimate projection is based on a two-sided 95 percent confidence interval. We are 95 percent confident that the point estimate is between six and 56. See Appendix IV.

the separated employees in our sample were used to enter two of four IRS buildings.[22] IRS electronic access logs show that four Smart ID cards belonging to former IRS employees were used to access the IRS Headquarters, after the employees' separation date. Although no security incidences were reported, there are nearly 2,000 employees[23] who work in this building and there are also very sensitive records located there.

IRS employees access the IRS Headquarters by scanning the Smart ID card on an electronic reader, and an electronic record is maintained of the access time and date. Review of available information for the four employees revealed the following:

- Clearance module records indicate that the Smart ID cards were recovered for all four employees, even though the cards were later successfully used to enter the IRS Headquarters building.
- The four employees' Smart ID cards were used three days to more than five months after the employees' separation dates.
- IRS management provided documentation showing eventual recovery for two of the four Smart ID cards, but could not support recovery of the remaining two Smart ID cards.
- Documentation for two recovered Smart ID cards indicate that ******2****** **********************************2**.
- One Smart ID card that was used three days after the employee's separation date belonged to an employee who also still had a laptop computer assigned to him or her nearly three months after his or her separation, therefore increasing the risk that he or she may have maintained access to taxpayer information.

Non-enforcement pocket commissions

Pocket commissions are designed to provide evidence of the holder's specific authority and responsibility when contacting the public outside of IRS facilities or when conducting U.S. Government business with Federal, State, local, or foreign officials as authorized. Non-enforcement pocket commissions do not provide electronic access to IRS facilities; however, they are used to show evidence of authority and can allow a holder to misrepresent themselves to taxpayers or other Government officials.

Similar to Smart ID cards, the clearance module is used to certify that non-enforcement pocket commissions are recovered. First, the manager certifies in the clearance module when the non-enforcement pocket commission is recovered from the employee. The commission is then

[22] We were unable to test the last accesses of employees in the remaining two of four buildings because this information was not maintained, as required by the Internal Revenue Manual.
[23] This figure does not take into consideration employees not in the office or visitors to the office.

sent to the Area Processing Center where a specialist certifies that it was received and destroyed (or retired) to prevent unauthorized use. However, confusion on the part of managers of separating employees when approving pocket commission records and the lack of a reliable inventory of pocket commissions make it difficult to determine how many non-enforcement pocket commissions should have been returned and how many pocket commissions were returned when employees separated.

We could not verify how many pocket commissions should have been returned or were returned by separated employees.

Source: gpo.gov

The clearance module indicated that 75 of our 200 sampled employees had non-enforcement pocket commissions (73 were recovered and two were unrecoverable). However, the Personal Identity Verification Data Synchronization (PDS) system[24] used by the IRS to control the inventory of pocket commissions showed that only 13 of these 200 employees actually were issued pocket commissions. PDS records did not exist for 65 of the 73 employees for which a pocket commission was indicated as recovered in the clearance module, which indicates that pocket commissions were never assigned to these employees. Although IRS management relied on the clearance module to verify that non-enforcement pocket commissions were returned, we determined that the clearance module was inaccurate. IRS management was unaware that the status of the non-enforcement pocket commissions was incorrect in the clearance module.

IRS management also stated that non-enforcement pocket commission information in the PDS was not reliable or up-to-date, even though the PDS is the authoritative source of pocket commission information. According to management, this occurred because of limited staffing needed to manually enter the information from prior inventory records. The PDS was implemented in September 2013 and, prior to that, the IRS maintained inventories of pocket commission records on Excel spreadsheets. We reviewed these spreadsheets and found four additional employees in our random sample that had a pocket commission record in one of the prior spreadsheets, but not in the PDS. Based on this review, we estimate that 318 employees had inaccurate or unreliable PDS records.[25]

IRS management stated that the clearance module may have been incorrect because some managers may not understand what a pocket commission is, and may select "returned" instead of "not applicable" in the required pocket commission field of the clearance module. In addition, IRS management stated that some security specialists may have incorrectly entered "returned" into the clearance module without verifying receipt of the non-enforcement pocket commission.

[24] The PDS is a feature within the HR Connect system used to process identity data for IRS employees.
[25] The point estimate projection is based on a two-sided 95 percent confidence interval. We are 95 percent confident that the point estimate is between 30 and 605. See Appendix IV.

Keys and combination locks

Local procedures for manual keys, key cards, and combination locks were not effective to account for employees who were assigned keys or provided lock combinations and assure recovery of the keys and changing of combination locks after the employee's separation. This may have occurred because of a decentralization of controls from the national level to the local level.

