TREASURY INSPECTOR GENERAL FOR TAX ADMINISTRATION

Private Collection Agency Security Over Taxpayer Data Needs Improvement

July 30, 2018

Reference Number: 2018-20-039

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.

PRIVATE COLLECTION AGENCY SECURITY OVER TAXPAYER DATA NEEDS IMPROVEMENT

Highlights

Final Report issued on July 30, 2018

Highlights of Reference Number: 2018-20-039 to the Commissioner of Internal Revenue.

IMPACT ON TAXPAYERS

The IRS shares sensitive taxpayer data with Private Collection Agencies (PCA) for tax administration purposes. IRS and Federal guidelines require that sensitive data be protected during transmission and at the agencies' sites to prevent unauthorized access or disclosure.

WHY TIGTA DID THE AUDIT

The Fixing America's Surface Transportation Act mandated the use of qualified tax collection contractors to collect inactive tax receivables. The IRS contracted with four PCAs to collect tax receivables on behalf of the Government. These PCAs are required to secure these data. This audit was initiated to evaluate the data protection measures of the PCAs participating in the IRS's Private Debt Collection Program.

WHAT TIGTA FOUND

The PCAs established secure environments for housing taxpayer data which included access and control policies for managing taxpayer data, procedures for employees who telework, and systems access logs that are monitored and reviewed to prevent employee browsing of taxpayer data.

However, the IRS was unaware that one PCA could not provide monthly vulnerability scans of systems containing taxpayer data, and three of the four PCAs were not timely remediating critical- and high-risk vulnerabilities within the required 30 calendar days. In addition, PCA reporting requirements should be updated to ensure that the IRS is apprised of the risk associated with the PCAs' vulnerabilities.

Also, the IRS did not enforce Publication 4812, *Contractor Security Controls,* requirements for cell phone use policy specific to IRS data nor ensure that data were encrypted before transferring it to the PCAs.

Finally, three of the four PCA mailrooms where taxpayer correspondence and payments are received were not included in the IRS's annual security assessments. One PCA did not have a secure mail processing area for payments and did not secure misdirected payments prior to sending them to the IRS. Also, one PCA did not back up video footage, and three PCAs did not back up their video footage to an offsite location.

WHAT TIGTA RECOMMENDED

TIGTA recommended that the IRS update and enforce Publication 4812 to remediate critical- and high-risk vulnerabilities within 30 calendar days, clarify all devices that should have vulnerability scans, and ensure timely communication of scan results to the IRS. The IRS should also require that policies be specific on mobile devices connected to systems containing sensitive information and include a mechanism to enforce the policy.

TIGTA also recommended that the IRS perform annual assessments of the PCAs' mailrooms; perform follow-up assessments for any deficiencies identified; and implement stronger security controls over mailrooms receiving taxpayer correspondence and payments, including enhanced security camera coverage to record all sensitive areas. Finally, the IRS should ensure that all taxpayer data at rest being transferred to the PCAs are encrypted.

In its response, IRS management agreed with six of our eight recommendations. The IRS plans to timely communicate all vulnerabilities, develop policies on the use of mobile devices, perform annual security assessments over mailrooms, and perform a feasibility study to identify possible options for ensuring data at rest are encrypted. For the two partially agreed to recommendations, the IRS did not address the enforcement of vulnerability remediation and the inclusion of all devices when scanning for vulnerabilities. TIGTA believes that the IRS should complete these items.

TREASURY INSPECTOR GENERAL
FOR TAX ADMINISTRATION

DEPARTMENT OF THE TREASURY

WASHINGTON, D.C. 20220

July 30, 2018

MEMORANDUM FOR COMMISSIONER OF INTERNAL REVENUE

FROM: Michael E. McKenney
Deputy Inspector General for Audit

SUBJECT: Final Audit Report – Private Collection Agency Security Over Taxpayer Data Needs Improvement (Audit # 201720010)

This report presents the results of our review to evaluate the data protection measures of the Private Collection Agencies participating in the Internal Revenue Service's (IRS) Private Debt Collection Program. This audit is included in the Treasury Inspector General for Tax Administration's Fiscal Year 2018 Annual Audit Plan and addresses the major management challenge of Security Over Taxpayer Data and Protection of IRS Resources.

Management's complete response to the draft report is included as Appendix 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 Danny R. Verneuille, Assistant Inspector General for Audit (Security and Information Technology Services).

Table of Contents

Abbreviations

CUI	Controlled Unclassified Information
FMSS	Facilities Management and Security Services
IRM	Internal Revenue Manual
IRS	Internal Revenue Service
NIST	National Institute of Standards and Technology
PCA	Private Collection Agency
POA&M	Plan of Action and Milestones
SB/SE	Small Business/Self-Employed

Background

On December 4, 2015, the President signed into law the Fixing America's Surface Transportation Act,[1] which included provisions amending Internal Revenue Code Sections (§§) 6306[2] and 6307[3] pertaining to the use of qualified tax collection contractors to collect inactive tax receivables. To address this legislative mandate, the Internal Revenue Service (IRS) established a new Private Debt Collection Program and selected four Private Collection Agencies (PCA) – CBE Group, ConServe, Performant, and Pioneer Credit. The IRS enabled these designated contractors to collect outstanding inactive tax receivables on the Government's behalf.

Because taxpayer accounts contain Internal Revenue Code § 6103 tax return information and Personally Identifiable Information, it is critical that the data are secure when they leave the IRS facilities.

The Small Business/Self-Employed (SB/SE) Division has overall responsibility for the administration of the Private Debt Collection Program. In addition, the implementation and monitoring of the program involves other IRS functions. For example, the Information Technology organization's Applications Development and Enterprise Operations organizations provide support for data transfers to and from the PCAs, while the Cybersecurity office provides cybersecurity assessments and monitoring of the PCAs. The Facilities Management and Security Services (FMSS) office provides physical security assessments of the PCAs.

As a general rule, all information technology systems operated by or on behalf of the Department of the Treasury are required to be adequately protected to ensure confidentiality, integrity, and availability in order to minimize the risk of unauthorized access, use, disclosure, disruption, modification, or destruction. Because taxpayer accounts shared with the PCAs contain Internal Revenue Code § 6103[4] tax return information and Personally Identifiable Information,[5] it is critical that these data remain secure when they leave the IRS and are being processed by the PCAs. The IRS previously issued Publication 4812,[6] *Contractor Security Controls*, which is based on National Institute of Standards and Technology (NIST) Special Publication 800-53 (Revision 4),[7] as it pertains to information technology assets owned and managed at contractor sites. This publication defines basic security controls and standards required of contractors when

[1] Pub. L. No. 114-94 (2015).
[2] I.R.C. § 6306, Qualified tax collection contracts.
[3] I.R.C. § 6307, Special compliance personnel program account.
[4] I.R.C. § 6103, Confidentiality and disclosure of returns and return information.
[5] See Appendix IV for a glossary of terms.
[6] *Contractor Security Controls*, IRS Pub. 4812 (Rev. 10-2015).
[7] NIST Special Publication 800-53 (Revision 4), *Security and Privacy Controls for Federal Information Systems and Organizations* (Apr. 2013).

they have access to, develop, operate, host, or maintain IRS tax data or information systems for tax administration purposes outside of IRS facilities or outside of the direct control of the IRS.

