TREASURY INSPECTOR GENERAL FOR TAX ADMINISTRATION

Improved Controls Are Needed to Account for the Return of Contractor Employee Identification Cards

November 1, 2017

Reference Number: 2018-10-004

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

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

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

1-800-366-4484

By Web:

www.treasury.gov/tigta/

Or Write:

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

Information you provide is confidential and you may remain anonymous.

IMPROVED CONTROLS ARE NEEDED TO ACCOUNT FOR THE RETURN OF CONTRACTOR EMPLOYEE IDENTIFICATION CARDS

Highlights

Final Report issued on November 1, 2017

Highlights of Reference Number: 2018-10-004 to the Internal Revenue Service Chief, Agency-Wide Shared Services.

IMPACT ON TAXPAYERS

Between April 1, 2015, and March 31, 2016, more than 1,700 contractor employees separated from the IRS, of which more than 600 were issued Government identification cards, known as Smart ID cards. It is important for the IRS to recover Smart ID cards from former contractor employees to prevent unauthorized access to IRS facilities, computers, and taxpayer information.

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 Smart ID cards are returned when contractor employees separate from the IRS.

WHAT TIGTA FOUND

The IRS designed controls to provide assurance that contractor employee Smart ID cards are returned when contractors no longer work on IRS contracts. However, these controls were not functioning effectively to provide reasonable assurance that facilities, computers, and taxpayer information were secure when contractor employees separated from the IRS.

The IRS could provide documentation showing the recovery of only 17 (15 percent) of 113 Smart ID cards associated with contractor employees in TIGTA's random sample. This occurred because IRS employees generally did not document serial numbers for the return of Smart ID cards on manual forms. This is necessary to ensure that specific Smart ID cards that were assigned to the contractor employees were returned when they separated.

Due to substantial recordkeeping issues, TIGTA could not determine whether the other 96 (85 percent) Smart ID cards were recovered. IRS records show that 79 of the 96 cards were deactivated and access logs indicate that most of the contractors associated with these 79 cards did not access IRS facilities or systems after their separation date. For those who did, IRS officials were able to provide reasonable explanations for the access. IRS documentation for the remaining 17 Smart ID cards was inconsistent. In addition, logs show that several of the contractors associated with these 17 cards accessed IRS facilities and systems after their separation date. However, IRS officials could not provide explanations or determine whether Smart ID cards were used for these accesses.

TIGTA informed the IRS about these issues during the audit and IRS management stated they had already begun taking corrective actions. Due to the sensitivity of data housed by the IRS, it is imperative that the IRS ensure that it recovers and accounts for Smart ID cards.

WHAT TIGTA RECOMMENDED

TIGTA recommended that the Chief, Agency-Wide Shared Services, develop processes to provide assurance that serial numbers are documented when Smart ID cards are returned and perform follow-up work to address separated contractor employees who, according to access logs, accessed IRS computers or facilities after separation.

In their response, IRS management agreed with the recommendations and will develop a process to provide reasonable assurance that Smart ID card serial numbers are documented when contractor employees separate, and will perform follow-up work on separated contractor employees who, according to access logs, accessed an IRS facility or computer after separation and determine whether they were authorized to make the access.

TREASURY INSPECTOR GENERAL
FOR TAX ADMINISTRATION

DEPARTMENT OF THE TREASURY
WASHINGTON, D.C. 20220

November 1, 2017

MEMORANDUM FOR CHIEF, AGENCY-WIDE SHARED SERVICES

FROM: Michael E. McKenney
Deputy Inspector General for Audit

SUBJECT: Final Audit Report – Improved Controls Are Needed to Account for the Return of Contractor Employee Identification Cards
(Audit # 201610020)

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 Smart Identification cards are returned when contractor employees separate from the IRS. This review was included in our Fiscal Year 2017 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 V.