In the past, controls over the issuance and recovery of keys and key cards were implemented at the national level. IRS managers were required to document the issuance and account for office keys and key cards on Form 1930, *Custody Receipt for Government Property*. In addition, annual key and key card audits were performed to assure the effectiveness of these controls. However, Form 1930 was declared obsolete in FY 2011 and local offices were told they could develop their own documentation for tracking key inventories. Third-party annual key audits were discontinued in August 2012. IRS management explained that offices were to implement local procedures at this time as a compensating control.

Recovering keys and changing combinations is important, even when the IRS may have recovered a separated employee's Smart ID card. This is because the IRS sometimes occupies public buildings with other tenants where a former employee can still gain access to the building and can use keys or combinations they had retained to access IRS space, if locks or combinations were not changed.

Manual keys

Manual keys are used to access some buildings and offices. Managers are required to input manual keys in the list of recoverable items in the clearance module and track if keys are recovered. However, managers did not understand their responsibility of recording the retrieval of keys in the clearance module. For example, according to the clearance module, one of our 200 sampled employees had a key that was listed as recovered. However, in responses to a questionnaire sent to managers of the 200 sampled employees, 87 managers indicated that their former employee had been assigned a secure office or workspace key that should have been recovered.[26] Of the 87 former employees, managers confirmed that 19 keys were recovered but could not account for the remaining 68 keys.

IRS officials could not confirm that former employees returned manual keys and key cards or that the IRS changed combination locks after employees separated.

[26] Twenty-six managers did not respond to this question.

Key cards

Key cards are used to access some buildings and secure offices, but differ from building to building. Managers are required to input a key card (if applicable) in the list of recoverable items in the clearance module and track if the key card was recovered. According to the clearance module, 186 of our 200 sampled employees had an electronic key card (183 recovered and three unrecoverable). However, in responses to a questionnaire sent to managers of the 200 sampled employees, managers stated that 94 key cards were not returned, 74 key cards were returned, and eight were found to be not applicable.[27] In response to the questionnaire, some managers indicated that a key card was returned; however, they provided documentation that supported only the return of a Smart ID card. This may indicate that some managers are confused with the term "key card."

Combination locks

If an employee separates who knows the combination to a door lock, the manager is required to submit a request to the local security office to have the combination changed. The disabling of lock combinations are not entered into the clearance module for separated employees and no universal inventory of lock combinations was available. However, based on a questionnaire we sent to managers of the random sample of 200 separated employees, 35 managers responded that their former employees were issued lock combinations.[28] IRS management and security office personnel provided documentation supporting the change of the combination after the employee separated for five of the 35 employees. The IRS could not verify that combinations were changed for the remaining 30 separated employees. In a separate judgmental sample, another employee (who was under investigation for criminal misconduct) had combination access to a workspace, according to the employee's manager. However, the IRS did not provide documentation to verify that the combination lock was changed when the employee separated.

Recommendations

The Chief, AWSS, should:

Recommendation 1*:* Review and update the current Separating Employee Clearance policies, procedures, and controls, including the Internal Revenue Manual, and provide comprehensive training on the updated procedures to managers and security personnel. This should include periodic reminders and highlights of the risk of Separating Employee Clearance procedures not being followed.

[27] Twenty-four managers did not respond to this question.

[28] For the remaining separated employees, 130 managers indicated no lock combinations were issued, 32 managers did not respond to this question, and 3 managers were unsure if a lock combination was issued.

Management's Response: IRS management agreed with the recommendation and stated that the Chief, AWSS, will ensure the development and implementation of a strategy to review and update current Separating Employee Clearance policies, procedures, and controls, including the Internal Revenue Manual, related to the recovery of security-related items, access revocation, card termination and destruction, ID Cards, manual keys, key cards, and other security-related items. The IRS also stated that FMSS managers and security personnel will receive comprehensive training on the updated procedures as well as periodic reminders.

Recommendation 2*:* Perform an inventory verification of non-enforcement pocket commissions assigned to IRS employees and update and maintain the PDS.

Management's Response: IRS management agreed with the recommendation and stated that the Chief, AWSS, will complete an inventory verification of non-enforcement pocket commissions assigned to IRS employees and update and maintain the PDS.

Recommendation 3: Develop an inventory process to include documenting the issuance of manual keys and key cards and changing combination locks so managers will know security items that need to be recovered or combinations that need to be changed during employee separations.

Management's Response: IRS management agreed with the recommendation and stated that the Chief, AWSS, will revise and implement current FMSS key custody policies and procedures. According to the IRS, the procedures will include documentation of issuance of manual keys and key cards. The recovery of manual keys and key cards and combination lock changes due to employee separations will also be included.

Recommendation 4: Coordinate with the IRS Information Technology office to review the process to confirm that computer and building access is deactivated *********2********* ****************************2****************************.

Management's Response: IRS management agreed with the recommendation and stated that the Chief, AWSS, will coordinate with the IRS Information Technology office to review the process and develop procedures to ensure the deactivation of computer and building access ***************************2****************************** ********2*********.

