TREASURY INSPECTOR GENERAL FOR TAX ADMINISTRATION

Access to Facilities and Sensitive Taxpayer Information Was Not Always Revoked for Separated Employees

June 25, 2020

Reference Number: 2020-10-034

TIGTACommunications@tigta.treas.gov | www.treasury.gov/tigta | 202-622-6500

HIGHLIGHTS: Access to Facilities and Sensitive Taxpayer Information Was Not Always Revoked for Separated Employees

Final Audit Report issued on June 25, 2020
Reference Number 2020-10-034

Why TIGTA Did This Audit

TIGTA previously reported that IRS controls to prevent access to Government facilities and computers after employees separated were ineffective. This audit was initiated to determine if the IRS implemented corrective actions to timely remove access to IRS facilities and computers when employees separate.

Impact on Taxpayers

During Fiscal Year 2018, more than 4,400 full-time, permanent employees separated from the IRS, including more than 300 employees who separated during a pending disciplinary case. 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.

The IRS must prevent former employees from unauthorized access to IRS buildings and computers.

What TIGTA Found

The IRS updated procedures in response to TIGTA's prior report; however, these changes were not effective in preventing access to facilities and computers after employees separated. For example, TIGTA identified processing delays in over 1,200 separations. These delays contributed to the untimely removal of former employees' access to IRS facilities and taxpayers' sensitive information, although there were valid reasons for some of the delays.

Even when managers processed separation paperwork on time, Facilities Management and Security Services personnel did not remove building access within the then-required 18 hours of the separation date for 79 percent of randomly sampled separated employees.

Most IRS managers properly collected departing employees' identification cards and timely processed their removal. However, during Fiscal Year 2018, the IRS never recovered identification cards from 396 separated employees, including 26 former employees who separated under adverse conditions. Furthermore, 19 managers were responsible for 91 (23 percent) of the unrecovered identification cards, including three managers who failed to recover nine cards each.

The IRS managers responsible for collecting these unrecovered identification cards did not always report that the cards had not been collected as required. Furthermore, management advised us that the IRS does not have the authority to compel departing employees to turn in their identification cards.

What TIGTA Recommended

TIGTA recommended that the Chief, Facilities Management and Security Services, work with the Human Capital Officer to (1) share pending retirement information; (2) notify supervisors of managers who input late separation personnel action requests; (3) encourage supervisors to hold managers accountable; (4) update employee separation guidance; (5) explore options to secure employees' unrecovered identification cards; and (6) ensure that required reports were filed and access was terminated for 396 unrecovered identification cards. In addition, the Chief, Facilities Management and Security Services, should (7) review overdue clearance module records every month and (8) determine if the clearance module can systemically alert the IRS of approaching access termination deadlines.

The IRS agreed with all of our recommendations and plans to take corrective actions.

TREASURY INSPECTOR GENERAL
FOR TAX ADMINISTRATION

U.S. DEPARTMENT OF THE TREASURY

WASHINGTON, D.C. 20220

June 25, 2020

MEMORANDUM FOR: COMMISSIONER OF INTERNAL REVENUE

FROM: Michael E. McKenney
Deputy Inspector General for Audit

SUBJECT: Final Audit Report – Access to Facilities and Sensitive Taxpayer Information Was Not Always Revoked for Separated Employees (Audit # 201910014)

This report presents the results of our review to follow up on recommendations from a prior report[1] and to determine if the Internal Revenue Service (IRS) has implemented corrective actions to remove access to IRS facilities and computers when employees separate. This audit is included in our Fiscal Year 2020 Annual Audit Plan and addresses the major management challenge of *Security Over Taxpayer Data and Protection of IRS Resources*.

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

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 Heather M. Hill, Acting Assistant Inspector General for Audit (Management Services and Exempt Organizations).

[1] Treasury Inspector General for Tax Administration, Ref. No. 2016-10-038, *Access to Government Facilities and Computers Is Not Always Removed When Employees Separate* (June 2016).

Table of Contents

Appendices

Background

During Fiscal Year (FY) 2018, more than 4,400 full-time, permanent employees separated from the Internal Revenue Service (IRS) through retirement, resignation, death, *etc.*, including more than 300 employees who separated during pending disciplinary cases.[1] IRS employees have various levels of access to buildings and computers that store sensitive information. Employees are issued security items (*i.e.*, identification cards, building access cards, and keys) that they use to access taxpayer information and facilities. When employees separate, these items must be recovered prior to the effective date of separation.

The Facilities Management and Security Services (FMSS) office is responsible for delivering nationwide facilities and security services for the IRS. This office provides and secures the physical locations where IRS employees conduct the day-to-day work of tax administration.

The IRS uses the HR Connect *Separating Employee Clearance Module* (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.[2] This process initiates when the employee, manager, or Human Resources personnel submits a Personnel Action Request (PAR) involving the separation of an employee.[3] Upon approval, the PAR generates a clearance module record, in which managers are responsible for entering security items that departing employees should return and indicating when, where, and how the items were returned. The approved clearance module record appears in the FMSS worklist, which personnel should use to monitor the recovery of security items.