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

FMSS	Facilities Management and Security Services
ID	Identification
IRS	Internal Revenue Service

Background

The Internal Revenue Service (IRS), like other Federal agencies, relies on contractor personnel to accomplish a broad range of mission-critical functions.[1] Between April 1, 2015, and March 31, 2016, more than 1,700 contractor employees with staff-like access[2] terminated their relationship with the IRS due to the expiration of contracts or for other reasons, such as entering into other employment arrangements. It is important for the IRS to recover Government identification cards (hereafter referred to as Smart Identification[3] (ID) cards) from former contractor employees prior to the effective date of separation to prevent unauthorized access to IRS facilities, computers, and taxpayer information.

Between April 1, 2015, and March 31, 2016, more than 1,700 contractor employees with staff-like access separated from the IRS.

The Facilities Management and Security Services (FMSS)[4] office is responsible for delivering nationwide facilities and security services for the IRS. It secures the physical locations where IRS employees conduct the day-to-day work of tax administration to meet the needs of American taxpayers.

Contractor employees who have a need to access IRS facilities,[5] computer systems, or taxpayer information are provided a Smart ID card if they meet all requirements and pass a background investigation.[6] When a contractor employee with a Smart ID card separates from the IRS, the return of the Smart ID card should be documented electronically in the USAccess system[7] and

[1] According to IRS management, the IRS employed more than 14,300 contractor employees as of July 2017.
[2] A contractor employee approved for staff-like access requires no escort while in an IRS-owned or controlled facility. "Access" is the authority granted to contractor employees to come into contact with Sensitive But Unclassified information in the performance of official duties, enter an IRS facility without escort, and access IRS computer systems when required.
[3] Homeland Security Directive-12 provides for a standardized Federal identity credential known as the Personal Identity Verification, or Smart ID card, that is designed to enhance security, reduce identity fraud, and protect the personal privacy of those issued Government identification.
[4] The FMSS office is part of the Agency-Wide Shared Services organization.
[5] The IRS Enterprise Physical Access Control System, which uses the Hirsch Identive Velocity™ suite of commercial off-the-shelf application database software, provides primary access control to IRS buildings and offices. 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.
[6] Smart ID card serial numbers are recorded in USAccess.
[7] The USAccess system is a managed service that provides agencies with all the key components necessary to manage the full life-cycle of a personal identity verification credential.

manually on Form 13716-A, *Request for ID Media/Access Card for Contractor Employees*, and destruction logs.

- **Electronic Documentation** – The FMSS Security office uses the Government-wide USAccess computer system to enroll and activate Smart ID cards. When Smart ID cards are recovered from contractor employees who are separating from the IRS, the FMSS Security office should use the USAccess system to deactivate Smart ID cards so that Smart ID cards can no longer be used to access IRS facilities or computer systems. To allow for cases in which Smart ID cards cannot be recovered from separating employees,[8] USAccess allows agencies to deactivate unreturned Smart ID cards without having possession of the cards. In addition, the FMSS Security office can use the USAccess to mark Smart ID cards as destroyed. However, we determined in a prior audit[9] that the FMSS Security office can mark a Smart ID card as destroyed in USAccess without having recovered the Smart ID card.
- **Manual Documentation** – The FMSS Security office is required to document the serial number of the Smart ID card assigned to the contractor employee on Form 13716-A prior to providing the card to a contractor employee. When the contractor employee separates from the IRS, the Smart ID card should be returned to the FMSS Security office and the serial number of the card documented on Form 13716-A and on a destruction log[10] in the FMSS Security office. The local servicing Security office is responsible for physically destroying the card within 18 hours of its return.

This review was performed with information obtained from the Agency-Wide Shared Services organization FMSS offices located in Phoenix, Arizona; Fresno, Los Angeles, and Oakland, California; Washington, D.C.; Jacksonville, Florida; Atlanta, Georgia; Chicago, Illinois; Covington, Kentucky; Lanham-Seabrook, Maryland; Andover, Massachusetts; Kansas City and St. Louis, Missouri; Philadelphia, Pennsylvania; Farmers Branch, Texas; Ogden, Utah; and Kearneysville, West Virginia; and from the Information Technology Organization Infrastructure Services Division in New Carrollton, Maryland, during the period October 2016 through August 2017. 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.