Appendix I

Detailed Objective, Scope, and Methodology

Our overall objective was to determine whether IRS management implemented policies and procedures designed to provide reasonable assurance that physical access to Government facilities is secure when employees separate from the IRS. To accomplish this objective, we:

I. Assessed whether controls were designed to provide reasonable assurance that physical access to Government facilities was secured when employees separated from the IRS.

   A. Reviewed the Internal Revenue Manual and held discussions with IRS management to identify controls for retrieving physical security items from separated employees, including: Smart ID cards, non-enforcement pocket commissions, and keys.

   B. Interviewed AWSS office management and reviewed documentation to determine how IRS management used the clearance module to record the receipt of: Smart ID cards, non-enforcement pocket commissions, and keys.

   C. Interviewed FMSS office management and reviewed documentation to determine procedures the Security Sections used to monitor whether managers returned retrieved physical security items or recorded those that were non-recoverable, including: Smart ID cards, non-enforcement pocket commissions, and keys.

   D. Determined how the requirements for retrieving physical security items from separated employees were communicated to IRS management, including IRS-wide memorandums and training provided to IRS managers.

II. Determined whether designed controls were functioning and provided reasonable assurance that physical access to Government facilities was secured when employees separated from the IRS.

   A. Obtained a download of the Treasury Integrated Management Information System Separated Employee file and determined that the data were reliable for our purpose by validating that the date fields contained dates, name fields contained names, *etc.*, and by matching a sample of records to the HR Connect Separating Employee Clearance Module records. We identified more than 4,100 former full-time, permanent IRS employees and their building locations, excluding Chief Counsel and Criminal Investigations employees,[1] who separated during FY 2014.

B. Selected a stratified random sample of 200 from the more than 4,100 former full-time, permanent IRS employees, excluding Chief Counsel and Criminal Investigations employees, who separated from the IRS during FY 2014.[2] We used the following criteria: 95 percent confidence level, 10 percent expected error rate, and ±5 percent precision rate. The sample included separated employees from four buildings: one processing center (Kansas City, Missouri); one office with more than 70 separations (Washington, D.C.); one office with 25-70 separations (Atlanta, Georgia); and one office with less than 25 separations (Nashville, Tennessee).

C. Identified a judgmental sample[3] of employees from the more than 4,100 former full-time, permanent IRS employees who separated under adverse conditions[4] by matching the Social Security Numbers from the separated employees for the four buildings that were included in the statistical sample and the Memphis Area Processing Center location to the Automated Labor and Employee Relations Tracking System. We performed key word searches (*e.g.*, criminal, drugs, fraud, theft) and identified 10 egregious, adverse separations.

D. Matched the 200 employees in the random sample and the 10 employees in the judgmental sample to the clearance module. We determined if physical security items including: Smart ID cards, non-enforcement pocket commissions, and manual keys were recovered and whether proper documentation was provided to support recovery, if applicable. If the physical security item was returned, requested inventory destruction records from the appropriate security office.

E. Reviewed manager comments entered into the clearance module and requested the following: report provided to the local Security Section explaining the circumstances of the non-recoverable items; documentation of the referral to the TIGTA Office of Investigations; and the Situation Awareness Management Center lost/stolen report for physical security items that were not returned. We requested the results of the

[1] Chief Counsel and Criminal Investigations were excluded because they use a different process for separating employees.

[2] A contract statistician assisted with developing the sampling plans and projections.

[3] A judgmental sample is a nonprobability sample, the results of which cannot be used to project to the population.

[4] Adverse conditions include a removal disposition code (*e.g.*, probation/separation, termination for job abandonment) of an employee with a pending conduct or performance issue in the Automated Labor and Employee Relations Tracking System. Disposition codes 015, 016, 017, 018, 116, 117, and 118 in the Automated Labor and Employee Relations Tracking System were used to identify adverse separations.

investigation in the Performance and Results Information System[5] for non-recoverable physical security items that were referred to the TIGTA Office of Investigations.

F. Sent a questionnaire to managers of the 200 employees in the random sample and the 10 employees in the judgmental sample to determine if key cards and keys were returned by separating employees, and if combination locks were changed.

G. Determined if the Smart ID cards for the employees included in the random sample were used to access an IRS building after the employee's effective separation date, and that all Smart ID cards were recovered from separated employees.

H. Determined if combination locks had been changed after employees separated. If individual combinations were assigned, reviewed the access log for attempted access after the effective date of separation.

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: IRS policies, procedures, and practices for retrieving security items from separated employees. We evaluated these controls by reviewing separation records and documentation supporting the retrieval of the security items, sending questionnaires to managers about recovered items, and interviewing management about actions taken when items were not returned for selected employees who separated during FY 2014. We also reviewed building access logs to determine if Smart ID cards for the employees included in the random sample were used to access IRS buildings after the employee's effective separation.