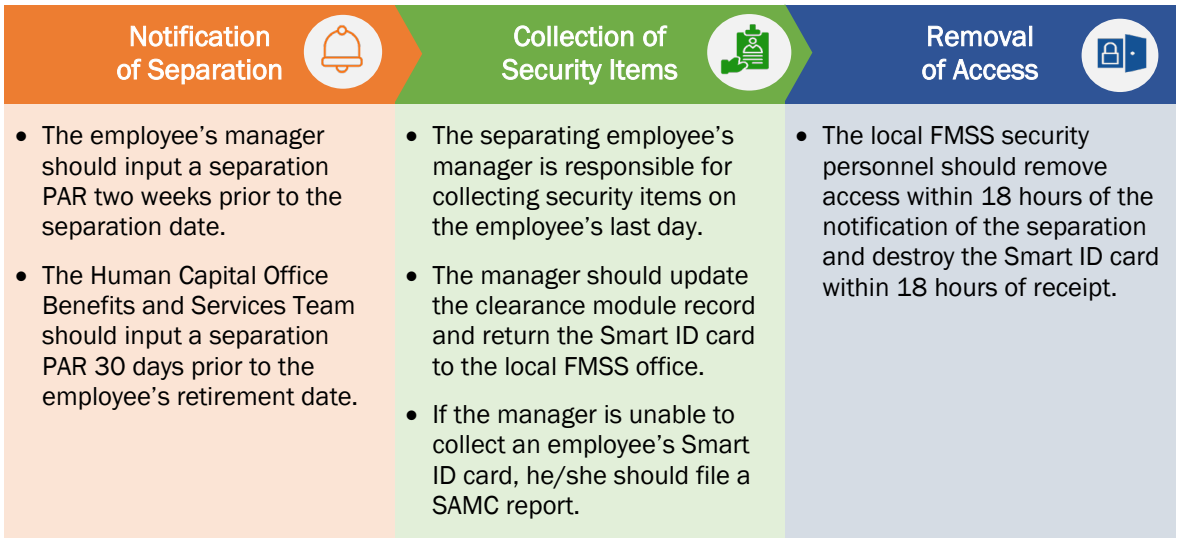
It is the manager's responsibility to return the smart identification (Smart ID) card to the local security office. FMSS personnel are required to access the clearance module daily to identify separating employees. FMSS personnel then verify recovery of the Smart ID card by IRS management, confirm that the Smart ID card is returned to the local servicing security office, and record the receipt of the Smart ID card in the clearance module. Local FMSS personnel must deactivate the Smart ID card within 18 hours of notification of the employee's separation, and the security officer must physically destroy the Smart ID card within 18 hours of receipt.[4] Deactivation of the Smart ID card eliminates the employees' access to IRS facilities and systems.

If the manager cannot recover a separating employee's Smart ID card, he or she must notify the local FMSS Security Services Office and note the circumstances of nonrecovery in the clearance module. A Situational Awareness Management Center (SAMC) report should also be filed explaining circumstances of nonrecovery and the Treasury Inspector General for Tax Administration (TIGTA) Office of Investigations (OI) should be notified. In addition, managers are responsible for verifying the accuracy of clearance module records for employees and

[1] The numbers exclude Chief Counsel and Criminal Investigation employees because those offices use a different process for separating employees and therefore were not included in the scope of this audit.
[2] 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.
[3] PARs are used to initiate and document employee events such as job reclassification, promotions, name changes, and retirements.
[4] During this audit, FMSS management changed the deactivation requirement to within three business days of notification and the requirement to physically destroy the card to within three business days of receipt.

ensuring that all items are collected and returned to their respective offices. Figure 1 includes a summary of the responsible parties for each portion of this process.

Figure 1: Separating Employee Clearance Process



Source: TIGTA summary of the Internal Revenue Manual and other internal IRS guidance.[5]

In a prior audit, TIGTA determined that IRS controls are not effective in preventing access to Government facilities and computers after employees separated.[6] Based on a random sample of FY 2014 employee separations, TIGTA estimated that the IRS could not verify that all security items were recovered for approximately 2,700 (66 percent) of the more than 4,100 full-time, permanent employee separations. Four credentials that were not properly collected were later used to enter IRS buildings. 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 OI as required. 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.