[8] If the manager cannot recover a separating contractor employee's Smart ID card, a report should be submitted to the FMSS Security office explaining the circumstances of the non-recovery.
[9] 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).
[10] A destruction log is a form used by FMSS Security offices to document the return of identification cards from IRS employees and contractor employees. IRS management stated there is not a specific format for the form, but at a minimum, the destruction log should include the contractor name, card number (serial number), and the date the Smart ID card is destroyed.

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 provide reasonable assurance that Smart ID cards are returned when contractor employees no longer work on IRS contracts. These controls include manually documenting dates and serial numbers of the Smart ID cards when they are assigned and then later when they are returned by contractor employees upon separation.

Despite these efforts, we found that the controls were not functioning effectively to provide assurance that facilities, computers, and taxpayer information were secure when contractor employees separated from the IRS. This occurred because FMSS Security office management did not require that IRS employees follow the established process of documenting the date and serial number for the return of Smart ID cards on manual forms. It is important for the IRS to recover security items, such as Smart ID cards, from former contractor employees to prevent unauthorized access to IRS facilities, computers, and taxpayer information.

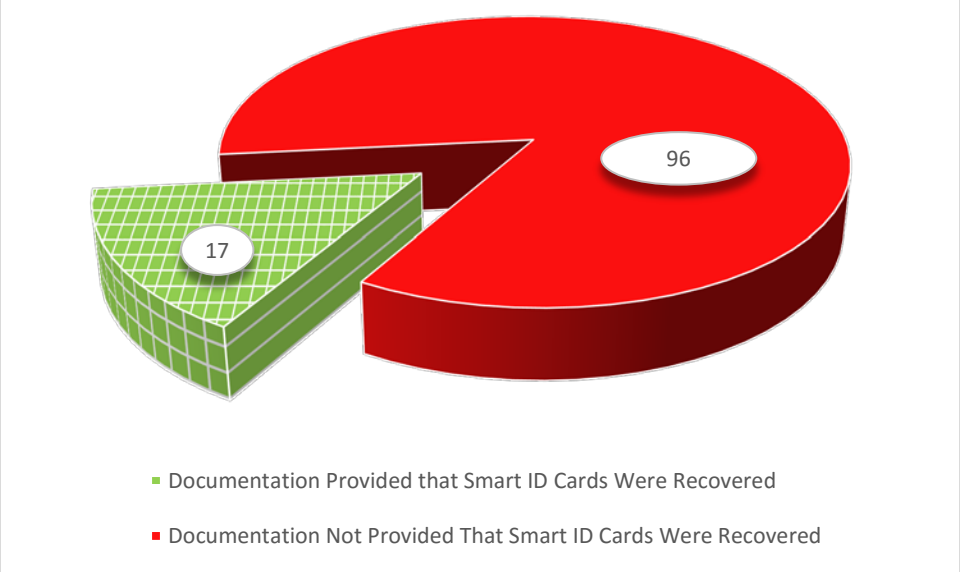
Controls Did Not Provide Assurance That Smart Identification Cards Were Returned When Contractor Employees Separated

Based on a review of contractor employee separations, we found substantial recordkeeping issues[11] and could not determine whether 96 (85 percent) of the 113 Smart ID cards were recovered for contractor employees in our random sample who separated from working on contracts for the IRS between April 1, 2015, and March 31, 2016.[12]

Figure 1 shows the results of our review of documentation for a random sample of 113 contractor employees who separated from working for the IRS on contracts.

[11] We reviewed Forms 13716-A and destruction logs to determine if Smart ID cards were returned. As we discuss later in this report, we did not accept USAccess information as proof that Smart ID cards were returned because the cards can be deactivated and marked as destroyed in the system without the IRS having recovered the card.
[12] See Appendix I for our sampling methodology.

