TREASURY INSPECTOR GENERAL FOR TAX ADMINISTRATION

Private Collection Agencies Adequately Protected Taxpayer Data

March 26, 2008

Reference Number: 2008-20-078

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
Email Address | inquiries@tigta.treas.gov
Web Site | http://www.tigta.gov

TREASURY INSPECTOR GENERAL
FOR TAX ADMINISTRATION

DEPARTMENT OF THE TREASURY
WASHINGTON, D.C. 20220

March 26, 2008

MEMORANDUM FOR COMMISSIONER, SMALL BUSINESS/SELF-EMPLOYED DIVISION

Michael R. Phillips

FROM: Michael R. Phillips
Deputy Inspector General for Audit

SUBJECT: Final Audit Report – Private Collection Agencies Adequately Protected Taxpayer Data (Audit # 200820021)

This report presents the results of our review to determine whether private collection agencies (hereafter referred to as PCAs or contractors) were adequately protecting taxpayer data at the time of our review. This review was included in the Treasury Inspector General for Tax Administration Fiscal Year 2008 Annual Audit Plan and was part of the Information Systems Programs business unit's statutory requirements to annually review the adequacy and security of IRS technology.

Impact on the Taxpayer

The Internal Revenue Code authorizes the Internal Revenue Service (IRS) to enter into contracts with PCAs to assist in the collection of delinquent Federal Government tax liabilities. Our review found that taxpayer data provided to the PCAs under these contracts were adequately protected during transmission from the IRS and while stored on PCA computer systems. Inadequate security controls over taxpayer data provided to PCAs would create increased risks of unauthorized access, misuse, disclosure, modification, or destruction of taxpayer data.

Synopsis

Currently, the IRS has contracts with two PCAs to assist in the collection of delinquent Federal Government tax liabilities. As of February 2008, nearly 98,000 accounts had been provided to these contractors for resolution, representing more than $911 million. Under the terms of their

contracts with the IRS, PCAs must ensure that their computer systems are compliant with the Federal Information Security Management Act of 2002[1] and adhere to National Institute of Standards and Technology guidance. The National Institute of Standards and Technology's *Recommended Security Controls for Federal Information Systems* (Special Publication 800-53) outlines
17 families of computer security controls that should be implemented. These control families include systems and communication protection, access controls, and audit records.

We reviewed the computer security controls over taxpayer data provided to the two current PCAs and determined that the controls were adequate. In particular, files were securely transmitted from the IRS to the contractors and adequately secured on the contractors' systems. In addition, workstations used by contractor collection personnel were adequately controlled to prevent unauthorized copying of taxpayer information to removable media or transfer via email. The contractors also maintained adequate audit trails and performed periodic reviews, including reviews to identify unauthorized access to taxpayer data. We also identified best practices that should be considered by current and future PCAs to strengthen computer security controls.

Response

We made no recommendations in this report and, therefore, did not require a formal written response from the IRS. However, key IRS management officials reviewed the report prior to issuance and agreed with the results of our review.

Copies of this report are also being sent to the IRS managers affected by the report. Please contact me at (202) 622-6510 if you have questions or Margaret E. Begg, Assistant Inspector General for Audit (Information Systems Programs), at (202) 622-8510.

[1] Pub. L. No. 107-347, Title III, 116 Stat. 2946 (2002).

Table of Contents

Abbreviations

IRS	Internal Revenue Service
PCA; contractor	Private collection agency

Background

The Internal Revenue Code authorizes the Internal Revenue Service (IRS) to enter into contracts with private collection agencies (hereafter referred to as PCAs or contractors) to assist in the collection of delinquent Federal Government tax liabilities. Currently, the IRS has contracts with two PCAs to assist in this effort: Pioneer Credit Recovery, Inc. in Perry, New York; and The CBE Group, Inc. in Waterloo, Iowa. As of February 2008, the IRS had provided nearly 98,000 accounts to these contractors for resolution, representing more than $911 million.

Under the terms of their contracts with the IRS, PCAs must ensure that their computer systems are compliant with the Federal Information Security Management Act of 2002.[1] To meet this requirement, the contractors must implement and adhere to National Institute of Standards and Technology[2] guidance. The IRS also evaluates the integrity of a contractor's computer systems to ensure that appropriate access controls are in place to protect taxpayer data.