[5] The primary management information system for TIGTA's Office of Investigations. It provides TIGTA the managerial ability to account for and track all leads developed by TIGTA, all complaints received from external sources, and all investigations initiated as a result of internal and external allegations.

Appendix II

Major Contributors to This Report

Gregory D. Kutz, Assistant Inspector General for Audit (Management Services and Exempt Organizations)
Troy D. Paterson, Director
Gerald T. Hawkins, Audit Manager
Melinda H. Dowdy, Lead Auditor
Catherine R. Sykes, Auditor

Appendix III

Report Distribution List

Commissioner
Office of the Commissioner – Attn: Chief of Staff
Deputy Commissioner for Operations Support
Deputy Commissioner for Services and Enforcement
Chief, Agency-Wide Shared Services
Acting Director, Employee Support Services, Agency-Wide Shared Services
Acting Director, Facilities Management and Security Services, Agency-Wide Shared 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; 2,060[1] employees with inaccurate or unreliable clearance module records (see page 3).

Methodology Used to Measure the Reported Benefit:

We reviewed a statistically valid stratified random sample of clearance module records for 200 of 4,158 full-time, permanent IRS employees who separated during FY 2014, excluding Chief Counsel and Criminal Investigations employees,[2] and compared the records to third-party documentation (including PDS, USAccess, and responses to a manager questionnaire). We determined that the third-party documentation was inconsistent with the information presented in the clearance module for 126[3] of the 200 employees. To estimate the total number of exceptions based on the sample error rate, we used the following methodology. We stratified the population into four strata and determined the percent of population by strata. The population was then adjusted by a Finite Population Correction Factor and the Observed Exception rate was calculated by strata and office and projected across the population. See Figure 1 for more details.

[1] The point estimate projection is based on a two-sided 95 percent confidence interval. We are 95 percent confident that the point estimate is between 1,618 and 2,503.

[2] Chief Counsel and Criminal Investigations were excluded because they use a different process for separating employees.

[3] There were 126 of 200 employees with at least one clearance module security item record inconsistent with third-party documentation (some employees had more than one). The number of clearance module records (for various security items) inconsistent with third-party documentation include the following: eight Smart ID cards; 74 pocket commissions; 23 key cards (all types); and 89 manual keys.

Figure 1: Exception Summary by Building Type (Strata)

Building Type	Population by Building Type	Exception Percentage	Estimated Number of Exceptions
Small Facility	1,826	48 [4]	873
Medium Facility	1,350	40	540
Large Facility	402	100	402
Large Processing Center	580	42 [5]	245
Total Estimated Number of Exceptions:			**2,060**

Source: Statistical projection of the results of our analysis.

Type and Value of Outcome Measure:

Reliability of Information – Potential; 318[6] employees with inaccurate or unreliable PDS records (see page 3).

Methodology Used to Measure the Reported Benefit:

We reviewed a statistically valid stratified random sample of clearance module records for 200 of 4,158 full-time, permanent IRS employees, excluding Chief Counsel and Criminal Investigations employees, who separated during FY 2014 and compared the records to the PDS to determine if the assigned pocket commissions had been returned. We also reviewed the Excel spreadsheets that were used to track pocket commission inventory prior to the PDS and identified four employees who had been issued pocket commissions with no record in the PDS. To estimate the total number or exceptions based on the sample error rate, we used the following methodology. We stratified the population into four strata and determined the percent of population by strata. The population was then adjusted by a Finite Population Correction Factor and the Observed Exception rate was calculated by strata and office and projected across the population. The four exceptions were from the small facility stratum, resulting in a 17 percent[7] exception rate for that stratum. When applied to the small facility population of 1,826, the result is 318 employees.

[4] This percentage has been rounded from 47.83 percent.
[5] This percentage has been rounded from 42.25 percent.
[6] The point estimate projection is based on a two-sided 95 percent confidence interval. We are 95 percent confident that the point estimate is between 30 and 605.
[7] This percentage has been rounded from 17.39 percent.

Type and Value of Outcome Measure:

Taxpayer Privacy and Security – Potential; 31[8] employees who did not return their Smart ID cards prior to separation and potentially maintained access to IRS facilities and taxpayer information (see page 3).

Methodology Used to Measure the Reported Benefit:

We reviewed building last access information for a statistically valid stratified random sample of 200 of 4,158 full-time, permanent IRS employees, excluding Chief Counsel and Criminal Investigations employees, who separated during FY 2014.

- We identified that Smart ID cards for four employees were used to access the IRS National Headquarters building after their separation date; therefore, these Smart ID cards were still in use after the employees' separation.
- We identified one employee in the IRS Kansas City Campus whose Smart ID card was not recovered.