The following are examples of the general security control requirements.

- The contractor shall develop a process that demonstrates how contract employees are approved for access, prior to being authorized access to information technology assets used for IRS work.
- The contractor shall establish and document usage restrictions, configuration/connection requirements, and implementation guidance for each type of remote access allowed and authorize remote access to the information system prior to allowing such connections.
- Contractors must maintain ongoing awareness of their information system and related security control processes to ensure compliance with security controls and adequate security of information and to support organizational risk management decisions.
- All workstations, servers, network, or mobile computing devices shall undergo monthly vulnerability scanning.
- For any security reports issued to the contractor, including internal independent reviews, the contractor is responsible for developing a Plan of Action and Milestones (POA&M) that identifies corrective actions and/or mitigating controls for any identified vulnerabilities.
- All returns and return information and other Controlled Unclassified Information (CUI)[8] shall be physically or logically partitioned within the information system and/or the information technology environment of the contractor site to ensure that this sensitive information is not commingled with the information of any other party or entity and is accessible only to authorized personnel.
- Contractors shall develop policies for any allowed portable and mobile devices when these information systems contain CUI data. The policies shall document the approved or disapproved use of mobile devices to connect to information technology assets hosting IRS information.
- The contractor or designee shall monitor physical access to CUI data and the information systems in which IRS information is stored to detect and respond to physical security incidents.
- The contractor shall identify and enable auditable events that shall allow the contractor to detect, deter, and report on suspicious activities.

[8] Effective November 14, 2016, Controlled Unclassified Information replaces the designation of Sensitive But Unclassified, per Executive Order 13556, *Controlled Unclassified Information*, 75 FR 68675 (Nov. 2010).

As a failsafe, the IRS added a clause within the PCA contracts that states the IRS reserves the unilateral right to recall all accounts and cancel task orders if the Contracting Officer determines that it is in the Government's best interest to do so. The IRS also reserves the right to award additional task orders to additional contractors at any time the Contracting Officer determines that it is in the Government's best interest.

In order for the PCAs to conduct their business for the IRS, the PCAs have multiple facilities where debt collection activities (collection centers) may be separate from the data centers that house the computer infrastructure. In addition, each of these facilities may also have a secondary location that is used as a backup facility in a geographically diverse location. In the event of a disaster, work will be performed and processed at the backup facility. This review was performed at the following PCA locations (in alphabetical order by PCA name).

- CBE Group in Cedar Falls and Waterloo, Iowa.
- ConServe in Cheektowaga, Fairport, and Henrietta, New York.
- Performant in Lathrop, Livermore, and Santa Clara, California.
- Pioneer Credit in Fishers, Indiana, and Horseheads, New York.

We also used information obtained from the IRS's SB/SE Division, the Information Technology organization's Cybersecurity, Applications Development, and Enterprise Operations offices, and the FMSS office during the period May 2017 through February 2018. We conducted this performance audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objective. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objective. Detailed information on our audit objective, scope, and methodology is presented in Appendix I. Major contributors to the report are listed in Appendix II.

Results of Review

When hiring private companies as contractors, the IRS is allowing external entities to perform or support the Federal Government's tax administration duties, and needs to ensure that these private companies maintain the same high level of security standards and protect taxpayer data against unauthorized access or misuse. For the IRS's Private Debt Collection Program, the IRS provides taxpayer account information to the four PCAs so they can fulfill their contractual goal of collecting delinquent taxes that the IRS itself cannot collect or has deemed uncollectible based on its scarce resources. The IRS has the expectation that the PCAs will maintain security controls and protective measures over tax data within their operations.

The IRS addressed security issues by completing certain important tasks prior to sending taxpayer data to the PCAs in the spring of 2017. For example, the IRS provided sufficient security guidance, requirements, and training so the PCAs understood and acknowledged their responsibility to protect taxpayer data in their possession. In addition, the Cybersecurity, Security Risk Management office conducted readiness visits to the PCAs to assess the initial state of security of their networks and facilities based on Publication 4812. To facilitate data transfers between the IRS and the PCAs and ensure the security of taxpayer account information, the IRS used its Enterprise File Transfer Utility process and tested specific directories in the Secure Data Transfer program in which the PCAs can access data downloads.

We found that the PCAs have a secure and dedicated infrastructure for housing taxpayer data, authentication and access control policies and procedures were working as intended for access management to IRS data, and processes for employee terminations and transfers. All PCAs complied with the IRS's record retention policy.[9] While not all PCAs have telework agreements, they have alternative agreements and policies and procedures for employees who telework or work from alternative work sites. Finally, the PCAs were also monitoring and reviewing system access logs to identify potential browsing violations of taxpayer data.

Although the IRS assessed the network and physical security of the PCAs and performed follow-up reviews, we identified areas of improvement to ensure the confidentiality, integrity, and availability of taxpayer data. Specifically, additional attention is needed to address system vulnerability scans, the physical security of misdirected taxpayer payments,[10] and the electronic transfer of taxpayer data. Addressing these security areas will improve the security posture of the PCAs while maintaining taxpayer data and collecting taxpayer debt.

[9] As of November 2016, the IRS Records Officer informed the Private Debt Collection Program that they were to retain all Private Debt Collection Program records until a formal disposition/retention plan is approved and updated to align with Servicewide Records Control Schedule Documents.
[10] Tax payments that should not have been mailed to the PCA.

Unknown and Unresolved Network Vulnerabilities Could Expose Taxpayer Data to Unauthorized Access

One of the basic tenets of network security is the periodic monitoring and scanning for network vulnerabilities and timely remediation of the vulnerabilities in order to reduce the exposure of exploiting vulnerabilities. The information technology landscape is dynamic and always evolving in order to become more efficient and secure. Hardware and software vendors are constantly identifying bugs and glitches within their components and issuing fixes to patch these weaknesses. Users must be diligent to identify weaknesses and take appropriate actions to minimize the chance of these weaknesses being exploited.

During our review, we identified that one PCA was not performing monthly vulnerability scans of systems as required by the IRS contract, three of the four PCAs were not always remediating vulnerabilities within required time frames, and all four PCAs were not reporting vulnerabilities identified on systems. In addition, one PCA's policy was silent on the use of cell phones connecting to systems that could store or process IRS data.