The taxpayer data provided by the IRS to the PCAs for use in collecting delinquent taxes include Social Security Numbers, names, addresses, and tax liability amounts. Due to the sensitivity of these data, it is paramount that strong measures are implemented to protect taxpayer information. Inadequate security controls over taxpayer data provided to contractors would create increased risks of unauthorized access, misuse, disclosure, modification, or destruction of taxpayer data.

We focused on the security controls over the transmission of data between the IRS and the contractors and the computer security controls used by the contractors to protect taxpayer data. This review was performed in the Small Business/Self-Employed Division in New Carrollton, Maryland, and the contractor worksites in Perry, New York, and Waterloo, Iowa, during the period December 2007 through February 2008. 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.

[1] Pub. L. No. 107-347, Title III, 116 Stat. 2946 (2002).
[2] The National Institute of Standards and Technology, under the Department of Commerce, is responsible for developing standards and guidelines for providing adequate information security for all Federal Government agency operations and assets.

Results of Review

Private Collection Agencies Implemented Adequate Security Controls Over Taxpayer Data

The National Institute of Standards and Technology's *Recommended Security Controls for Federal Information Systems* (Special Publication 800-53) outlines 17 families of security controls that should be implemented in Federal Government computer systems. These control families include systems and communication protection, access controls, and audit records. Under the terms of their contracts with the IRS, PCAs are required to comply with National Institute of Standards and Technology guidelines.

We reviewed the computer security controls over taxpayer data provided to the two current PCAs and determined that the controls were adequate to protect taxpayer data during transmission to the contractors and while stored on the contractors' computer systems. Specifically:

- The contractors securely obtained files from the IRS through the IRS Registered User Portal. Access to this Portal was limited to two users at each PCA who used their own Portal user account to download the files to the contractor systems.
- Files downloaded from the IRS were adequately secured on contractor systems. Each contractor had appropriately restricted access to the downloaded files to only those employees who needed to use the files in the performance of their duties.
- The contractors configured workstations used by their collection personnel to prevent copying files to the workstation or removable media. Collection personnel also did not have access to email. By using web-filtering software, the collectors' Internet access was limited to only a few sites they needed for locating taxpayer addresses and phone numbers. Printing was limited and printouts were adequately secured to prevent unauthorized removal.
- PCA user accounts we reviewed had the appropriate authorizations for access to contractor systems.
- All contractor employees hired within the last 6 months had completed background investigations. Because our March 2007 report[3] found that background investigations

[3] *The Private Debt Collection Program Was Effectively Developed and Implemented, but Some Follow-up Actions Are Still Necessary* (Reference Number 2007-30-066, dated March 27, 2007).

were adequately completed, we limited the scope of this review to the 6-month period prior to our site visits.

- Contractor collection and other employee access to the collection application were determined to be appropriate and based on business need.
- The contractors maintained adequate audit trails and performed periodic reviews, including reviews to identify unauthorized access to taxpayer data.
- The contractors do not delete taxpayer files or remove them from their systems once a case has been closed or recalled by the IRS, per the terms of their contracts. However, the contractors adequately protected these data by restricting access to taxpayer data files to only necessary employees. In addition, both contractors' computer applications categorized closed or recalled taxpayer cases to restrict their access to authorized managers and supervisors.

In addition, each contractor implemented a best practice that should be considered by current and future PCAs.

- One contractor requires a second password, in addition to a standard username and password, before access to the contractor's collection application is granted. This second password is generated through a password token device, small enough to fit on a key ring, which generates and displays a new password every 60 seconds. Each user accessing the contractor's application is given a device, which is synchronized with a secure server.
- The other contractor places files downloaded from the IRS on a dedicated server.

The PCAs also took steps to address control weaknesses identified in the March 2007 Treasury Inspector General for Tax Administration report previously cited and in IRS Safeguard reviews. We reviewed the weaknesses listed on their Plan of Actions and Milestones[4] and determined the contractors took appropriate actions to address the weaknesses. See Appendix IV for a list of all Treasury Inspector General for Tax Administration reports on the IRS private debt collection program.

[4] A Plan of Actions and Milestones is a management tool used to assist organizations in identifying, assessing, prioritizing, and monitoring the progress of corrective actions for security weaknesses found in programs and systems.