To estimate the total number or exceptions based on the sample error rate, we used the following methodology. We stratified the population into four strata and determined the percent of population by strata. The population was then adjusted by a Finite Population Correction Factor and the Observed Exception rate was calculated by strata and office and projected across the population. The four exceptions from the large facility stratum resulted in a 6 percent[9] exception rate for that stratum. When applied to the large facility population of 402, the result is 23 employees. The one exception from the large processing center stratum resulted in a 1 percent[10] exception rate for that stratum. When applied to the large processing center population of 580, the result is 8 employees.

[8] The point estimate projection is based on a two-sided 95 percent confidence interval. We are 95 percent confident that the point estimate is between six and 56.
[9] This percentage has been rounded from 5.63 percent.
[10] This percentage has been rounded from 1.41 percent.

Appendix V

Estimate of Employees With an Unrecovered Security Item

This appendix presents detailed information and the methodology used to estimate the number of employees with at least one security item that the IRS could not verify as recovered.

Based on our review of a stratified random sample of clearance module records for FY 2014 employee separations,[1] we estimate that the IRS cannot verify that all security items were recovered for 2,733 (66 percent)[2] of the more than 4,100 employee separations. We reviewed a statistically valid stratified random sample of clearance module records for 200 of 4,158 full-time, permanent IRS employees who separated during FY 2014, excluding Chief Counsel and Criminal Investigations employees,[3] and compared the records to third-party documentation (including PDS, USAccess, and responses to a manager questionnaire). There were 165 of 200 employees with at least one security item not verified as recovered (some employees had more than one inconsistent security item).

To estimate the total number of exceptions based on the sample error rate, we used the following methodology. We stratified the population into four strata and determined the percent of population by strata with at least one security item not verified as returned. The population was then adjusted by a Finite Population Correction Factor and the Observed Exception rate was calculated by strata and office and projected across the population. See Figure 1 for more details.

[1] See Appendix I for our sampling methodology.

[2] The point estimate projection is based on a two-sided 95 percent confidence interval. We are 95 percent confident that the point estimate is between 2,302 and 3,165.

[3] Chief Counsel and Criminal Investigations were excluded because they use a different process for separating employees.

Figure 1: Exception Summary by Building Type (Strata)

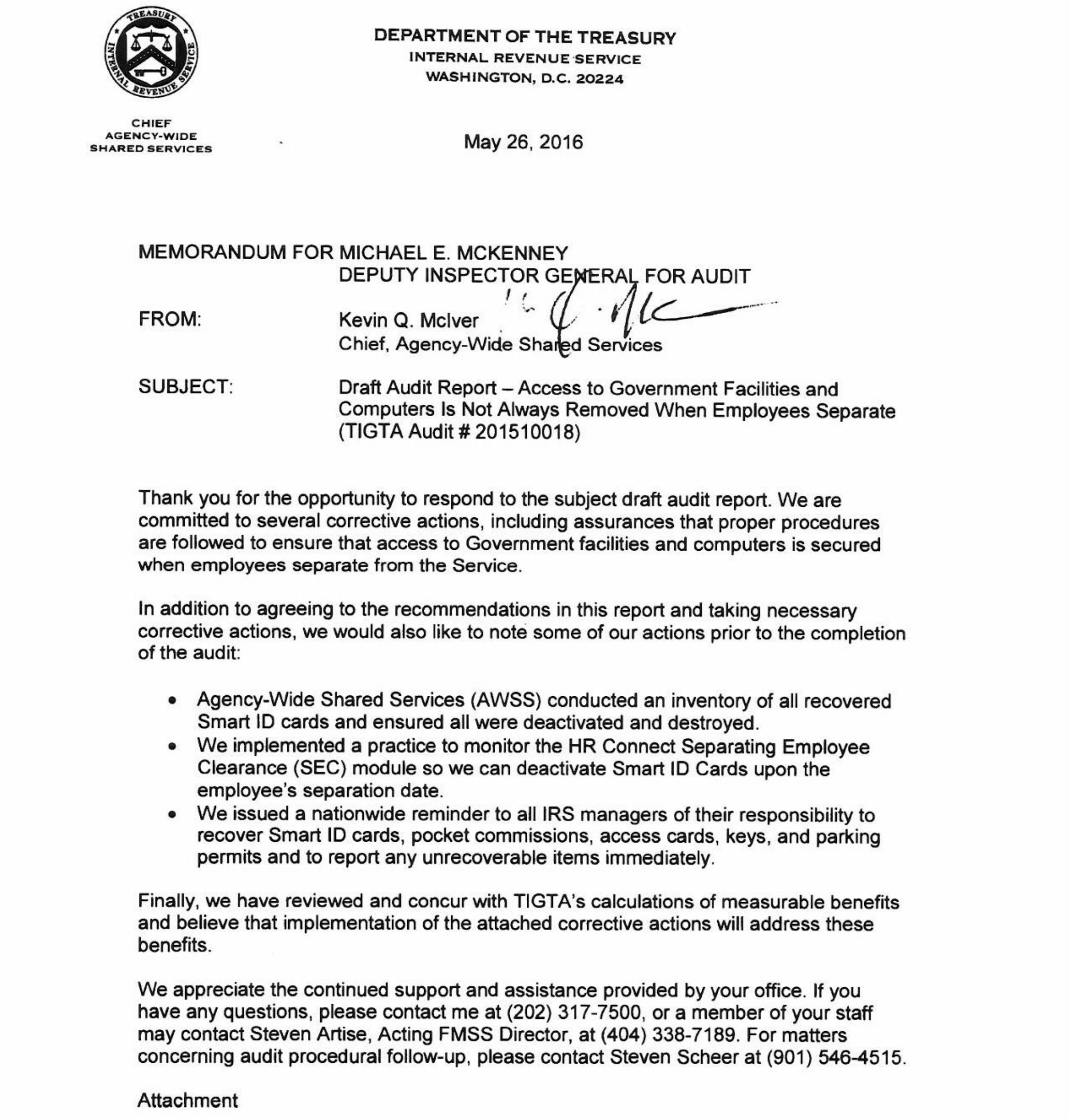
Building Type	Population by Building Type	Exception Percentage	Estimated Number of Exceptions
Small Facility	1,826	48[4]	873
Medium Facility	1,350	71[5]	964
Large Facility	402	89[6]	357
Large Processing Center	580	93[7]	539
Total Estimated Number of Exceptions:			**2,733**