Figure 1: Results of a Review of a Random Sample of 113 Separated Contractor Employees to Determine Whether Smart ID Cards Were Recovered



Source: Our analysis of documentation for a random sample of contractor employees who separated from contracts with the IRS.

We determined that the IRS documented the return of 17 (15 percent) of 113 Smart ID cards associated with contractor employees in our random sample. This documentation included either a Form 13716-A or destruction log with the serial number of the Smart ID card for the separating contractor employee.[13] Based on the results shown in Figure 1, we estimate that the IRS cannot verify the return of Smart ID cards for 523 (85 percent)[14] of the more than 600 contractor employee separations from April 1, 2015, through March 31, 2016.

This occurred because FMSS Security office employees either did not retain or did not document serial numbers for the return of Smart ID cards on Form 13716-A and destruction logs, as required by IRS guidelines. Our analysis of Forms 13716-A and destruction logs for our random sample of 113 contractor employee separations identified the following:

- **Forms 13716-A** – Of the 113 Forms 13716-A requested, only three (3 percent) of 113 documented the serial number for the return of a Smart ID card. The remaining

[13] While we determined that documentation existed for the return of 17 Smart ID cards, we found that cards were generally not destroyed within 18 hours of separation, as required by IRS guidelines. We notified the IRS of this issue in a prior audit and executive management took corrective actions. 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).

[14] 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 479 and 557. See Appendix IV.

Forms 13716-A documented an unknown number other than the serial number of the Smart ID card (four forms), the ID number of the contractor employee instead of the Smart ID serial number (51 forms), or were not provided (55 forms).

- **Destruction Logs** – Of the 113 destruction logs requested, only 15 (13 percent) of 113 documented the serial number for the return of a Smart ID card. The remaining destruction logs documented the contractor employee ID number instead of the Smart ID serial number (45 destruction logs), contained unusable information (two destruction logs), or were not provided (51 destruction logs).

FMSS Security office management did not provide oversight to require employees to document Forms 13716-A and destruction logs with Smart ID card serial numbers, as required. This documentation is necessary to establish that a specific Smart ID card was recovered because Smart ID cards can be marked as destroyed on USAccess without the cards being recovered.

Documentation did not account for the recovery of 96 Smart ID cards for separated contractor employees

The IRS did not provide documentation showing that Smart ID cards for 96 (85 percent) of 113 contractor employees in our random sample were recovered. As previously stated, this occurred because the FMSS Security offices either did not provide Forms 13716-A or destruction logs, or the documentation provided did not include serial numbers documenting the return of the Smart ID cards. We performed additional analyses of the destruction logs, the deactivation and destruction dates in USAccess, and the last IRS computer system or facilities access by the contractor employee and identified the following:

- Seventy-nine Smart ID cards associated with contractor employees in our sample were marked as deactivated and destroyed in USAccess. We also found that eight of the 79 former contractor employees accessed systems, according to access logs, after IRS records show the contractor separated. In these instances, IRS management provided reasonable explanations for the accesses.[15]
- Seventeen Smart ID cards associated with contractor employees in our sample were either not marked as destroyed in USAccess[16] or had conflicting information regarding the cards' use and destruction. In addition, logs show that several of the contractors associated with these 17 cards accessed IRS facilities and systems after their separation date; however, IRS officials could not provide explanations, or determine whether Smart ID cards were used, for these accesses.

[15] For example, several of the system accesses were made by former contractor employees who we were informed later became IRS employees. We verified that the system accesses were made after the former contractor employees became IRS employees.
[16] The Smart ID card for one contractor employee was still active in USAccess.