The IRS is not ensuring that PCAs are performing monthly and complete vulnerability scans and reviewing the scan results

Vulnerability scanning is a process that tests workstations, servers, and network or mobile computing devices for security weaknesses or flaws. The test relies on vulnerability scanning software that is configured to inspect devices for missing updates, patches, and common configuration problems. Vulnerability scanners are commonly used in organizations to identify known vulnerabilities on hosts and networks and on commonly used operating systems and applications. These scanning tools proactively identify vulnerabilities, provide a fast and easy way to measure exposure, identify out-of-date software versions, validate compliance with an organizational security policy, and generate alerts and reports about identified vulnerabilities.

Publication 4812 requires monthly vulnerability scanning on information technology assets. We requested three consecutive months of vulnerability scans for the months of April through June 2017 from the four PCAs. However, one of the four PCAs could not provide us scans for three consecutive months because, per PCA personnel, it did not have any scan data prior to June because its system was not running at that time. Subsequently, the PCA clarified its previous statement and stated that it had the May and July scans, but not the June scan. The PCA did not provide a reason why it could not provide the June scan. To assist in our analysis, we requested the August scan so we would have consecutive months of July and August 2017. However, the PCA stated that the upgraded system deleted scan data more than 30 calendar days old so it could not provide the August scan. We notified the IRS of the situation; it was not aware of the PCA scanning issue.

In addition, one of the four PCAs provided us with the scan result for only one workstation for the month of July. We found that Publication 4812 did not explicitly state that all components are to be scanned. Publication 4812, System Integrity requirement #2, states:

> *Contractors shall identify, report, and correct information system flaws. The contractor shall promptly install security-relevant software updates (e.g., patches, service packs, and hot fixes). Software and firmware updates related to flaw remediation shall be tested for effectiveness and potential side effects before installation. Flaws discovered during security assessments, continuous monitoring, incident response activities, or information system error handling shall be addressed expeditiously.*

In lieu of this omission in Publication 4812, Internal Revenue Manual (IRM) 10.8.1 which takes precedent over Publication 4812, states that automated mechanisms shall be employed, at a minimum monthly, to determine the state of information system components with regard to flaw remediation. All workstations (including laptops and mobile devices) shall be appropriately reviewed for security purposes, *e.g.*, checks for malicious code and updated virus protection software, critical software updates and patches, operating system integrity, disabled hardware, prior to connection or reconnection to the IRS network. Therefore, vulnerability scanning should include all devices that are connected to the PCA network for the Private Debt Collection Program. We determined that, based on the IRS's logical controls assessment, control System Integrity requirement #2 was not included.

Although the IRS required that monthly scans be performed by the PCAs, we determined that the IRS is not regularly reviewing the scan results. The IRS reviewed the results of PCA vulnerability scans only during its on-site annual assessments of the PCAs. As a result, the IRS was unaware of any of the issues we identified.

Hackers find weaknesses and flaws in those devices that are connected to the network. As a result of this lapse in vulnerability scanning, taxpayer data at the PCAs were at risk and could have been compromised.

The IRS is not requiring and enforcing timely remediation of critical- and high-risk vulnerabilities

Vulnerability scans are to be performed on the PCAs' workstations, servers, and network or mobile computing devices. The purpose of these scans is to apprise management of known vulnerabilities on their systems. According to IRM 10.8.2, critical- and high-risk vulnerabilities are to be remediated within 30 calendar days. However, Publication 4812 does not address the 30-calendar-day remediation timeline for vulnerabilities and should be updated to reflect the same standards the IRS follows. We analyzed two consecutive months of vulnerability scans for both servers and workstations to determine if the PCAs were timely remediating the vulnerabilities. Figure 1 shows unique critical- and high-risk vulnerabilities identified on servers and workstations not remediated within the required 30 calendar day time frame.

Figure 1: PCAs' Unique Critical- and High-Risk Vulnerabilities Not Remediated Within 30 Calendar Days

PCA (in random order)	Servers (Critical and High Risks)	Workstations (Critical and High Risks)
PCA #1	67	260
PCA #2	3	0
PCA #3	85	Data Not Provided
PCA #4	0	0

Source: Treasury Inspector General for Tax Administration analysis of two consecutive monthly scans for PCAs' servers and workstations from April to October 2017, depending on the availability of reports for each PCA.

Our review determined that only one of the four PCAs remediated all critical- and high-risk vulnerability factors identified during the two months reviewed. The other three PCAs had vulnerabilities which were not remediated within the required 30 calendar days. The critical risk factors have a range of 9 - 10 rating (highest) on the Common Vulnerability Scoring System. Known exploits exist for a large number of these vulnerabilities, which could lead to the exposure of Personally Identifiable Information as occurred when Equifax did not patch its vulnerabilities in a timely fashion.

The IRS is not informed of the PCAs' security postures

Contractor Security Assessments are on-site evaluations performed by the IRS to assess and validate the effectiveness of security controls established to protect IRS information and information systems. Publication 4812 requires that vulnerabilities identified during these annual assessments or an independent contractor assessment be reported and tracked on a POA&M. The contractor is responsible for developing a POA&M that identifies corrective actions and/or mitigating controls for any identified vulnerabilities. The POA&Ms shall be provided to the IRS Contracting Officer Representative or delegate quarterly, demonstrating progress toward weakness remediation.

During our visitations, we requested the POA&Ms from the four PCAs. Two of the four PCAs did not have a POA&M because all issues found during the IRS annual assessment were corrected prior to our request. The other two PCAs provided us with a POA&M. We determined that the first PCA had corrected its critical- and high-risk vulnerabilities. The second PCA did not correct the critical- and high-risk vulnerabilities within the required 30 calendar days, and the vulnerabilities remained on its POA&M for several months after the IRS performed its assessment.

Information security continuous monitoring is defined as maintaining ongoing awareness of information security, vulnerabilities, and threats to support organizational risk management decisions. Publication 4812 also requires the PCAs to perform monthly vulnerability scans as

part of continuous monitoring, but it does not require identified issues to be listed on a POA&M and tracked. As a result, the IRS would be unaware of any vulnerabilities identified during monthly scanning on the PCAs' machines until the annual or any follow-up visitations. The PCAs are not required to send any reports or notification of their monthly scans to the IRS nor report the vulnerabilities and the number of machines affected. Therefore, we believe the current Publication 4812 requirements do not ensure that the IRS is adequately informed about the true security posture of the PCAs.