Source: Statistical projection of the results of our analysis.

[4] This percentage has been rounded from 47.83 percent.
[5] This percentage has been rounded from 71.43 percent.
[6] This percentage has been rounded from 88.73 percent.
[7] This percentage has been rounded from 92.96 percent.

Appendix VI

Management's Response to the Draft Report



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

CHIEF
AGENCY-WIDE
SHARED SERVICES

May 26, 2016

MEMORANDUM FOR MICHAEL E. MCKENNEY
DEPUTY INSPECTOR GENERAL FOR AUDIT

FROM: Kevin Q. McIver
Chief, Agency-Wide Shared Services

SUBJECT: Draft Audit Report – Access to Government Facilities and Computers Is Not Always Removed When Employees Separate (TIGTA Audit # 201510018)

Thank you for the opportunity to respond to the subject draft audit report. We are committed to several corrective actions, including assurances that proper procedures are followed to ensure that access to Government facilities and computers is secured when employees separate from the Service.

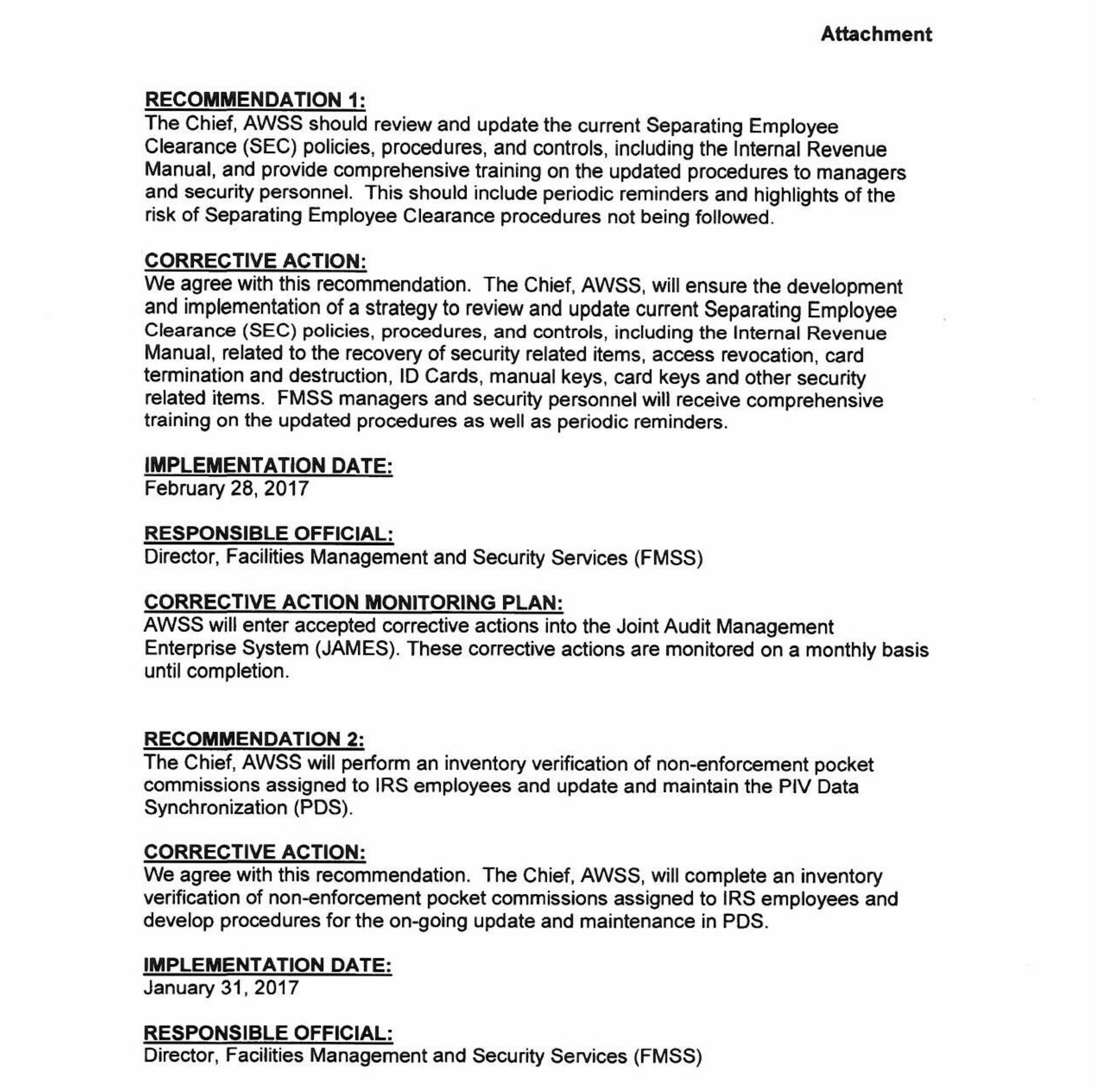
In addition to agreeing to the recommendations in this report and taking necessary corrective actions, we would also like to note some of our actions prior to the completion of the audit:

