Some Taxpayers Were Not Appropriately Notified When Their Personally Identifiable Information Was Inadvertently Disclosed

May 24, 2011

Reference Number: 2011-40-054

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

Redaction Legend:
1 = Tax Return/Return Information

Phone Number | 202-622-6500
Email Address | TIGTACommunications@tigta.treas.gov
Web Site | http://www.tigta.gov

SOME TAXPAYERS WERE NOT APPROPRIATELY NOTIFIED WHEN THEIR PERSONALLY IDENTIFIABLE INFORMATION WAS INADVERTENTLY DISCLOSED

Highlights

Final Report issued on May 24, 2011

Highlights of Reference Number: 2011-40-054 to the Internal Revenue Service Deputy Commissioner for Operations Support.

IMPACT ON TAXPAYERS

Taxpayers need to be assured that the Internal Revenue Service (IRS) will promptly notify them of inadvertent disclosures of their Personally Identifiable Information so they can take the necessary steps to protect themselves from identity theft or other harm. The IRS has many processes and regulations that protect taxpayer information, but there are times when taxpayer information is inadvertently disclosed.

WHY TIGTA DID THE AUDIT

More than 142 million taxpayers entrust the IRS with sensitive financial and personal data. The objective of this audit was to determine whether the IRS is making appropriate decisions to promptly and properly notify taxpayers of inadvertent disclosures of their tax information.

WHAT TIGTA FOUND

TIGTA reviewed a statistical sample of 98 case files of incidents reported as inadvertent disclosures in Fiscal Years 2009 and 2010 and found not all taxpayers were properly and/or timely notified of disclosures.

- Five (5 percent) of 98 incidents were closed and taxpayers were not properly notified of the disclosures because IRS employees reporting the disclosures did not document the identity of the individuals whose Personally Identifiable Information had been disclosed.
- 10 (10 percent) of 98 incidents were closed and taxpayers were not properly notified of the disclosures because only tax account information was disclosed and IRS procedures did not include tax account information in its definition of Personally Identifiable Information.
- 20 (74 percent) of the 27 incidents in the 98 incidents sampled that required taxpayer notification were not sent timely. TIGTA considered notifications timely if taxpayers were sent notifications within 45 days of the date the incident was reported to or identified by the IRS. The notification letters in the sample averaged 86 days.

In addition, TIGTA reconciliations performed on the four systems the IRS uses to capture disclosure incident-related information identified 815 missing incidents.

WHAT TIGTA RECOMMENDED

TIGTA recommended that the IRS 1) educate employees on the importance of obtaining sufficient information on individuals whose Personally Identifiable Information was disclosed, 2) revise procedures to include tax account information in the Personally Identifiable Information definition and to forward disclosure incidents to the IRS's Identity Theft Program for victims of identity theft, 3) implement a timeliness measure, and 4) implement sufficient controls to ensure that all incidents are accurately documented and considered.

In the response to the report, the IRS agreed to the recommendations. The IRS has implemented a protection campaign to educate employees on data protection and plans to study whether tax account information should be included in the definition of Personally Identifiable Information. In addition, the IRS plans to strengthen procedures to address identity theft and expand current time metrics to include the elapsed time between initial incident reporting and taxpayer notifications date. It plans to consolidate all systems data for the most serious incidents.

TREASURY INSPECTOR GENERAL
FOR TAX ADMINISTRATION

DEPARTMENT OF THE TREASURY
WASHINGTON, D.C. 20220

May 24, 2011

MEMORANDUM FOR DEPUTY COMMISSIONER FOR OPERATIONS SUPPORT

Michael R. Phillips

FROM: Michael R. Phillips
Deputy Inspector General for Audit

SUBJECT: Final Audit Report – Some Taxpayers Were Not Appropriately Notified When Their Personally Identifiable Information Was Inadvertently Disclosed (Audit # 201040050)

This report presents the results of our review to determine whether the Internal Revenue Service is making appropriate decisions to promptly and properly notify taxpayers of inadvertent disclosures of their tax information. This audit is included in our Fiscal Year 2011 Annual Audit Plan and addresses the major management challenge of Taxpayer Protection and Rights.