In addition, one of the four PCAs initially provided us with a high-level overview presentation of vulnerabilities on its computer systems instead of their raw scan data. We compared the presentation data to the raw scan data that the PCA provided and identified a large discrepancy between the vulnerabilities reported to the IRS and the total number of vulnerabilities on its systems. We determined that the PCAs were reporting the number of vulnerabilities; however, they did not detail the number of machines each vulnerability affected. For example, if it reported one critical vulnerability, that one vulnerability could actually be present on 30 servers which significantly increases the risk than if it was a single instance in the server environment. Figure 2 reflects the results of our analysis of two months of raw scan data to identify the unique vulnerabilities and, for transparency, the actual number of instances that those vulnerabilities were present in the server environment.

Figure 2: Actual Number of Vulnerabilities of the PCAs

PCA (in random order)	Month One Unique Vulnerabilities	Month One Instances in the Server Environment	Month Two Unique Vulnerabilities	Month Two Instances in the Server Environment
PCA #1	15	27	25	85
PCA #2	9	37	1	3
PCA #3	49	339	42	188
PCA #4	10	19	3	5

Source: Treasury Inspector General for Tax Administration analysis of monthly vulnerability scans provided by the PCAs from April to October 2017, depending on the availability of reports for each PCA.

The unique vulnerabilities are a combined total of both critical- and high-risk vulnerabilities that need to be corrected within 30 calendar days. The figure shows a significant difference when the vulnerability is applied to the number of affected machines in the server environment. Knowing how widespread the vulnerability is throughout the components that are used for the IRS contract gives a better picture of the PCAs' security postures. With this information, the IRS knows the risk involved with its data at the contractor sites.

Although the PCAs are compliant with the current reporting requirements and the IRS is compliant with performing annual assessments, these activities do not allow the IRS to be cognizant of the overall security posture of the PCAs. For example, our analysis of the monthly

vulnerability scan results showed that the IRS annual assessment of PCA vulnerabilities does not accurately reflect the magnitude of the risks identified by the scans. Because the IRS did not require the PCAs to notify it of vulnerabilities from the monthly scans, the IRS was unaware that one PCA could not provide the monthly scans for our review and the number of machines affected by the critical- and high-risk vulnerabilities. Until the IRS requires this information from the PCAs, the IRS will not have a true sense of the PCAs' security posture.

The IRS should ensure that risks associated with the PCAs' mobile devices are minimized

Organizations should assume that all mobile devices are vulnerable unless the organization has properly secured them and monitors their security continuously while in use with enterprise applications or data. During our visit to one of the PCAs, we observed an information technology executive who plugged their phone into their laptop. When we asked why they would need to plug the phone into the laptop, the executive responded that it was to download music files. Publication 4812 does not allow the use of personal cell phones in the IRS contract environment. We also determined that this PCA's policy is silent on whether employees can use company-issued devices for downloading personal information from the Internet while connected to the network. Further, we did not identify any policy specific to cell phones connecting directly to the IRS CUI as required by Publication 4812. The IRS stated that it was unaware cell phones were being connected to the network by the PCA's information technology staff. The IRS annual security assessment was only a review of first-level cell phone usage by employees responsible for contacting taxpayers, not all employees.

Publication 4812 specifically states that contractors shall develop policies for any allowed portable and mobile devices when these information systems contain CUI data. This includes the use of BlackBerry devices, cellular phones, iPhones, *etc*. The policies shall document the approved or disapproved use of mobile devices to connect to information technology assets hosting IRS information. Non-business personally owned information systems shall never be used to handle IRS information. Publication 4812 also requires that all devices connected to the network must be scanned. However, we did not identify any policies for the PCAs that required employees to have their cell phones scanned monthly. We also did not receive any scan results from the PCAs that included cell phones.

Allowing mobile devices into the work environment comes with risks. Because mobile devices primarily use non-organizational networks for Internet access, organizations normally have no control over the security of the external networks the devices use. Communications systems may include wireless mechanisms such as Wi-Fi and cellular networks. These communications systems are susceptible to eavesdropping, which places sensitive information transmitted at the risk of compromise. Man-in-the-middle attacks[11] may also be performed to intercept and modify

[11] A form of active wiretapping attack in which the attacker intercepts and selectively modifies communicated data to masquerade as one or more of the entities involved in a communication association.

communications. Unless it is certain that the mobile device will be used only on trusted networks controlled by the organization, organizations should plan their mobile device security on the assumption that mobile devices are not secure and cannot be trusted.

Recommendations

Recommendation 1**:** The Chief Information Officer should update Publication 4812 to require the remediation of critical- and high-risk vulnerabilities within 30 calendar days and clarify that vulnerability scans should include all devices that process and store IRS information or are connected to the PCA network.

> ***Management's Response:*** The IRS partially agreed with this recommendation. The IRS is in the process of updating the current policy for vulnerability remediation. This policy will change the remediation time frame for high-risk vulnerabilities. The IRS will ensure that the next version of Publication 4812 is updated to reflect the remediation timeline in accordance with the IRM.
>
> ***Office of Audit Comment:*** The IRS's partial agreement did not address our recommendation to include all devices that process and store IRS data or are connected to the contractor's network when scanning for security vulnerabilities. We believe that the IRS should ensure all devices are scanned because security vulnerabilities on a single device can allow a bad actor to infiltrate the contractor's network, and possibly expose IRS data to unauthorized access and disclosure or adversely affect connectivity on the contractor's network.

Recommendation 2: The Chief Information Officer and the Director, Headquarters Collection, SB/SE Division, should ensure that monthly vulnerabilities of the PCAs' systems are timely communicated to the IRS. This continuous monitoring reporting will provide the IRS with a better assessment of the overall security posture of the PCAs and reduce the risk to the Private Debt Collection Program.

> ***Management's Response:*** The IRS agreed with this recommendation. The IRS will update the procedures to ensure that the monthly vulnerabilities of the PCAs' systems are timely communicated to the IRS.

Recommendation 3: The Chief Information Officer and the Director, Headquarters Collection, SB/SE Division, should enforce the timely remediation of critical- and high-risk vulnerabilities within 30 calendar days or consider removing the PCA from the Program.

> ***Management's Response:*** The IRS partially agreed with this recommendation. The IRS will update procedures in the Private Debt Collection Program Operations Guide to ensure the timely remediation of critical and high-risk vulnerabilities within 30 calendar days, per Publication 4812, and will consider removing the PCA from the program if they are not timely.

Office of Audit Comment: The IRS's partial agreement focused on updating procedures as opposed to enforcing the remediation of critical- and high-risk vulnerabilities within 30 calendar days. We believe that the IRS should enforce the timely remediation of these vulnerabilities to minimize the exposure and possible exploitation of existing vulnerabilities on the contractor's network.