Results of Review

Updated Procedures Did Not Ensure That Access to IRS Facilities Was Revoked

As a result of TIGTA's prior recommendations, FMSS management updated employee exit procedures to emphasize the required timeline to recover, deactivate, and dispose of security items from employees separating from the IRS.[7] However, the updated procedures did not

[5] Internal Revenue Manual 1.4.6, *Resource Guide for Managers* (August 2, 2016).
[6] TIGTA, Ref. No. 2016-10-038, *Access to Government Facilities and Computers Is Not Always Removed When Employees Separate* (June 2016).
[7] Smart ID cards require deactivation to prevent their future use for access to IRS buildings and computers.

effectively prevent delays when removing former employees' access to IRS facilities and computer systems. The Government Accountability Office's *Standards for Internal Control in the Federal Government* requires that management take corrective action as necessary to enforce accountability for internal control.[8] However, the IRS lacks sufficient oversight of the separating employee clearance process, and managers and employees were not held accountable when they failed to follow procedures. Figure 2 shows that there were problems in all three phases of the employee clearance process.

Figure 2: Separating Employee Clearance Process

Notification of Separation	Collection of Security Items	Removal of Access
• 1,221 (13 percent) of the 9,469 FY 2018 HR Connect clearance module records were created more than a week after the employee's separation date.[9]	• 396 Smart ID cards were not recovered from employees who separated from the IRS in FY 2018. • Managers did not file required SAMC reports or notify TIGTA OI that Smart ID cards were not recovered for 86 (25 percent) employees.	• We estimate that building access was not removed within 18 hours of the separation date for 3,567 (80 percent) of the 4,439 full-time, permanent IRS employee separations.[10]

Source: Results of TIGTA analysis.

Although managers are supposed to complete a Separation PAR at least two weeks before separation, many of these PARs were not created until more than a week after separation. In addition, managers sometimes failed to collect Smart ID cards and then failed to report it as required. Even when clearance module records were timely created, the FMSS office usually did not remove building access within required time frames. It is important for the IRS to recover security items and timely remove access to prevent former employees from unauthorized entry to IRS facilities and workspaces, accessing IRS computers and taxpayer information, or potentially misrepresenting themselves to taxpayers.

IRS managers did not always input separation notifications timely

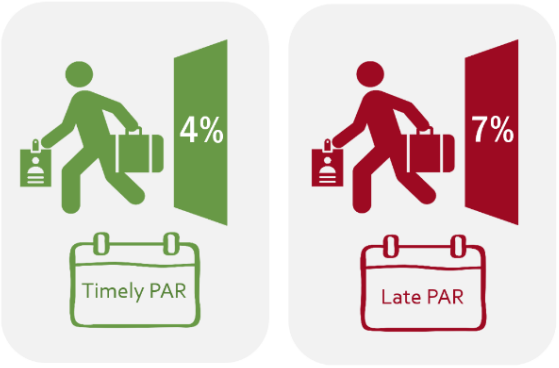
Employee separations are initiated in HR Connect by a PAR in advance of the separation date, when possible.[11] The separation PAR generates a clearance module record, which notifies FMSS security personnel of the pending separation so they can timely terminate the employees' access to facilities and systems. When an employee is retiring, the Benefits and Services Team

[8] Government Accountability Office, GAO-14-704G, *Standards for Internal Control in the Federal Government* (Sept. 2014).
[9] During FY 2018, 4,439 full-time, permanent employees separated from service. The remaining 5,030 clearance module records involved other types of employees, such as part-time and seasonal. The managers' procedures for notification of separation are the same for all of these employees.
[10] We limited this analysis to full-time, permanent employees because IRS procedures allow the FMSS office to delay processing of temporary and seasonal employees in circumstances such as a potential return to work.
[11] In situations such as death or unexpected separation, this time frame will not be met. Our analysis focused on employees for whom the separation PAR was input more than seven days after the employee's separation to account for these unexpected separations.

specialist should input the separation PAR 30 days prior to the employee's retirement date in accordance with their internal guidance. All other separations are processed by the employee's manager at least two weeks prior to the separation date in accordance with guidance established in the *Separating Employee Clearance Manager and Proxy Guide*.

We found that 1,221 (13 percent) of the 9,469 HR Connect clearance module records were created more than a week after the employee's separation date during FY 2018, including 69 records that were more than 100 days after separation. When a separation PAR is not input timely, the FMSS office is not notified of the separation and therefore does not terminate the building and computer access timely. As many as 1,221 employees' Smart ID cards remained active with building and computer access more than a week after separation.[12] In addition, when separation PARs are input after the employee's separation date, there is a higher risk that the Smart ID card will not be recovered. The IRS never recovered the Smart ID cards from 7 percent (84) of the 1,221 employees whose clearance module records were created more than seven days past the employee's separation date, compared with 4 percent recovered when separation PARs were input timely.

There is a greater chance that Smart IDs are not recovered when a separation PAR is filed late.



In addition, four of these employees separated under adverse conditions. The managers of these four employees did not create the clearance module until an average of 25 days after the separation date, including one that was 52 days after separation.[13] These separated employees pose a high risk to IRS security because a disgruntled employee could retain access to IRS buildings after his or her separation date during the period between separation and termination of access. In addition, if separated employees access Federal buildings, they may be able to use their Smart ID card to access taxpayer information on a stand-alone computer or paper files in storage areas, which is in violation of Internal Revenue Code Section 6103. This information could be used to compromise taxpayers' Personally Identifiable Information.