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

Copies of this report are also being sent to the Internal Revenue Service managers affected by the report recommendations. Please contact me at (202) 622-6510 if you have questions or Michael E. McKenney, Assistant Inspector General for Audit (Returns Processing and Account Services), at (202) 622-5916.

Table of Contents

Abbreviations

CSIRC	Computer Security Incident Response Center
IRS	Internal Revenue Service
OMB	Office of Management and Budget

Background

Identity theft is the number one consumer complaint nationwide. Identity theft occurs when someone uses Personally Identifiable Information, such as an individual's name or Social Security Number, credit card numbers, or other account information, to commit fraud and other crimes. Another person's Social Security Number is the most valuable tool an identity thief can obtain to commit financial fraud, and the Social Security Number becomes even more valuable if it is linked to other personal data of the Social Security Number owner, such as information required to prepare a tax return. While the overall number of identity theft complaints dropped from Calendar Year 2009 to Calendar Year 2010, identity theft remains the single largest type of complaint submitted to the Federal Trade Commission's Consumer Sentinel Network with more than 1.3 million complaints received since Calendar Year 2006.

Personally Identifiable Information includes an individual's:

- Name.
- Address.
- E-mail Address.
- Social Security Number.
- Telephone Number.
- Bank Account Number.
- Date and Place of Birth.
- Mother's Maiden Name.
- Biometric Data (e.g., height, weight, eye color, finger prints).

More than 142 million taxpayers entrust the Internal Revenue Service (IRS) with sensitive financial and personal data. The IRS has many processes and regulations that protect taxpayer information, but there are times where taxpayer information is inadvertently disclosed. For example, an employee could inadvertently include Jane Smith's tax return in an envelope with Mary Smith's tax return and send it to Mary–thus inadvertently disclosing Jane's Personally Identifiable Information to Mary. Alternatively, at the taxpayer's request, the IRS could fax a copy of the taxpayer's tax return but use an incorrect fax number. When inadvertent disclosures happen and the risk of identity theft or other harm is likely, taxpayers need to be assured that the IRS will promptly notify them so they can take the necessary steps to protect themselves from identity theft or other harm.

Laws and regulations

Various laws require that Federal Government agencies protect Personally Identifiable Information and implement programs to provide security for Personally Identifiable Information and the systems on which it resides. In addition, the Internal Revenue Code prohibits the unauthorized disclosure of taxpayer information. Figure 1 provides a list of the various laws and regulations on disclosure of Personally Identifiable Information and/or taxpayer information.

Figure 1: Laws and Regulations Regarding Disclosure of Taxpayer Information

Privacy Act of 1974[1]	With specifically mentioned exceptions, no agency shall disclose any record which is contained in a system of records,[2] except pursuant to a written request by, or with the prior written consent of, the individual to whom the record pertains. Agencies with systems of records (e.g., taxpayer information) must establish appropriate administrative, technical, and physical safeguards to ensure the information contained in the records remains secure and confidential. This includes protecting the information against threats or hazards which could result in substantial harm, embarrassment, inconvenience, or unfairness to any individual on whom the agency maintains information. In addition, each agency shall keep an accurate accounting of the date, nature, and purpose of each disclosure to any person or agency, as well as the name and address of the person or agency to whom disclosure is made.
E-Government Act of 2002[3]	This Act established a Federal Chief Information Officer within the Office of Management and Budget to improve the methods by which Government information, including information on the Internet, is organized, preserved, and made accessible to the public. It established a framework of measures that require using Internet-based information technology to improve citizen access to Government information and services and for other purposes.
Federal Information Security Management Act of 2002[4]	This Act recognized the importance of information security to the economic and national security interests of the United States. The Act requires each Federal agency to develop, document, and implement an agency-wide program to provide information security for the information and information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source.

[1] 5 U.S.C. Section 552a (2006).
[2] The Privacy Act defines a system of records as a group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual.
[3] Pub. L. 107-347, 116 Stat. 2899; 44 U.S.C. Section 101.
[4] 44 U.S.C. Sections 3541 - 3549.