Recommendation 4**:** The Chief Information Officer and the Director, Headquarters Collection, SB/SE Division, should require PCAs' policies to be specific on the use of mobile devices connecting to the PCA network and include a mechanism for enforcing the policy.

Management's Response: The IRS agreed with this recommendation, which was completed in February 2018. Specific PCA policies on the use of mobile devices has been added, and this requirement has been incorporated into the IRS's annual assessment of each site.

Physical Security Measures Need Improvements to Ensure That Payments and Data Are Protected Against Theft

Prior to the receipt of taxpayer account information by the PCAs, the FMSS office assessed the physical security of the collection center and headquarter facilities of the PCAs. The FMSS office generally found that the physical security of the four PCAs' facilities met the Publication 4812 standards. The FMSS office identified issues in which items were still lacking such as an authorized list of employees allowed to remove property from the premises, documentation explaining the process and procedures for receipt and logging of electronic CUI data, and an Intrusion Detection System.

We assessed the physical security measures of both the collection and data centers, and the security controls within the mailrooms and mail processing areas of all four PCAs. We determined that the physical access controls were working as intended and the restricted areas such as the collection, data, and mail processing areas had limited access. Three of the four PCAs had a separate secure space for extracting mail. Security cameras recorded video footage for various doors and restricted areas in all the PCAs' facilities. However, we determined that security controls could be enhanced in the following areas.

The IRS did not assess the security of the PCAs' mailrooms and mail processing areas

The FMSS office has the task of conducting all physical security assessments on the PCAs. For three of the four PCAs, we determined that the FMSS office did not perform a physical security assessment of the PCAs' mailrooms or mail processing areas.

Publication 4812 states for all information systems that house CUI, the contractor shall authorize and control information system-related items entering and exiting the facility, and maintain appropriate records of those items. If mailrooms are used, controls shall be put in place to ensure

that mail is also controlled. However, the IRS's annual assessments were performed prior to the start of the program and before misdirected payments were sent to the PCAs. This coupled with the fact that all CUI data were sent electronically to the PCAs may have contributed to some miscommunication on the part of the IRS in not assessing the mailrooms or mail processing areas. In addition, the current policy that requires an assessment be performed annually would not have identified these weaknesses until much later.

Publication 4812 does not cover specific controls for when misdirected payments are received. Because the mailroom and processing areas are high risk and the PCAs are receiving payments similar to those received by IRS lockbox sites, we determined that Lockbox Site Guidelines should be added to the FMSS office assessments. Lockbox Site Guidelines are very specific on security controls, such as separating mailroom processing from other business processes, and security camera coverage and recording.

Without assessing the security of the mailrooms and mail processing areas, the IRS may not realize the risk that taxpayer payments are vulnerable to theft. Ensuring that higher security standards are implemented in high-risk areas at the PCAs mitigates the risk of theft and ensures continued trust in the Private Debt Collection Program.

Security over taxpayer misdirected payments needs improvement

To illustrate the significance of not assessing the security of the mailroom and mail processing areas, we determined whether misdirected payments were coming into the PCAs. Taxpayers whose accounts are assigned to the PCAs are instructed to send payments directly to the IRS. However, some taxpayers still inadvertently send payments directly to the PCA. During our review, we found that, from June through November 2017, all four PCAs received more than 200 "misdirected" payments totaling more than $150,000.

If a PCA receives a taxpayer payment, the PCA is required to send the check "as is" via overnight traceable mail to the IRS within one business day. Until the check is sent, it should be stored in a locked metal container that requires two people to access.

During our site visit to a PCA, we observed a courier envelope containing taxpayer checks left in an open wire tray on a file cabinet next to an exit door. We did not identify any security camera that monitored or captured video of the area, and the tray was not secure. The envelope remained in the tray unsecured until the courier came to pick it up. This same PCA had more than 63 employees with physical access to the mailroom where all incoming mail is processed. However, only 12 of the 63 employees are authorized IRS contracted employees, and only three of the 12 employees are approved to open IRS and taxpayer correspondence.

Areas that receive taxpayer payments, even when unexpected, should enforce high security standards that are equivalent to other IRS sites that receive taxpayer payments. Payments that are left in an unsecured area creates an opportunity for theft.

The PCAs should implement higher standards for security camera coverage of IRS contract areas

The purpose of a security camera system is to reduce risk and to assist with the deterrence, detection, surveillance, and investigation of incidents or potential incidents relevant to the protection of information and facilities. Areas and functions that need appropriate visual coverage are mailrooms, opening and printing of taxpayer correspondence, taxpayer payments received and sent to the IRS, and other areas with sensitive taxpayer data.

We reviewed the security controls for visual coverage over taxpayer data provided by the four PCA facilities. We found that one PCA did not provide security cameras in areas where taxpayer correspondence was received and letters printed, sensitive shred documents were stored, and mail was transported, sorted, and delivered.

We also identified that three of four PCAs did not store backup video footage of IRS contract areas at alternate off-site locations.

- One of the PCAs did not create backups of video footage. All video footage from security cameras was on a stand-alone system at the site where it was recorded, not a networked system.
- The other two PCAs had a networked system to view the video footage and backed up the taxpayer information; however, neither one stored the footage at an alternate location.
- One PCA stored the footage at an alternate off-site location.

We determined that Publication 4812 does not address video camera footage or specifications in-depth. Appendix D of the publication states, "*Placement of cameras is largely driven by risk or potential risk. High risk areas must be effectively covered and include the following areas: Doors that permit access, data centers, and controlled rooms.*" However, there are no specifications on the types of cameras, how they are networked, or the extent of recording time.

Current IRS Lockbox Security Guidelines are specific for high-risk areas where taxpayer payments are received. For example, these guidelines require video recordings be retained for one year for high-risk areas and six months for low-risk areas.

Without appropriate visual coverage for high-risk areas, the PCAs increase the risk that taxpayer data are exposed to potential loss, damage, theft, or destruction. Backup video recordings stored at off-site locations may help determine the cause or source of an incident that may happen at a facility. Without live backup data, it is difficult to determine if suspicious activities can be investigated immediately and action taken as necessary if taxpayer information is comprised.

Recommendations

The Director, Headquarters Collection, SB/SE Division, should provide oversight to ensure that:

Recommendation 5**:** Physical security assessments of the mailrooms and mail processing sites are conducted annually for the Private Debt Collection Program.

> ***Management's Response:*** The IRS agreed with this recommendation. The IRS will create procedures in the Private Debt Collection Program Operations Guide that will ensure that the physical security assessments of mailrooms and mail processing sites are conducted annually.

Recommendation 6: Follow-up assessments are performed within the same year for any deficiencies identified in the annual assessment.