In some cases, there were valid reasons for these delays; however, others were a result of managers who failed to follow procedures.[14] There are no consequences for the responsible parties when these delays occur. Although the IRS updated procedures based on TIGTA's prior recommendations, continued weaknesses in the employee exit procedures process indicate that accountability is needed. Additionally, in instances when employees submit late applications for retirement, the IRS Human Capital Office does not have controls in place to notify the FMSS office of the impending retirement. The FMSS office has begun discussions with the Human

[12] We cannot be certain about the exact number because employee PARs that had corrections may not have been untimely; the computer reset could have made them appear that way.
[13] The reasons for these adverse separations include absence without leave, failure to follow instructions, failure to resolve debts, and tax issues.
[14] Valid reasons for the delays included backdated separation PARs for furloughed employees and corrections to an employee's separation PAR that resulted in the creation of a new clearance module record. These actions disrupted timeliness because the system resets the clearance module record creation date and makes the termination appear late. However, it is not possible to quantify how often this occurred because the system does not differentiate furloughed employees or corrections.

Capital Office to address this delay and is now considering new reports to notify the office of these pending retirements.

The Chief, FMSS, and the Human Capital Officer should work together to:

Recommendation 1: Ensure that the FMSS office has a list of monthly pending retirements in order to ensure that building access is terminated timely.

> **Management's Response**: IRS management agreed with this recommendation. The Human Capital Officer will provide a list of monthly pending retirements to the FMSS office to ensure that building access is terminated timely.

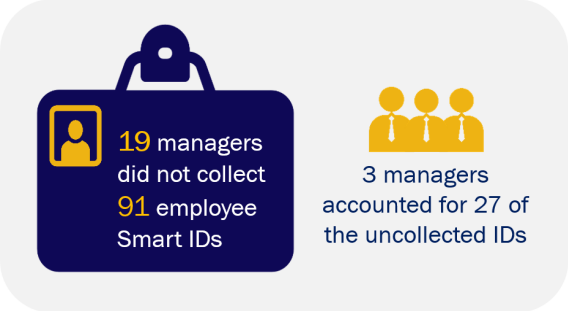
Recommendation 2: Develop a process to notify the supervisors of managers who input late separation PARs that encourages supervisors to remind managers of their responsibilities for inputting separation PARs timely.

> **Management's Response**: IRS management agreed with this recommendation. The Human Capital Office will explore providing a report with the names of managers who have employees with late separation actions to the business units. The report will provide the business units with the information needed to notify supervisors and remind managers of their responsibility for timely inputting separation PARs.

IRS managers did not always collect Smart ID cards from separated employees

The IRS did not recover 396 (4 percent) of 9,469 Smart ID cards from employees who separated from the IRS in FY 2018, including 105 from full-time, permanent employees.[15] Twenty-six of these unrecovered cards belonged to employees who separated under adverse circumstances.[16] It is important to collect Smart ID cards from separating employees even if the building access is systemically terminated because Smart ID cards can be used to access some Federal buildings by showing the card to a security officer instead of scanning the card at an access point.

The majority of IRS managers appear to be successful in collecting Smart ID cards from separating employees. However, 19 managers were responsible for collecting 91 (23 percent) of the 396 unrecovered identification cards, including three managers who failed to recover nine cards each. Managers we interviewed indicated that their employees had a high turnover rate and in many cases would leave and not return to work. Once an employee leaves an IRS building, it is difficult to retrieve their security items, despite recovery efforts such as phone calls and letters. In addition, managers were often uncertain about their responsibilities.



[15] Based on analysis of FY 2018 separations in the clearance module. At the conclusion of our audit, the IRS told us that 46 of these Smart IDs had since been recovered.
[16] The reasons for these adverse separations included absence without leave, tax issues, substance abuse, unauthorized access violations, falsification of documents, and unprofessional conduct.

When a manager is unable to collect a separating employee's Smart ID card, the *Separating Employee Clearance Manager and Proxy Guide* requires the manager to file an incident report with the SAMC in order to notify the FMSS office and the IRS's law enforcement partners that the Smart ID card was not recovered.[17] In addition, the Internal Revenue Manual requires that all lost/stolen Smart ID cards be reported to the SAMC via a website portal, telephone, fax, or e-mail. The SAMC report must include certain information such as the time and date of the incident, details of what occurred, who was notified (*i.e.*, TIGTA OI), and a point of contact for follow-up questions.[18] According to FMSS management, SAMC reports were not filed for 86 of the 396 unrecoverable Smart ID cards in FY 2018. Some managers were unaware of the requirement to submit a SAMC report for unrecoverable Smart IDs and instead relied on the FMSS office to file the reports.