Internal Revenue Code Section 6103	Tax return information is confidential and no officer or Federal employee should disclose tax return information except as authorized. Section 6103(c) authorizes the Department of the Treasury Secretary to prescribe requirements and conditions that would allow officers and Federal employees to disclose tax return information to persons the taxpayer designates in a request for, or consent to, such disclosure.
Internal Revenue Code Section 7216	Section 7216 applies to any person who is engaged in the business of preparing or providing services in connection with the preparation of tax returns for compensation. Any such person who knowingly or recklessly discloses any information furnished to him or her for, or in connection with, the preparation of any such tax return, or uses any such information for any purpose other than to prepare, or assist in preparing, any such return, shall be guilty of a misdemeanor.

Source: Laws as cited.

Office of Management and Budget guidance

The Office of Management and Budget (OMB) has also issued numerous memoranda to Federal agencies providing guidance on how to handle and report disclosures. On July 12, 2006, the OMB issued Memorandum 06-19 (M-06-19), "Reporting Incidents Involving Personally Identifiable Information and Incorporating the Cost for Security in Agency Information Technology Investments," to Chief Information Officers stating that agencies are:

> *. . . to report all incidents involving Personally Identifiable Information (PII) to the United States Computer Emergency Readiness Team (US-CERT) within one hour of discovering the incident … and should not distinguish between suspected and confirmed breaches.*

On May 22, 2007, the OMB issued Memorandum 07-16 (M-07-16), "Safeguarding Against and Responding to the Breach of Personally Identifiable Information." This memorandum requires agencies to develop and implement a breach notification policy and outlines the framework within which agencies must develop this policy while ensuring proper safeguards are in place to protect the information. All Federal information and information systems are subject to the privacy and security requirements addressed in OMB M-07-16. Breaches subject to notification requirements include both electronic systems as well as paper documents.

Agencies must determine whether notification of a breach is required, stating:

> *. . . the agency should first assess the likely risk of harm caused by the breach and then assess the level of risk. Agencies should consider a wide range of harms, such as harm to reputation and the potential for harassment or prejudice, particularly when health or financial benefits information is involved in the breach. Agencies should bear in mind*

that notification when there is little or no risk of harm might create unnecessary concern and confusion. Additionally, under circumstances where notification could increase a risk of harm, the prudent course of action may be to delay notification while appropriate safeguards are put in place.

The Privacy, Information Protection, and Data Security Office

In Fiscal Year 2007, the IRS established the Privacy, Information Protection, and Data Security Office. Its mission supports four key programs.

- **Privacy Policy** to promote the protection of individual privacy and integrate privacy into business practices, behaviors, and technology solutions.
- **Identity Protection** to identify risks and reduce vulnerabilities for identity theft.
- **Incident Management** to improve victim assistance.
- **Online Fraud Detection and Prevention** to reduce online fraud against the IRS and taxpayers.

The Privacy and Information Protection Office is responsible for the Privacy Policy, Identity Protection, and Incident Management Programs. This Office develops and implements an enterprise-wide approach to privacy and information protection of taxpayer and employee information, supports identity theft initiatives such as implementing a number of indicators to mark taxpayer accounts affected by identity theft, and manages the IRS's process for responding to the loss of Personally Identifiable Information.

The Incident Management Program is responsible for ensuring IRS incidents involving the loss, theft, or disclosure of Personally Identifiable Information and the loss or theft of an IRS asset are investigated, analyzed, and resolved. Risk assessments are completed to evaluate the likely risk of harm, specifically the potential for identity theft. Potentially affected individuals who are determined to be at high risk of harm are notified without unreasonable delay. This office manages the reporting, taxpayer notification, and tracking of data loss incidents (Disclosure Notification Process) in accordance with OMB M-07-16.

This review was performed at the IRS National Headquarters in Washington, D.C., in the Privacy, Information Protection, and Data Security Office and the Incident Management Program during the period July 2010 to February 2011. We also held discussions and/or obtained documentation from the Office of Technology Computer Security Incident Response Center, the Small Business/Self-Employed Division Disclosure Office, and the Wage and Investment Division Office of Taxpayer Correspondence. We conducted this performance audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objective. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our

audit objective. Detailed information on our audit objective, scope, and methodology is presented in Appendix I. Major contributors to the report are listed in Appendix II.

Results of Review

The Disclosure Notification Process Needs Improvement to Ensure Taxpayers Are Appropriately Notified of Inadvertent Disclosures

Our review of a statistical sample of 98 case files of incidents reported as inadvertent disclosures in Fiscal Years 2009 and 2010 found that not all taxpayers were properly and/or timely notified of disclosures.