> ***Management's Response:*** The IRS agreed with this recommendation. The IRS will create procedures in the Private Debt Collection Program Operations Guide that will ensure that follow-up assessments for any deficiencies are performed within the same year.

Recommendation 7: Stronger security controls are included in the annual assessments such as the Lockbox Security Guidelines, including a separate secure room for mail processing and securing payments, and enhancing security camera coverage to include record times of all sensitive areas where taxpayer data are present.

> ***Management's Response:*** The IRS agreed with this recommendation. The IRS will update security controls to mirror the requirements in the Lockbox Security Guidelines, as applicable, for future assessments. The updated requirements will be used during the Fiscal Year 2019 annual assessments of the PCAs.

Taxpayer Data Transfers Need Increased Security

We identified that end-to-end encryption is not enforced for the transferring of taxpayer data to the PCAs. According to IRM 10.8.1, IRS sensitive data, *i.e.*, Controlled Unclassified Information, Personally Identifiable Information, that is processed, stored, or transmitted by an information system outside of IRS facilities or IRS information system shall be protected with Federal Information Processing Standards-validated encryption. In addition, all encryption implementations shall use Federal Information Processing Standards 140-2 (or later) validated encryption.

The process for transferring cases to the PCAs requires a secure tunnel for transmission of the data. The data at rest prior to being transmitted are located in a folder that is specific to each PCA. The PCA retrieves the data from the specific folder. We determined that the data at rest in the specific folders were not encrypted before transit and after transit once it reached the PCA.

The data owners, the SB/SE Division, would be responsible for ensuring that the data files are encrypted prior to being transferred. However, the data owners were unaware that it was their responsibility and assumed that the IRS function that delivers Secure File Transfers was responsible. The Secure File Transfer function does not need to know what is on the files; therefore, they should not have viewable access to the data. The data should be encrypted before reaching this function and should remain encrypted until reaching the employees at the PCAs who are authorized to have the data.

When the data at rest are not encrypted, unauthorized disclosure of taxpayer information can occur because the file containing the data is unencrypted and anyone with access to the file can read the information. Therefore, taxpayer data are at risk of unauthorized browsing.

Recommendation

Recommendation 8**:** The Chief Information Officer should ensure that the data at rest being transferred to the PCAs are encrypted at the IRS and at the PCA.

> ***Management's Response:*** The IRS agreed with this recommendation. The IRS will perform a feasibility study to determine the ability and possible solution to encrypt files at rest inside the firewall before being sent to Secure Data Transfer services for transmission between the IRS and the PCAs. Based on those findings, the IRS will determine the appropriate action needed and generate a new corrective action for this recommendation. Any approved actions will also include options for ensuring that the PCAs maintain the encrypted data at rest within their systems.

Appendix I

Detailed Objective, Scope, and Methodology

Our overall objective was to evaluate the data protection measures of the PCAs participating in the Private Debt Collection Program. To accomplish our objective, we:

I. Assessed the interconnecting controls for transferring data between the IRS and the PCAs to determine if taxpayer data are protected during all data transmissions.

- A. Determined if the Secure Data Transfer recommendations were implemented specifically for transferring taxpayer data from the IRS to the PCAs.
- B. Determined if the four PCAs' systems are compatible with the IRS for end-to-end encryption or if the IRS has accepted the risk when they are not compatible.
- C. Determined if the new Private Debt Collection Data Transfer Component for sending taxpayer information back to the IRS is secure.

II. Assessed the physical security controls at the PCAs to determine if taxpayer data are secure.

- A. Determined if the physical security processes for gaining access at the PCAs' collection and data centers are secure.
- B. Assessed how often reviews are performed to reconcile authorized access and identify unauthorized access.
- C. Assessed the physical security controls for allowing employees to telecommute.
- D. Evaluated physical security over payments (checks) and associated taxpayer information directly received from taxpayers.

III. Assessed the logical security controls at the PCAs to determine if taxpayer data are secure.

- A. Assessed the four PCAs' vulnerability scans for two months to determine if vulnerabilities exist and are mitigated timely. We determined that the data were sufficiently reliable. We obtained the raw Nessus scan data from the PCAs and developed a script to identify any irregularities. No irregularities were identified.
- B. Determined if workstations are secure.
- C. Determined if the four PCAs' access controls are adequate to protect taxpayer data.
- D. Assessed the PCAs' audit trail process to determine if they are adequate to prevent taxpayer browsing by employees.

E. Determined if the four PCAs' processes for disposing of taxpayer data are secure.

IV. Evaluated whether IRS oversight of security at the PCAs is sufficient.

A. Evaluated whether the IRS's oversight of the PCAs in accordance with Publication 4812, *Contractor Security Controls*, is adequate.

V. Determined whether the IRS's oversight of secure data transfers was adequate.

Internal controls methodology

Internal controls relate to management's plans, methods, and procedures used to meet their mission, goals, and objectives. Internal controls include the processes and procedures for planning, organizing, directing, and controlling program operations. They include the systems for measuring, reporting, and monitoring program performance. We determined that the following internal controls were relevant to our audit objective: Internal Revenue Code Sections 6103,[1] 6306,[2] and 6307;[3] NIST Special Publication 800-53 Revision 4;[4] IRM 10.8.1;[5] IRS Publication 4812;[6] and related IRS guidelines for physical security controls. We evaluated these controls by conducting visitations and meetings with the PCAs that contracted with the IRS, the IRS's SB/SE Division and Enterprise Operations organization, the FMSS office, and the Information Technology organization Cybersecurity and Applications Development offices. We also reviewed relevant documentation.

[1] I.R.C. §6103, Confidentiality and disclosure of returns and return information.
[2] I.R.C. §6306, Qualified tax collection contracts.
[3] I.R.C. §6307, Special compliance personnel program account.
[4] NIST Special Publication 800-53 (Revision 4), *Security and Privacy Controls for Federal Information Systems and Organizations* (Apr. 2013).
[5] IRM 10.8.1, *Information Technology Security, Policy and Guidance*, July 2015.
[6] *Contractor Security Controls*, IRS Pub. 4812 (Rev. 10-2015).