Appendix I

Detailed Objective, Scope, and Methodology

The overall objective of this audit was to determine whether PCAs were adequately protecting taxpayer data at the time of our review. To accomplish this objective, we:

I. Determined whether taxpayer data are transmitted securely between the IRS and the PCAs.

- A. Identified security requirements for the transmission of taxpayer data from sources such as the Internal Revenue Manual, National Institute of Standards and Technology guidance, and PCA contract documentation.
- B. Assessed the adequacy of controls over the transmission of taxpayer data between the IRS and the contractors.
- C. Identified the reasons for inadequacy of data transmission controls.
- D. Assessed the impact of inadequate control weaknesses on privacy and security of taxpayer data transmitted to and from the contractors.

II. Determined whether taxpayer data residing on PCA computer systems are secure.

- A. Identified security requirements for taxpayer data maintained on computer systems from sources such as the Internal Revenue Manual, National Institute of Standards and Technology guidance, and PCA contract language.
- B. Determined whether vulnerabilities identified in previous Treasury Inspector General for Tax Administration and IRS security reviews had been adequately addressed.
- C. Assessed the adequacy of data security controls over taxpayer data on PCA systems. Tests included assessing whether contractor employee access to taxpayer data was authorized and appropriate and evaluating the effectiveness of the contractors' audit trail management for systems maintaining taxpayer data. We also assessed the adequacy of background investigations for employees that were hired in the 6-month period prior to our site visits to the contractor worksites.
- D. Identified the reasons for inadequacy of data security controls.
- E. Assessed the impact of inadequate control weaknesses on privacy and security of taxpayer data residing at the PCAs.

III. Determined whether taxpayer data are appropriately disposed of after use by the PCAs.

A. Identified security requirements for the destruction of taxpayer data from sources such as the Internal Revenue Manual, National Institute of Standards and Technology guidance, and PCA contract language.

B. Assessed the adequacy of controls over destruction of taxpayer data on contractor systems.

C. Identified the reasons for inadequacy of data destruction controls.

D. Assessed the impact of inadequate control weaknesses on privacy and security of taxpayer data residing at the contractors' sites once the data are no longer needed.

Appendix II

Major Contributors to This Report

Margaret E. Begg, Assistant Inspector General for Audit (Information Systems Programs)
Stephen Mullins, Director
Michael Howard, Audit Manager
Richard Borst, Senior Auditor
Myron Gulley, Senior Auditor
Louis Lee, Senior Auditor
Thomas Nacinovich, Senior Auditor

Appendix III

Report Distribution List

Commissioner C
Office of Commissioner – Attn: Acting Chief of Staff C
Deputy Commissioner for Services and Enforcement SE
Director, Collection, Small Business/Self-Employed Division SE:S:C
Project Director, Filing and Payment Compliance Modernization, Small Business/Self-Employed Division SE:S:C:FPCMO
Chief Counsel CC
National Taxpayer Advocate TA
Director, Office of Legislative Affairs CL:LA
Director, Office of Program Evaluation and Risk Analysis RAS:O
Office of Internal Control OS:CFO:CPIC:IC
Audit Liaison: Commissioner, Small Business/Self-Employed Division SE:S

Appendix IV

Treasury Inspector General for Tax Administration Audit Reports on the Private Debt Collection Program

The Treasury Inspector General for Tax Administration has issued the following reports on the IRS private debt collection program:

1. *Management Needs to Continue Monitoring Some Case Selection Issues As the Private Debt Collection Program Is Implemented* (Reference Number 2006-30-064, dated April 2006).
2. *The Revised Private Debt Collection Request for Quotation Adequately Addressed Prior Deficiencies in the Solicitation Methodology* (Reference Number 2006-10-078, dated April 2006).
3. *The Private Debt Collection Program Was Effectively Developed and Implemented, but Some Follow-up Actions Are Still Necessary* (Reference Number 2007-30-066, dated March 27, 2007).
4. *Complete Actions Were Not Taken to Validate the Best Software Solution Was Chosen for the Private Debt Collection Program* (Reference Number 2007-20-065, dated April 10, 2007).
5. *Invoice Audit of Fees Paid Under the Private Debt Collection Initiative* (Reference Number 2008-10-054, dated December 26, 2007).