- 5 (5 percent) of 98 incidents were closed and taxpayers were not properly notified of the disclosures because IRS employees reporting the disclosure did not document the identity of the individuals whose Personally Identifiable Information had been disclosed.
- 10 (10 percent) of 98 incidents were closed and taxpayers were not properly notified of the disclosures because only tax account information was disclosed and IRS procedures did not include tax account information in its definition of Personally Identifiable Information.
- 20 (74 percent) of the 27 incidents in the 98 incidents sampled that required taxpayer notification were not sent timely. We considered notifications timely if taxpayers were sent notifications within 45 days of the date the incident was reported to or identified by the IRS. The notification letters in the sample averaged 86 days.

Twenty-one (21 percent) of 98 incidents were also closed without the IRS notifying taxpayers that their Personally Identifiable Information had been disclosed because the disclosure was made to individuals with power of attorney[5] responsibilities, State agencies, law firms, or payroll processors. The IRS considers that these individuals and businesses do not pose a likely risk of identity theft or other harm to taxpayers. In addition, in **********1********** **********1**********but the IRS took no further action on the case.

IRS records show that there were 4,081 inadvertent disclosures processed in Fiscal Years 2009 and 2010. Of these, 1,493 incidents required that 2,812 taxpayers be notified.[6] Without improvements to the Disclosure Notification Process, there is no assurance that all taxpayers who have had their Personally Identifiable Information inadvertently disclosed by the IRS will be properly identified and/or notified timely. Therefore, taxpayers may not take the proper precautions needed to protect themselves from identity theft or other harm.

[5] Taxpayers grant a power of attorney to an individual so that individual can represent the taxpayer before the IRS.
[6] Each incident may affect more than one taxpayer.

Management controls should provide reasonable assurance that all disclosures are appropriately recorded and considered. Systems used to record and track disclosures need to be complete and accurate with sufficient reviews to ensure all actions have been appropriate. Activities need to be established to monitor performance measures and indicators.

In Fiscal Year 2007, the IRS created the Incident Management Program to manage the reporting and notification for data loss incidents in accordance with OMB M-07-16

In September 2007, the IRS established the Incident Management Program to manage the IRS's Personally Identifiable Information Incident Notification Process for taxpayers and employees potentially affected by IRS data loss incidents. In 3 years, the IRS has:

- Developed procedures to comply with applicable laws and regulations.
- Developed various management information systems to report, control, and track disclosures and data losses.
- Provided guidance to IRS employees on disclosures and how to report them.[7]
- Established the Disclosure Notification Process and developed user desk guides and manuals for employees to follow when investigating, analyzing, and resolving incidents.

In Fiscal Year 2009, the IRS took several steps to improve its ability to report and assess potential breaches of Personally Identifiable Information. It revised incident reporting procedures, and due to the volume and complexity of taxpayer correspondence, determined that all taxpayer correspondence issues should first be reviewed by the IRS's Office of Taxpayer Correspondence.[8]

The Disclosure Notification Process

When sensitive information is lost, stolen, or inadvertently disclosed in any way, whether it be electronically, verbally, or in hardcopy form, IRS employees are required to report the incident within 1 hour. IRS guidelines state:

> *The timely reporting within one hour of all information losses or thefts is critical. This is so that any needed investigation can be initiated quickly to decrease or mitigate the possibility the information will be compromised and used to perpetrate identity theft or other forms of fraud.*

If an employee sees indications of an *intentional* unauthorized disclosure, the incident must be reported to the Treasury Inspector General for Tax Administration as soon as possible.

[7] See Appendix V for a description of the IRS Employee Instructions on Reporting Inadvertent Disclosures.
[8] The Office of Taxpayer Correspondence provides comprehensive correspondence services—from design and development to effectiveness and downstream impact.

The IRS determined that incidents involving notices should be submitted to the IRS Office of Taxpayer Correspondence. Employees in the Office of Taxpayer Correspondence determine if the disclosure meets criteria and if it does, the incident is reported to the Computer Security Incident Response Center (CSIRC). The CSIRC is a centralized reporting facility for all computer security privacy incidents.