Appendix II

Major Contributors to This Report

Danny Verneuille, Assistant Inspector General for Audit (Security and Information Technology Services)
Kent Sagara, Director
Joseph Cooney, Audit Manager
Cari Fogle, Lead Auditor
Suzanne Westcott, Senior Auditor
Thomas Martin, Information Technology Specialist

Appendix III

Report Distribution List

Deputy Commissioner for Operations Support
Deputy Commissioner for Services and Enforcement
Commissioner, Small Business/Self-Employed Division
Chief Information Officer
Deputy Chief Information Officer for Operations
Associate Chief Information Officer, Applications Development
Associate Chief Information Officer, Cybersecurity
Chief, Facilities Management and Security Services
Director, Collection, Small Business/Self-Employed Division
Director, Security Risk Management
Senior Operations Advisor, Small Business/Self-Employed Division
Director, Office of Audit Coordination

Appendix IV

Glossary of Terms

Attack	An attempt to gain unauthorized access to system services, resources, or information, or an attempt to compromise system integrity.
Common Vulnerability Scoring System	A Security Content Automation Protocol specification for communicating the characteristics of vulnerabilities and measuring their relative severity.
Continuous Monitoring	The process implemented to maintain a current security status for one or more information systems or for the entire suite of information systems on which the operational mission of the enterprise depends. The process includes: 1) the development of a strategy to regularly evaluate selected Information Assurance controls/metrics; 2) recording and evaluating relevant events and the effectiveness of the enterprise in dealing with those events; 3) recording changes to controls or changes that affect risks; and 4) publishing the current security status to enable information-sharing decisions involving the enterprise.
Contracting Officer	Processes and negotiates complex procurements. Performs contract administration involving extensions of periods of performance.
Contracting Officer Representative	The principal program representative assigned to Government procurements. The primary role of the Contracting Officer Representative is to provide technical direction, monitor contract performance, and maintain an arm's-length relationship with the contractor, ensuring that the Government pays only for the services, materials, and travel authorized and delivered under the contract.

Controlled Unclassified Information	A categorical designation that refers to unclassified information that does not meet the standards for National Security Classification under Executive Order 12958, as amended, but is (i) pertinent to the national interests of the United States or to the important interests of entities outside the Federal Government, and (ii) under law or policy requires protection from unauthorized disclosure, special handling safeguards, or prescribed limits on exchange or dissemination. Henceforth, the designation Controlled Unclassified Information replaces "Sensitive But Unclassified."
Data at Rest	In the context of data handling systems, data at rest refers to data that are being stored in stable destination systems. Data at rest are frequently defined as data that are not in use or are not traveling to system endpoints, such as mobile devices or workstations.
Eavesdropping Attack	An incursion in which someone tries to steal information that computers, smartphones, or other devices transmit over a network. An eavesdropping attack takes advantage of unsecured network communications in order to access the data being sent and received. Eavesdropping attacks are difficult to detect because they do not cause network transmissions to appear to be operating abnormally.
Enterprise File Transfer Utility	An IRS proprietary program that automates the delivery of files from hundreds of projects throughout the organization. It was first deployed in 2006 and is a major component of data exchange in the IRS.
Federal Information Processing Standard	A standard for adoption and use by Federal departments and agencies that has been developed within the Information Technology Laboratory and published by the NIST, a part of the U.S. Department of Commerce. A Federal Information Processing Standard covers some topic in information technology in order to achieve a common level of quality or some level of interoperability.

Lockbox Site	In the Lockbox program, the U.S. Treasury agrees to let certain financial institutions process individual and business tax payments. Financial institutions, or sites, deposit the taxpayer's payment and forward any tax forms or documentation to the IRS as quickly and efficiently as possible. The nationwide Lockbox Network was established on behalf of the U.S. Treasury, the IRS, and the Fiscal Service. As a fiduciary of the IRS, the Lockbox Network processes sensitive, private information pertaining to U.S. citizens, financial information, proprietary information, and mission-critical information. The Lockbox Network has a legal obligation to protect the confidentiality of tax returns and related information.
National Institute of Standards and Technology	Under the Department of Commerce, this organization is responsible for developing standards and guidelines for providing adequate information security for all Federal Government agency operations and assets.
Personally Identifiable Information	Information which can be used to distinguish or trace an individual's identity, such as their name, Social Security Number, or biometric records, alone or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, or mother's maiden name.
Plan of Action and Milestones	A document that identifies tasks needing to be accomplished. It details resources required to accomplish the elements of the plan, any milestones in meeting the tasks, and scheduled completion dates for the milestones.

Publication 4812, *Contractor Security Controls*	Functions as the standard for security controls to be employed by contractors that will have or need access to IRS information, and/or will have or need access to maintain or operate IRS information systems in order to perform or carry out and meet their contractual obligations. Publication 4812 is a "layperson's guide" to NIST Special Publication 800-53[1] when access to IRS information or information systems under contracts for services on behalf of the IRS is outside of IRS-controlled facilities or the direct control of the IRS (as opposed to IRM 10.8.1 – *Information Technology Security, Policy and Guidance*, which applies when contractors are accessing IRS information and information systems at Government-controlled facilities).
Secure Data Transfer	A file-sharing information system used to securely exchange electronic files with external entities over the Internet. External entities may choose from multiple data extracts that make up the program.
Security Content Automation Protocol	A method for using specific standardized testing methods to enable automated vulnerability management, measurement, and policy compliance evaluation against a standardized set of security requirements.

[1] NIST Special Publication 800-53 (Revision 4), *Security and Privacy Controls for Federal Information Systems and Organizations* (Apr. 2013).

Appendix V

Management's Response to the Draft Report

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

COMMISSIONER
SMALL BUSINESS/SELF-EMPLOYED DIVISION

June 22, 2018

MEMORANDUM FOR MICHAEL E. McKENNEY
DEPUTY INSPECTOR GENERAL FOR AUDIT

FROM: Mary Beth Murphy for Kirsten Wielobob
Commissioner, Small Business/Self-Employed Division

SUBJECT: Draft Audit Report – Private Collection Agency Security Over Taxpayer Data Needs Improvement (Audit # 201720010)

Thank you for the opportunity to review and comment on the above subject draft audit report. The Fixing America's Service Transportation (FAST) Act, enacted in December 2015, requires the IRS to enter into qualified collection contracts with private debt collection agencies for the collection of inactive tax receivables. The private collection agencies (PCAs) who do this work are required to secure all taxpayer data. The IRS is committed to protecting the security and the integrity of taxpayer data. To ensure these protections, the IRS initiated a controlled launch of the program in April 2017 when it contracted with four PCAs to initiate the private collection of certain overdue federal tax debts. Through an incremental implementation of the program, we increased the likelihood that the program would work effectively while at the same time ensuring the protection and security of taxpayer data. We appreciate your acknowledgement of our efforts to ensure the PCAs established secure environments for housing taxpayer data which included access and control policies for managing taxpayer data, procedures for employees who telework, and systems access logs that are monitored and reviewed to prevent employee browsing of taxpayer data.

Protecting taxpayer information from internal and external cyber security-related threats has been an IRS priority for many years. We are committed to continually improving data security controls. IRS data at rest is within a fully tested and secured system boundary that assures its confidentiality. Data transmissions are encrypted while in transit from the IRS to the PCA. In addition, transmission methods are tested annually to ensure security is maintained at the appropriate risk level. While we are confident in the security of the data, we will perform a feasibility study to determine our ability and possible solution to encrypt files at rest inside the firewall before being sent to Secure Data Transfer services for transmission between IRS and PCAs.