While the FMSS Security office is responsible for issuing and recovering Smart ID cards for contractor employees, the contractor employees are generally not employed by the FMSS Security office, and the office does not always have accurate information about when contractor employees separate. We identified the following issues that emphasize the importance of documenting serial numbers for the return of Smart ID cards on Forms 13716-A and destruction logs when contractor employees separate.

- The IRS system that records separation dates of contractor employees is not always accurate or up-to-date. For example, a contractor employee's contract may be extended or the contractor employee may move to another contract without the FMSS Security office being notified.
- Contractor employees may have been issued multiple Smart ID cards over time. For example, the original card may have expired after the five-year life of the Smart ID card and been replaced with a new card, the contractor employee may have left IRS employment and received a new Smart ID card when returning to IRS employment, the contractor employee may have become an IRS employee and been issued a new Smart ID card, or the contractor employee may have lost the original Smart ID card and been issued a replacement. The USAccess computer system will indicate Smart ID cards were deactivated and destroyed, but will not always provide the dates of these actions.[17]
- Contractor employees may be issued more than one type of identification card that can be used to access facilities. For example, contractor employees may be issued Smart ID cards and a key card,[18] both of which can be used to access IRS facilities. The IRS system used to record accesses to IRS facilities only identifies the individual who accessed the facility and not the specific identification card that was used to gain entry.
- Smart ID cards are not always used to access IRS computer systems. A Smart ID card is normally required to access IRS computer systems, but employees and contractor employees are allowed to access the computer systems with an employee name and password, if their Smart ID card is not available. The IRS system used to record accesses to IRS computer systems only identifies the individual who accessed the system and not whether a Smart ID card was used for the access.

Due to the sensitivity of data housed by the IRS, it is imperative that the IRS ensure that Smart ID cards are recovered or accounted for.

Management began taking corrective action during the audit

During the audit, we notified IRS executive management of the security concerns we identified and they stated the following actions had been taken to address the issues.

[17] The destruction date is only available for the last Smart ID card in USAccess.
[18] Key cards are used to access some buildings and secure offices, but differ from building to building.

- In a January 25, 2017, conference call, Smart ID card deactivation and destruction procedures were discussed and FMSS Security offices were reminded to document the Smart ID card serial number on Form 13716-A when a Smart ID card is recovered.
- In October 2016, the Agency-Wide Shared Services organization began sending Contractor Separation and Contractor Access Denial reports to local FMSS Security offices. The Contractor Separation Report includes the most recent list of contractors who have separated from the IRS and do not require access to IRS facilities or systems. The Contractor Access Denial Report includes contractors who have received a final denial memo for staff-like access to all IRS facilities or systems by IRS Personnel Security. Contractors included on the reports should no longer be accessing IRS facilities or systems and should have physical access removed and all security items returned to the local FMSS Security office.

In addition, IRS management stated that in February 2016, as a corrective action for a prior TIGTA audit,[19] the FMSS Security office began sending an e-mail to the General Services Administration for all buildings where the IRS is a tenant when a contractor employee separates from the IRS. The e-mail informs the General Services Administration that the contractor should be denied access to the building.

Recommendations

The Chief, Agency-Wide Shared Services, should:

Recommendation 1**:** Develop a process to provide reasonable assurance that Smart ID card serial numbers are documented on Forms 13716-A and destruction logs when contractor employees separate, retain this documentation to enable reconciling unreturned Smart ID cards, and require managers to assure this process is followed.

> ***Management's Response:*** The Acting Chief, Agency-Wide Shared Services, agreed with this recommendation and by September 30, 2018, will develop a process to provide reasonable assurance that Smart ID card serial numbers are documented when contractor employees separate, retain this documentation to enable reconciling unreturned Smart ID cards, and require managers to assure this process is followed.

Recommendation 2: Perform follow-up work on separated contractor employees who, according to access logs, accessed an IRS computer or facility after separation. If it is determined that a contractor employee accessed an IRS computer or facility when they were no longer authorized to make such accesses or someone else was inappropriately using a separated

[19] 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).

contractor employee's identification to access systems or facilities, this information should be referred to the Treasury Inspector General for Tax Administration Office of Investigations.