- Agency-Wide Shared Services (AWSS) conducted an inventory of all recovered Smart ID cards and ensured all were deactivated and destroyed.
- We implemented a practice to monitor the HR Connect Separating Employee Clearance (SEC) module so we can deactivate Smart ID Cards upon the employee's separation date.
- We issued a nationwide reminder to all IRS managers of their responsibility to recover Smart ID cards, pocket commissions, access cards, keys, and parking permits and to report any unrecoverable items immediately.

Finally, we have reviewed and concur with TIGTA's calculations of measurable benefits and believe that implementation of the attached corrective actions will address these benefits.

We appreciate the continued support and assistance provided by your office. If you have any questions, please contact me at (202) 317-7500, or a member of your staff may contact Steven Artise, Acting FMSS Director, at (404) 338-7189. For matters concerning audit procedural follow-up, please contact Steven Scheer at (901) 546-4515.

Attachment



Attachment

RECOMMENDATION 1:
The Chief, AWSS should review and update the current Separating Employee Clearance (SEC) policies, procedures, and controls, including the Internal Revenue Manual, and provide comprehensive training on the updated procedures to managers and security personnel. This should include periodic reminders and highlights of the risk of Separating Employee Clearance procedures not being followed.

CORRECTIVE ACTION:
We agree with this recommendation. The Chief, AWSS, will ensure the development and implementation of a strategy to review and update current Separating Employee Clearance (SEC) policies, procedures, and controls, including the Internal Revenue Manual, related to the recovery of security related items, access revocation, card termination and destruction, ID Cards, manual keys, card keys and other security related items. FMSS managers and security personnel will receive comprehensive training on the updated procedures as well as periodic reminders.

IMPLEMENTATION DATE:
February 28, 2017

RESPONSIBLE OFFICIAL:
Director, Facilities Management and Security Services (FMSS)

CORRECTIVE ACTION MONITORING PLAN:
AWSS will enter accepted corrective actions into the Joint Audit Management Enterprise System (JAMES). These corrective actions are monitored on a monthly basis until completion.

RECOMMENDATION 2:
The Chief, AWSS will perform an inventory verification of non-enforcement pocket commissions assigned to IRS employees and update and maintain the PIV Data Synchronization (PDS).

CORRECTIVE ACTION:
We agree with this recommendation. The Chief, AWSS, will complete an inventory verification of non-enforcement pocket commissions assigned to IRS employees and develop procedures for the on-going update and maintenance in PDS.

IMPLEMENTATION DATE:
January 31, 2017

RESPONSIBLE OFFICIAL:
Director, Facilities Management and Security Services (FMSS)

CORRECTIVE ACTION MONITORING PLAN:
AWSS will enter accepted corrective actions into JAMES. These corrective actions are monitored on a monthly basis until completion.

RECOMMENDATION 3:
The Chief, AWSS will revise current key custody policies and procedures to include documenting the issuance of manual keys and key cards and changing combination locks so managers will know security items that need to be recovered or combinations that need to be changed during employee separations.

CORRECTIVE ACTION:
We agree with this recommendation. The Chief, AWSS, will revise and implement current FMSS key custody policies and procedures. The procedures will include documentation of issuance of manual keys and/or key cards. The recovery of manual keys and/or key cards and combination lock changes due to employee separations will also be included.