The following are the steps in the Disclosure Notification Process for incidents not related to notices:[9]

Step One	When disclosure incidents involving Personally Identifiable Information occur, the incident is reported to the CSIRC. IRS employees report the incident using the CSIRC online reporting form or by calling 866-216-4809. The completed form is electronically submitted through the CSIRC portal creating a systemically numbered email to the CSIRC "Disclosure of Sensitive Data" mailbox.
Step Two	An employee in the Incident Management Program reviews the incident report emails received in the CSIRC "Disclosure of Sensitive Data" mailbox. An initial assessment is performed to determine if Personally Identifiable Information or "Sensitive But Unclassified" data are involved. If the incident appears to be an inadvertent unauthorized disclosure, it is entered into the CSIRC centralized Incident Tracking System[10] maintained by the IRS Modernization and Information Technology Services organization.
Step Three	The Incident Tracking System automatically assigns an Incident Response number to the new incident created and generates an email that is forwarded to the Incident Management Program "Personally Identifiable Information" mailbox. The email contains an incident summary to notify Incident Management Program employees a new incident has been created. To obtain incident details, an Incident Management Program employee emails the reporting employee and manager to request completion of the Personally Identifiable Information Analysis Template and the Impacted Taxpayer Data Spreadsheet.
Step Four	The Incident Tracking System is accessed to obtain incident details needed to establish a new incident on the E-Trak System.[11] The E-Trak System is used to control and track data breach, disclosure, loss, and theft incidents reported through the CSIRC. Incident Management Program employees perform a second assessment to evaluate the risk of harm for all reported IRS data loss incidents involving Personally Identifiable Information, based on standardized factors and

[9] See Appendix VI for a flowchart of the Disclosure Notification Process.
[10] The Incident Tracking System provides an automated process to capture, process, and track incident data and generate reports.
[11] The E-Trak System is an off-the-shelf case-tracking tool used to respond to a public law.

ratings criteria. After complete analysis, they will code the incident:

Orange Incident does not contain Personally Identifiable Information, so there is no risk of identity theft or other harm. Notification letters are not required.

Green The risk of identity theft or other harm is unlikely. Notification letters are not required.

Red The risk of identity theft or other harm is likely. Notification letters are required. Some cases are coded Red-No Notification if the risk of identity theft or harm is likely but the reporting business unit is unable to provide the names and Social Security Numbers of the potentially affected individuals.

Blue This data loss could compromise national security, is grand jury, or could compromise an ongoing investigation.

Incidents coded Orange and Red - No Notification are updated on the E-Trak System and closed without further actions. Code Blue incidents are forwarded to an Executive Team. Executive Summary Reports are generated for incidents coded Green and Red.

Step Five Incidents coded Green and Red are forwarded to the Incident Management Working Group for review. When approved, incidents coded Green are updated on the E-Trak System and closed. Incidents coded Red are updated on the E-Trak System and forwarded for additional review and approval.

Step Six Incidents coded Red are presented to IRS executives who are members of the Privacy and Information Protection Advisory Committee for approval and concurrence. If all concur, the potentially affected individuals are then notified of the data loss via Incident Management Breach Notification Letter (Letter 4281C).

The IRS also offers taxpayers 1 year of free credit report monitoring through a national credit reporting bureau. In addition, it inputs an identity theft data loss indicator on the taxpayers' accounts so the IRS can identify a taxpayer whose Personally Identifiable Information was lost or disclosed because of an IRS data loss incident. The E-Trak System is updated and the cases are closed.

The IRS codes incidents Orange or Green in four circumstances and will not send notifications

Guidance from the OMB states that upon learning of a disclosure, agencies should assess the likelihood that Personally Identifiable Information will be or has been used by unauthorized individuals. This is a difficult standard to measure because the IRS cannot know if those who

inadvertently come by another individual's Personally Identifiable Information or tax account information will use that information to cause harm. However, though there is a risk, it is reasonable to assume the risk is unlikely when a disclosure is inadvertently made to a third party that routinely handles Personally Identifiable Information or tax information, or has a trusted relationship with the IRS.