Management's Response: The Acting Chief, Agency-Wide Shared Services, agreed with this recommendation and by February 28, 2018, with assistance from Information Technology as needed, will perform follow-up work on separated contractor employees who, according to access logs, accessed an IRS facility or computer after separation and determine whether they were authorized to make the access. If it is determined the access was inappropriate, the information will be referred to the Treasury Inspector General for Tax Administration Office of Investigations.

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 Smart ID cards are returned when contractor employees separate from the IRS. To accomplish our objective, we:

I. Assessed whether controls were designed to provide reasonable assurance that Smart ID cards are returned when contractor employees separate from the IRS by reviewing the Internal Revenue Manual and holding discussions with IRS management to identify controls for retrieving and documenting the receipt of Smart ID cards and marking Smart ID cards as deactivated and destroyed in USAccess.

II. Determined whether designed controls were functioning to provide reasonable assurance that Smart ID cards are returned when contractor employees separate from the IRS.

A. Obtained computer extracts from the Personal Identity Verification Background Investigation Process system[1] for the period April 1, 2015, through July 30, 2016, 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 select information to USAccess data when reviewing the sample of cases in Step II.F.

B. Performed analysis of the Personal Identity Verification Background Investigation Process system and identified the population of contractor employees who separated from their contract between April 1, 2015, and March 31, 2016, and did not return to a subsequent IRS contract by July 30, 2016.

C. Obtained USAccess computer extracts of all active contractor employee Smart ID cards, by month, for the period April 2015 through July 2016, 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 select information to the Personal Identity Verification Background Investigation Process system data when reviewing the sample of cases in Step II.F.

D. Compared the Personal Identity Verification Background Investigation Process system population of contractor employees who separated from their contract between April 1, 2015, and March 31, 2016, to the USAccess extracts of all active contractor employee Smart ID cards for the period April 2015 through July 2016 to

[1] The Personal Identification Verification Background Investigation Process is an IRS system designed to track and report on contractors before, during, and after the background investigation process, from on-boarding through separation from the contract.

identify the population of separated contractor employees who had been issued Smart ID cards by the IRS.

E. Selected a statistically valid random sample[2] of 113 contractor employees from the population of 616 contractor employees who were issued Smart ID cards by the IRS and separated from their contract between April 1, 2015, and March 31, 2016. We used the following criteria to select our sample: 95 percent confidence level, 10 percent expected error rate, and ± 5 percent precision rate. We selected a statistically valid random sample so we could project our results across the population of separated contractor employees. A contract statistician reviewed our sampling plans and projections.

F. Determined whether Smart ID cards were returned, deactivated, and destroyed timely when contractor employees separated from their IRS contract by reviewing Forms 13716-A, *Request for ID Media/Access Card for Contractor Employees,* destruction logs, and USAccess data for the random sample of 113 separated contractor employees identified in Step II.E.

G. Determined whether contractor employees for the random sample accessed IRS facilities or the IRS computer network after separation from their IRS contract.

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 documenting the recovery of Smart ID cards from separated contractor employees. We evaluated these controls by reviewing documentation and computer data supporting the recovery of Smart ID cards and interviewing management about actions taken when Smart ID cards are not returned. We also reviewed building and computer access data to determine if contractor employees in our random sample accessed IRS facilities and the IRS computer network after they separated from the IRS.

[2] We worked with a contract statistician to design a sampling plan to address our audit methodology.

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
Allen L. Brooks, Lead Auditor
Andrew J. Burns, Lead 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
Director, Employee Support Services, Agency-Wide Shared Services
Director, Facilities Management and Security Services, Agency-Wide Shared Services
Director, Office of Audit Coordination

Appendix IV

Outcome Measure

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

Type and Value of Outcome Measure:

Reliability of Information – Potential; 523 contractor employees whose separation documentation did not provide specific information showing that Government identification cards, known as Smart ID cards, were recovered when the contractor employees separated from the IRS (see page 4).