The managers' supervisors did not remind managers to take the appropriate actions. In addition, the FMSS office does not review the number of unrecoverable security items by manager. The office notifies managers when separated employees have not returned their Smart ID cards; however, the manager's supervisor is not notified. Therefore, managers are not questioned or held accountable for having a high number of separated employees with unrecoverable security items, and there may be less of an incentive for the managers to attempt to retrieve these items.

In addition, there is currently no process to penalize employees who do not return their security items. As a result, it is solely the responsibility of the employee's manager to recover security items, and there is little incentive for the departing employee to return IRS equipment. Although most employees return their security items, there is a risk that employees who do not may attempt to use them inappropriately or for nefarious reasons. As a result of this audit, the Human Capital Office and IRS Chief Counsel agreed to explore various options that could encourage separated employees to return their security items.

At the time of our audit, unrecoverable Smart ID cards were reported in the SAMC website portal using a combination lost/stolen designation field, which could make it challenging for TIGTA OI to differentiate the unrecoverable Smart IDs from those that were lost during the year. TIGTA OI treats unrecoverable Smart IDs as potential theft of Government property. IRS management made a process improvement in October 2019 by adding a field in the SAMC website portal to notate that the Smart ID card was unrecoverable. This will allow TIGTA OI to more clearly identify Smart ID cards that were not recovered from separated employees. IRS management took action during the course of this audit; therefore, we are not making a recommendation related to this issue.

The Chief, FMSS, and the Human Capital Officer should work together to:

Recommendation 3: Develop procedures to notify supervisors of managers who do not recover security items from separating employees, and include guidance to remind managers of their responsibilities for securing security items from separating employees.

Management's Response: IRS management agreed with this recommendation. The FMSS office will develop procedures to notify supervisors of managers who do not

[17] IRS's law enforcement partners include TIGTA OI, IRS Criminal Investigation, and the Federal Protective Service.
[18] Internal Revenue Manual 10.2.8, *Incident Reporting* (July 25, 2019).

recover security items from separating employees and include guidance to remind managers of their responsibilities for securing security items from separating employees.

Recommendation 4: Update the Internal Revenue Manual to clarify that managers are responsible for filing a SAMC report when they are unable to recover security items from separating employees.

Management's Response: IRS management agreed with this recommendation. The FMSS office will update the Internal Revenue Manual to clarify that managers are responsible for filing a SAMC report when they are unable to recover security items from separating employees.

Recommendation 5: Work with IRS Chief Counsel and other organizations, as appropriate, to review and explore the various options available to address employees' Smart ID cards that would otherwise be unrecovered.

Management's Response: IRS management agreed with this recommendation. The FMSS office will work with other Treasury Department organizations to review and explore options available to address employees' Smart ID cards that would otherwise be unrecovered.

Recommendation 6: Ensure that SAMC reports are filed and access was terminated for the 350 unrecovered Smart ID cards identified by TIGTA.

Management's Response: IRS management agreed with this recommendation. The FMSS office will ensure that SAMC reports are filed and access was terminated for the 350 unrecovered Smart ID cards identified by TIGTA.

Once notified, the FMSS office did not timely remove building access when IRS employees separated

At the time of our review, IRS guidance required that FMSS security personnel deactivate separating employees' physical access in the Velocity access control system within 18 hours of notification of the separation.[19] However, we determined that building access was not removed from all assigned credentials within 18 hours of the separation date for 69 (82 percent) of 84 randomly sampled full-time, permanent employees who separated from the IRS in FY 2018.[20] For seven of these employees, the FMSS office did not deactivate all building access until more than 100 days after the employee's separation date. Based on these results, we estimate that building access was not removed within 18 hours of 3,567 employees' separation date.[21] FMSS procedures emphasize the importance of prompt removal of access in systems and databases to ensure that

[19] The Identiv Hirsch Velocity is an integrated software platform that manages access control and security operations in IRS facilities.

[20] The Velocity Operator Logs provided by the IRS show each date and time that the separated employee's credentials were deactivated.

[21] Our sample was selected using a 95 percent confidence interval, 25 percent error rate, and ±3 percent precision factor. When projecting the results of our statistical sample, we are 95 percent confident that the actual total amount is between 2,932 and 4,201, assuming that the exception rate is consistent for all offices in each stratum. See Appendix I for our sampling methodology.

only authorized personnel have access to IRS systems and facilities. In addition, because there are circumstances that can prevent Smart ID cards from being recovered, terminating access in a timely manner is an important control. FMSS employees should use daily clearance module worklists to monitor the termination date timeliness. However, the clearance module system does not alert the FMSS employee or their manager when a credential is nearing the termination deadline. IRS management has since updated procedures to require that FMSS security personnel deactivate separating employees' physical access in the Velocity access control system within three business days of notification of the separation.