We agree with your recommendations and have already implemented one. We will update Publication 4812, *Contractor Security Controls*, and add processes to the

Private Debt Collection Operations Guidelines to ensure the annual assessments and follow-up assessments of the PCAs are completed timely.

Attached is a detailed response outlining our corrective actions to address your recommendations. If you have any questions, please contact me, or a member of your staff may contact Paul Mamo, Director, Collection, Small Business/Self-Employed Division.

Attachment

Attachment

RECOMMENDATION 1:
The Chief Information Officer should update Publication 4812 to require the remediation of critical- and high-risk vulnerabilities within 30 calendar days and clarify that vulnerability scans should include all devices that process and store IRS information or are connected to the PCA network.

CORRECTIVE ACTION:
We partially agree with this recommendation. The IRS is in the process of updating the current policy for vulnerability remediation. This policy will change the remediation timeframe for High Risk vulnerabilities. We will ensure that the next version of Publication 4812 is updated to reflect the remediation timeline in accordance with the IRM.

IMPLEMENTATION DATE:
January 15, 2019

RESPONSIBLE OFFICIAL:
Associate Chief Information Officer for Cybersecurity

CORRECTIVE ACTION MONITORING PLAN:
IRS will monitor this corrective action as part of our internal management system of controls.

RECOMMENDATION 2:
The Chief Information Officer and the Director, Headquarters Collection, SB/SE, should ensure that monthly vulnerabilities of the PCAs' systems are timely communicated to the IRS. This continuous monitoring reporting will provide the IRS with a better assessment of the overall security posture of the PCAs and reduce the risk to the Private Debt Collection Program.

CORRECTIVE ACTION:
We agree with this recommendation. We will update procedures to ensure the monthly vulnerabilities of the PCAs' systems are timely communicated to the IRS.

IMPLEMENTATION DATE:
August 15, 2018

RESPONSIBLE OFFICIAL:
Director, Headquarters Collection, Small Business/Self-Employed Division (SB/SE)

CORRECTIVE ACTION MONITORING PLAN:
IRS will monitor this corrective action as part of our internal management system of controls.

RECOMMENDATION 3:
The Chief Information Officer and the Director, Headquarters Collection, SB/SE, should enforce the timely remediation of critical- and high-risk vulnerabilities within 30 calendar days or consider removing the PCA from the Program.

CORRECTIVE ACTION:
We partially agree with this recommendation. We will update procedures in the PDC Operations Guide to ensure the timely remediation of critical and high-risk vulnerabilities within 30 calendar days, per Publication 4812, and will consider removing the PCA from the program if they are not timely.

IMPLEMENTATION DATE:
October 15, 2019

RESPONSIBLE OFFICIAL:
Director, Headquarters Collection, Small Business/Self-Employed Division

CORRECTIVE ACTION MONITORING PLAN:
IRS will monitor this corrective action as part of our internal management system of controls.

RECOMMENDATION 4:
The Chief Information Officer and the Director, Headquarters Collection, SB/SE, should require PCAs' policies to be specific on the use of mobile devices connecting to the PCA network and include a mechanism for enforcing the policy.

CORRECTIVE ACTION:
This recommendation was completed in February 2018. Specific PCA's policies on the use of mobile devices has been added. This requirement has been incorporated into our annual assessment of each site.

IMPLEMENTATION DATE:
Completed

RESPONSIBLE OFFICIAL:
Associate Chief Information Officer for Cybersecurity

CORRECTIVE ACTION MONITORING PLAN:
Not applicable.

RECOMMENDATION 5:
The Director, Headquarters Collection, SB/SE, should provide oversight to ensure that physical security assessments of the mailrooms and mail processing sites are conducted annually for the Private Debt Collection Program.

CORRECTIVE ACTION:
We agree with this recommendation. We will create procedures in the PDC Operations Guide that will ensure the Physical Security Assessments of mailrooms and mail processing sites are conducted annually.

IMPLEMENTATION DATE:
July 15, 2018

RESPONSIBLE OFFICIAL:
Director, Headquarters Collection, Small Business/Self-Employed Division

CORRECTIVE ACTION MONITORING PLAN:
IRS will monitor this corrective action as part of our internal management system of controls.

RECOMMENDATION 6:
The Director, Headquarters Collection, SB/SE, should provide oversight to ensure that follow-up assessments are performed within the same year for any deficiencies identified in the annual assessment.

CORRECTIVE ACTION:
We agree with this recommendation. We will create procedures in the PDC Operations Guide (POG) that will ensure follow-up assessments for any deficiencies are performed within the same year.

IMPLEMENTATION DATE:
October 15, 2018

RESPONSIBLE OFFICIAL:
Director, Headquarters Collection, Small Business/Self-Employed Division

CORRECTIVE ACTION MONITORING PLAN:
IRS will monitor this corrective action as part of our internal management system of controls.

RECOMMENDATION 7:
The Director, Headquarters Collection, SB/SE, should provide oversight to ensure that stronger security controls are included in the annual assessments such as the Lockbox Security Guidelines, including a separate secure room for mail processing and securing payments; and enhancing security camera coverage to include record times of all sensitive areas where taxpayer data is present.

CORRECTIVE ACTIONS:
1. The IRS will update security controls to mirror the requirements in the Lockbox Security Guidelines, as applicable, for future assessments.
2. The updated requirements will be used during the FY 2019 annual assessments of the PCAs.

IMPLEMENTATION DATES:
1. December 15, 2018
2. October 15, 2019

RESPONSIBLE OFFICIAL:
Director, Headquarters Collection, Small Business/Self-Employed Division

CORRECTIVE ACTION MONITORING PLAN:
IRS will monitor this corrective action as part of our internal management system of controls.

RECOMMENDATION 8:
The Chief Information Officer should ensure that the data at rest being transferred to the PCAs are encrypted at the IRS and at the PCA.

CORRECTIVE ACTION:
We agree with this recommendation. We will perform a feasibility study to determine the ability and possible solution to encrypt files at rest inside the firewall before being sent to Secure Data Transfer services for transmission between IRS and PCAs, and based on those findings, IRS will determine the appropriate action needed and generate a new corrective action for this recommendation. Any approved actions will also include options for ensuring the PCAs maintain the encrypted data at rest within their systems.

IMPLEMENTATION DATE:
August 15, 2019

RESPONSIBLE OFFICIAL:
Associate Chief Information Officer, Applications Development

5

CORRECTIVE ACTION MONITORING PLAN:
IRS will monitor this corrective action as part of our internal management system of controls.