IMPLEMENTATIONDATE:
August 31, 2017

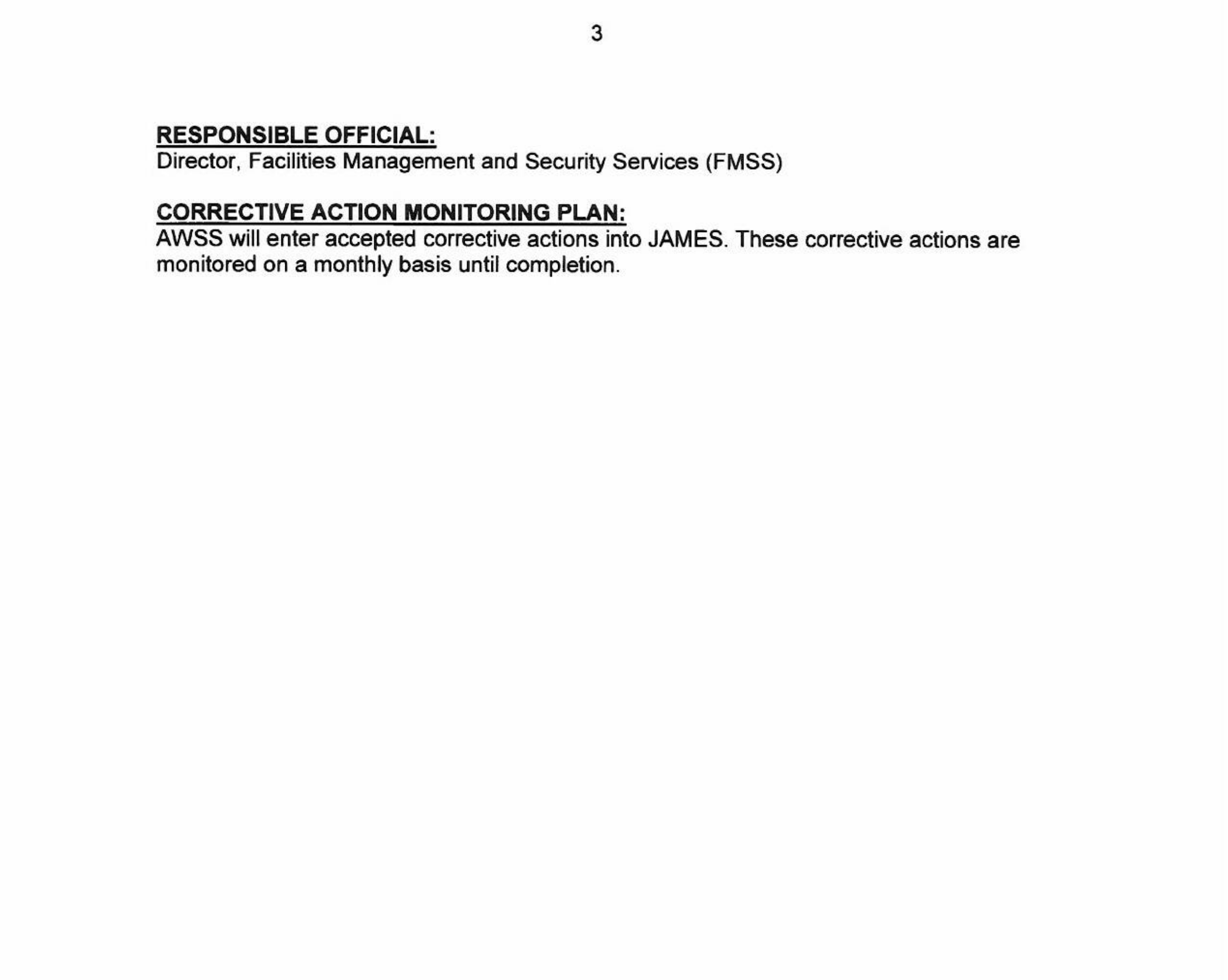
RESPONSIBLE OFFICIAL:
Director, Facilities Management and Security Services (FMSS)

CORRECTIVE ACTION MONITORING PLAN:
AWSS will enter accepted corrective actions into JAMES. These corrective actions are monitored on a monthly basis until completion.

RECOMMENDATION 4:
The Chief, AWSS will coordinate with the IRS Information Technology office to review the process to confirm that computer and building access is deactivated when **2****************************
*****2*****.

CORRECTIVE ACTION:
The Chief, AWSS, will coordinate with the IRS Information Technology office to review the process and develop procedures to ensure the deactivation of computer and building access when ********************2***************************
2***************.

IMPLEMENTATION DATE:
March 31, 2017



3

RESPONSIBLE OFFICIAL:
Director, Facilities Management and Security Services (FMSS)

CORRECTIVE ACTION MONITORING PLAN:
AWSS will enter accepted corrective actions into JAMES. These corrective actions are monitored on a monthly basis until completion.