The IRS Identity Credential and Access Management office previously issued a monthly report to each FMSS Area Director that included a review of the time it took to remove building access from separated employee credentials; however, this report was unintentionally discontinued due to staffing changes in August 2017. The Identity Credential and Access Management office resumed the issuance of this report in October 2019. However, even if the report is used to identify termination delays, FMSS personnel are not held accountable when they do not meet the required time frames.

When building access is not removed timely, there is a risk that separated employees may obtain unauthorized access to IRS facilities and potentially cause harm or misrepresent themselves for personal gain. In the prior TIGTA audit, we identified four Smart ID cards that were used to access a Government facility after the employee had separated. Although we did not identify any post-separation accesses in this audit, the risk remains.

The Chief, FMSS, should:

Recommendation 7: Ensure that the Identity Credential and Access Management office performs reviews of overdue clearance module records and issues reports on a monthly basis. This report should include a review of the termination dates in the Velocity Operator Logs to validate that building access is terminated timely by FMSS employees. Ensure that FMSS management uses the reports to address any timeliness issues and to hold personnel accountable for not meeting the required time frames.

> **Management's Response:** IRS management agreed with this recommendation. The FMSS office will perform reviews of the Separating Employee Clearance Overcycle Report and issue a report on a monthly basis. This report will include a review of the termination dates in the Velocity Operator Logs to validate that building access is terminated timely by FMSS employees. FMSS management will use the reports to address any timeliness issues and to hold FMSS personnel accountable for not meeting the required time frames.

Recommendation 8: Determine the feasibility of systemically alerting FMSS employees and their manager when a Smart ID card nears the three-business-day termination deadline, and update the system accordingly.

> **Management's Response:** IRS management agreed with this recommendation. The FMSS office will determine the feasibility of systemically alerting FMSS employees and their managers when a Smart ID card nears the three-business-day termination deadline and update the system accordingly.

Appendix I

Detailed Objective, Scope, and Methodology

Our overall objective was to follow up on recommendations in a prior report to determine if the IRS has implemented corrective actions to remove access to IRS facilities and computers when employees separate. To accomplish this objective, we:

- Identified and reviewed any FMSS management updates to separating employee clearance policies, procedures, and controls since June 30, 2016. We determined whether designed controls are functioning to provide reasonable assurance that physical access to Government facilities is secured when employees separate from the IRS.
- Identified 4,439 former full-time, permanent IRS employees, excluding Chief Counsel and Criminal Investigation employees, who separated during FY 2018 and obtained a download of the related clearance modules.
- Performed a trend analysis to identify managers with a high number of employees with unrecoverable items. We identified employees whose clearance modules were created untimely (more than seven days after the employee separation date).
- Selected a stratified random sample of 84 of the 4,439 former full-time, permanent IRS employees, excluding Chief Counsel and Criminal Investigation employees, who separated during FY 2018.[1] We used the following criteria: 95 percent confidence level, 3 percent precision rate, and 25 percent expected error rate. The sample included separated employees from four buildings: one processing center (Ogden, Utah); one office with more than 70 separations (Chamblee, Georgia); one office with 25 to 70 separations (Austin, Texas); and one office with less than 25 separations (Jacksonville, Florida).
- Identified a judgmental sample of employees who separated under adverse conditions from the more than 4,439 former full-time, permanent IRS employees.[2] We manually reviewed the case notes to identify egregious, adverse separations.
- Matched the employees in our random sample to the clearance module to determine whether the Smart ID cards were certified as returned. If the Smart ID card was returned, we reviewed the documentation to support the recovery. If the Smart ID card was not returned, we requested the SAMC report and referral to TIGTA. We determined if the Smart ID cards were used to access the building after the employee's effective separation date.

Performance of This Review

This review was performed at the FMSS offices in Chamblee, Georgia; Austin, Texas; and Ogden, Utah, and with information from the FMSS office in Jacksonville, Florida, and the FMSS and Human Capital Office Headquarters in Washington, D.C., during the period February 2019 through December 2019. We conducted this performance audit in accordance with generally

[1] A contract statistician assisted with developing the sampling plans and projections.
[2] A judgmental sample is a nonprobability sample, the results of which cannot be used to project to the population.

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.

Major contributors to the report were Heather M. Hill, Acting Assistant Inspector General for Audit (Management Services and Exempt Organizations); Carl L. Aley, Director; Brian G. Foltz, Audit Manager; Melinda H. Dowdy, Lead Auditor; and Sylvia Sloan-McPherson, Senior Auditor.

Validity and Reliability of Data From Computer-Based Systems

We performed tests to assess the reliability of data from the Treasury Integrated Management Information System Separated Employee file and HR Connect clearance module. We evaluated the data by (1) validating that the date fields contained dates, name fields contained names, *etc.*, and by matching a sample of records from the Treasury Integrated Management Information System Separated Employee file to the HR Connect clearance module. We determined that the data were sufficiently reliable for purposes of this report.