Methodology Used to Measure the Reported Benefit:

We requested Forms 13716-A, *Request for ID Media/Access Card for Contractor Employees*, and destruction logs for a random sample of 113 of the 616 contractor employees who separated from the IRS between April 1, 2015, and March 31, 2016. The IRS was either unable to provide these forms or unable to provide forms that included serial numbers to show that Smart ID cards were returned for 96 (85 percent) of the 113 Smart ID cards associated with contractor employees in our sample.

Based on our review of the random sample of separated contractors, we estimate that the IRS cannot verify that all Smart ID cards were recovered for 85 percent of the 616 contractor employees who separated from the IRS between April 1, 2015, and March 31, 2016, (616 * 0.85 = 523).[1]

[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 479 and 557.

Appendix V

Management's Response to the Draft Report

DEPARTMENT OF THE TREASURY
INTERNAL REVENUE SERVICE
WASHINGTON, DC 20224

CHIEF
AGENCY-WIDE
SHARED SERVICES

October 10, 2017

MEMORANDUM FOR MICHAEL E. MCKENNEY
DEPUTY INSPECTOR GENERAL FOR AUDIT

FROM: Richard L. Rodriguez
Acting Chief, Agency-Wide Shared Services

SUBJECT: Improved Controls Are Needed to Account for the Return of Contractor Employee Identification Cards (Audit # 201610020)

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 contractor employees separate from the Service. Your review and recommendations will assist us in that effort.

As noted in the report, we have designed controls to provide a reasonable assurance that SmartID cards are returned when contractor employees no longer work on IRS contracts. We agree with both recommendations and will develop and implement the corrective actions detailed in our attached response.

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 (703) 414-2143, or a member of your staff may contact David Abercrombie, Associate Director, FMSS Security Policy, at (703) 414-2122. For matters concerning audit procedural follow-up, please contact Kelly D. Smith, FMSS Audit Analyst, at (202) 317-4491.

Attachment

Attachment

TIGTA RECOMMENDATION #1:
The Acting Chief, Agency-Wide Shared Services (AWSS), should develop a process to provide reasonable assurance that Smart ID card serial numbers are documented on Forms 13716-A and destruction logs when contractor employees separate, retain this documentation to enable reconciling unreturned Smart ID cards, and require managers to assure this process is followed.

CORRECTIVE ACTION #1:
We agree with this recommendation. By September 30, 2018, the Acting Chief, Agency-Wide Shared Services, will develop a process to provide reasonable assurance that Smart ID card serial numbers are documented when contractor employees separate, retain this documentation to enable reconciling unreturned Smart ID cards, and require managers to assure this process is followed.

IMPLEMENTATION DATE:
September 30, 2018

RESPONSIBLE OFFICIAL:
Acting Chief, Agency-Wide Shared Services

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 Acting Chief, AWSS, should perform follow-up work on separated contractor employees who, according to access logs, accessed an IRS computer or facility after separation. If it is determined that a contractor employee accessed an IRS computer or facility when they were no longer authorized to make such accesses or someone else was inappropriately using a separated contractor employee's identification to access systems or facilities, this information should be referred to the Treasury Inspector General for Tax Administration Office of Investigations.

CORRECTIVE ACTION #2:
We agree with this recommendation. By February 28, 2018, the Acting Chief, Agency-Wide Shared Services, with assistance from Information Technology (IT) as needed, will perform follow-up work on separated contractor employees who, according to access

logs, accessed an IRS facility or computer after separation and determine whether they were authorized to make the access. If it is determined the access was inappropriate, the information will be referred to Treasury Inspector General for Tax Administration Office of Investigations.

IMPLEMENTATION DATE:
February 28, 2018

RESPONSIBLE OFFICIAL:
Acting Chief, Agency-Wide Shared Services

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

2