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 reviewing SAMC reports filed for items that were not returned for selected employees who separated during FY 2018. 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.

Appendix II

Management's Response to the Draft Report

DEPARTMENT OF THE TREASURY
INTERNAL REVENUE SERVICE
WASHINGTON, DC 20224

CHIEF
FACILITIES MANAGEMENT AND
SECURITY SERVICES

June 10, 2020

MEMORANDUM FOR MICHAEL E. MCKENNEY
DEPUTY INSPECTOR GENERAL FOR AUDIT

FROM: Richard L. Rodriguez Richard L. Rodriguez Digitally signed by Richard L. Rodriguez Date: 2020.06.10 15:41:03 -04'00'
Chief, Facilities Management & Security Services

SUBJECT: Draft Audit Report – Access to Facilities and Sensitive Taxpayer Information Was Not Always Revoked for Separated Employees (Audit # 201910014)

Thank you for the opportunity to review and comment on the draft audit report. We appreciate that your report acknowledged that most IRS managers properly collected departing employees' identification cards and timely processed their removal. We are committed to the security of our offices and the employees and taxpayer information they contain. Your recommendations will assist us in our efforts to ensure that access to facilities and sensitive taxpayer information is timely revoked for separated employees.

We agree with your recommendations and have developed corrective actions to remediate the report findings. We have already begun making progress on multiple recommendations included in the report, even as we continue to deal with the effect of COVID-19 on operations and take necessary steps to protect the safety and health of employees. For example, FMSS is already receiving a list of monthly pending retirements from HCO in order to ensure that building access is terminated timely. The next step of adding location data to the report will be completed in the near future.

As stated in the report, the IRS recovered Smart IDs from 96 percent of employees who separated in FY18. We are making substantial progress in addressing the remaining 350 unrecovered Smart IDs noted in the report and have already confirmed that building access has been terminated and that the appropriate reports have been filed for 315 of these cases. The IRS continues to address the challenges associated with recovering Smart IDs. Recovering Smart IDs from separating personnel can be particularly challenging when employees are not co-located with their managers, when turn-over rates are high, and when employees leave without notice.

In addition, the IRS does not have legal authority to compel departed employees to turn in their identification cards and instead is reliant on TIGTA to enforce the requirement when an employee fails to voluntarily comply; however, we have begun considering options available to address employees' Smart ID cards that would otherwise be unrecovered. Attached is our corrective action plan describing how we plan to address your recommendations.

We appreciate the continued support and assistance provided by your office. If you have any questions, please contact me at 202-317-4480, or a member of your staff may contact Edward Pelcher, associate director, Security Policy, Facilities Management and Security Services at 707-646-7278.

Attachment

Attachment

TIGTA RECOMMENDATION #1:
The Chief, Facilities Management and Security Services, and the Human Capital Officer should work together to ensure that the FMSS office has a list of monthly pending retirements in order to ensure that building access is terminated timely.

CORRECTIVE ACTION #1:
We agree with this recommendation. By September 15, 2020, the Human Capital Officer will provide a list of monthly pending retirements to the FMSS office in order to ensure that building access is terminated timely.

IMPLEMENTATION DATE:
September 15, 2020

RESPONSIBLE OFFICIAL:
Human Capital Officer

CORRECTIVE ACTION MONITORING PLAN:
Corrective actions are entered into the Joint Audit Management Enterprise System (JAMES) and are monitored monthly through completion.

TIGTA RECOMMENDATION #2:
The Chief, Facilities Management and Security Services, and the Human Capital Officer should work together to develop a process to notify the supervisors of managers who input late separation PARs that encourages supervisors to remind managers of their responsibilities for inputting separation PARs timely.

CORRECTIVE ACTION #2:
We agree with this recommendation. The Human Capital Officer will explore providing a report with the names of managers who have employees with late separation actions to the business units by February 15, 2021. The report will provide the business units with the information needed to notify supervisors and remind managers of their responsibility for timely inputting separation PARs.

IMPLEMENTATION DATE:
February 15, 2021

RESPONSIBLE OFFICIAL:
Human Capital Officer

CORRECTIVE ACTION MONITORING PLAN:
Corrective actions are entered into the Joint Audit Management Enterprise System (JAMES) and are monitored monthly through completion.

TIGTA RECOMMENDATION #3:
The Chief, Facilities Management and Security Services, and the Human Capital Officer should work together to develop procedures to notify supervisors of managers when they do not recover security items from separating employees and include guidance to remind managers of their responsibilities for securing security items from separating employees.

CORRECTIVE ACTION #3:
We agree with this recommendation. By May 15, 2021, FMSS will develop procedures to notify supervisors of managers when they do not recover security items from separating employees and include guidance to remind managers of their responsibilities for securing security items from separating employees.

IMPLEMENTATION DATE:
May 15, 2021

RESPONSIBLE OFFICIAL:
Chief, Facilities Management and Security Services, Security Policy, ICAM

CORRECTIVE ACTION MONITORING PLAN:
Corrective actions are entered into the Joint Audit Management Enterprise System (JAMES) and are monitored monthly through completion.

TIGTA RECOMMENDATION #4:
The Chief, Facilities Management and Security Services, and the Human Capital Officer should work together to update the Internal Revenue Manual to clarify that managers are responsible for filing a SAMC report when they are unable to recover security items from separating employees.

CORRECTIVE ACTION #4:
We agree with this recommendation. By May 15, 2021, FMSS will update the Internal Revenue Manual to clarify that managers are responsible for filing a SAMC report when they are unable to recover security items from separating employees.

IMPLEMENTATION DATE:
May 15, 2021

RESPONSIBLE OFFICIAL:
Chief, Facilities Management and Security Services, Security Policy, ICAM

CORRECTIVE ACTION MONITORING PLAN:
Corrective actions are entered into the Joint Audit Management Enterprise System (JAMES) and are monitored monthly through completion.

TIGTA RECOMMENDATION #5:
The Chief, Facilities Management and Security Services, and the Human Capital Officer should work together to work with IRS Chief Counsel and other organizations, as appropriate, to review and explore the various options available to address employees' Smart ID cards that would otherwise be unrecovered.

CORRECTIVE ACTION #5:
We agree with this recommendation. By September 15, 2020, FMSS will work with other Treasury organizations to review and explore options available to address employees' Smart ID cards that would otherwise be unrecovered.

IMPLEMENTATION DATE:
September 15, 2020

RESPONSIBLE OFFICIAL:
Chief, Facilities Management and Security Services, Security Policy, ICAM

CORRECTIVE ACTION MONITORING PLAN:
Corrective actions are entered into the Joint Audit Management Enterprise System (JAMES) and are monitored monthly through completion.

TIGTA RECOMMENDATION #6:
The Chief, Facilities Management and Security Services, and the Human Capital Officer should work together to ensure that SAMC reports are filed and access was terminated for the 350 unrecovered Smart ID cards identified by TIGTA.

CORRECTIVE ACTION #6:
We agree with this recommendation. By October 15, 2020, FMSS will ensure that SAMC reports are filed and access was terminated for the 350 unrecovered Smart ID cards identified by TIGTA.

IMPLEMENTATION DATE:
October 15, 2020

RESPONSIBLE OFFICIAL:
Chief, Facilities Management and Security Services, Security Policy, ICAM

CORRECTIVE ACTION MONITORING PLAN:
Corrective actions are entered into the Joint Audit Management Enterprise System (JAMES) and are monitored monthly through completion.

TIGTA RECOMMENDATION #7:
The Chief, Facilities Management and Security Services, should ensure that the Identity Credential and Access Management office performs reviews of overdue clearance module records and issues reports on a monthly basis. This report should include a review of the termination dates in the Velocity Operator Logs to validate that building access is terminated timely by FMSS employees. Ensure that FMSS management uses the reports to address any timeliness issues and to hold personnel accountable for not meeting the required time frames.

CORRECTIVE ACTION #7:
We agree with this recommendation. By June 15, 2021, FMSS will perform reviews of the SEC Overcycle Report and issue a report on a monthly basis. This report will include a review of the termination dates in the Velocity Operator Logs to validate that building access is terminated timely by FMSS employees. FMSS management will use the reports to address any timeliness issues and to hold FMSS personnel accountable for not meeting the required time frames.

IMPLEMENTATION DATE:
June 15, 2021

RESPONSIBLE OFFICIAL:
Associate Director, Facilities Management and Security Services, Security Policy

CORRECTIVE ACTION MONITORING PLAN:
Corrective actions are entered into the Joint Audit Management Enterprise System (JAMES) and are monitored monthly through completion.

TIGTA RECOMMENDATION #8:
The Chief, Facilities Management and Security Services, should determine the feasibility of systemically alerting FMSS employees and their manager when a Smart ID card nears the three-business-day termination deadline, and update the system accordingly.

CORRECTIVE ACTION #8:
We agree with this recommendation. By October 15, 2020, FMSS will determine the feasibility of systemically alerting FMSS employees and their managers when a Smart

ID card nears the three-business-day termination deadline and update the system accordingly.

IMPLEMENTATION DATE:
October 15, 2020

RESPONSIBLE OFFICIAL:
Chief, Facilities Management and Security Services, Security Policy, ICAM

CORRECTIVE ACTION MONITORING PLAN:
Corrective actions are entered into the Joint Audit Management Enterprise System (JAMES) and are monitored monthly through completion.

Appendix III

Abbreviations

FMSS	Facilities Management and Security Services
FY	Fiscal Year
ID	Identification
IRS	Internal Revenue Service
OI	Office of Investigations
PAR	Personnel Action Request
SAMC	Situational Awareness Management Center
TIGTA	Treasury Inspector General for Tax Administration