Accordingly, when considering whether a taxpayer is likely to be at risk of identity theft or other harm, the Incident Management Program developed procedures that state it will code incidents Orange or Green (i.e., the IRS will not send notifications or place indicators on the accounts) in the following four circumstances:

1. Where the IRS employee follows all IRS established procedures (e.g., mailed to address of record; provided with an incorrect fax number; caller subsequently determined not taxpayer after authentication requirements completed) but a disclosure of sensitive information still occurs. These are to be coded Orange.
2. Where the IRS transmits taxpayer Personally Identifiable Information to registered participants of the Income Verification Express Services Program.[12] These are to be coded Green.
3. Where the IRS sends the taxpayer's Personally Identifiable Information to an incorrect employer (one in which the taxpayer has no current or past relationship) originating from the IRS's Criminal Investigation Questionable Refund Detection Team or Accounts Management function Taxpayer Assurance Program. These are to be coded Green.
4. Where the IRS inadvertently discloses taxpayer account information (i.e., unfiled return or balance due information) to an individual who already has the personal or business information and the information disclosed is not categorized as Personally Identifiable Information. These are to be coded Orange.

Twenty-one (21 percent) of 98 incidents sampled were closed without the IRS notifying taxpayers that their Personally Identifiable Information had been disclosed to individuals and businesses that routinely handle Personally Identifiable Information and/or tax account information. The IRS considers certain third parties who routinely obtain or process Personally Identifiable Information and/or tax account information, such as individuals with a power of attorney, State agencies, or payroll processors, to present little or no risk of identity theft or other harm to the taxpayer. Therefore, it was determined that it was not necessary to notify the taxpayer of these disclosures.

[12] Taxpayers commonly request tax return transcripts for many reasons, including verifying income to obtain a loan. They can order the transcripts directly from the IRS or others can order the transcripts on the taxpayer's behalf. Lenders and other entities verify income information on behalf of a taxpayer through the IRS's Income Verification Express Services Program.

Data loss indicators are posted only for individuals with IRS tax accounts

A taxpayer's Master File[13] account should be marked with the identity theft data loss indicator on accounts where Letter 4281C has been issued. Thirty-two taxpayers were sent notification letters related to the 27 incidents in our sample that required a Letter 4281C. Of the 32 individuals:

- **********1**********.
- **********1**********.

Individuals who have had their Personally Identifiable Information disclosed may not have a tax account. In most instances, these individuals are spouses, children, or dependents of the primary taxpayer and the primary taxpayer has provided their names and Social Security Numbers on his or her tax return, which was inadvertently disclosed.

These spouses, children, or dependents may not currently have a filing obligation or have a tax account. In instances where Personally Identifiable Information for a minor child has been disclosed, notification letters are mailed to the parents, but credit monitoring is not provided if the minor child is the only individual affected and a data loss indicator is not placed on a tax account because the minor child does not have a tax account. The burden is shifted to the parent of a minor child to remain aware of consequences resulting from the inadvertent disclosure if and when they file a tax return of their own.

Not all cases included the identity of the individual whose Personally Identifiable Information was disclosed

In 5 (5 percent) of the 98 incidents, the incidents were closed code Red but without the IRS notifying taxpayers that their Personally Identifiable Information had been disclosed because the incident report did not include the identity of the individuals whose Personally Identifiable Information had been disclosed. Projected to the population of 4,081 inadvertent disclosures processed in Fiscal Years 2009 and 2010, there may have been 204 incidents where the IRS acknowledged Personally Identifiable Information had been disclosed but the IRS did not notify the affected taxpayers. This happened because IRS employees did not document the identities of the individuals whose Personally Identifiable Information was disclosed, even though the taxpayers' identities were obtainable.

Five percent of incidents sampled were closed without the IRS notifying taxpayers because the incident report did not include the identity of the individuals whose Personally Identifiable Information had been disclosed.

[13] The IRS database that stores various types of taxpayer account information. This database includes individual, business, and employee plans and exempt organizations data.

For example, a taxpayer calls the toll-free telephone lines and asks what he or she should do with a copy of another taxpayer's tax return when it was included in the envelope with the copy of the tax return he or she had requested. The assistor instructs the caller to mail it back to the IRS, but fails to ask for or document the name and Social Security Number of the taxpayer whose tax return was mistakenly included with the caller's.

However, there may be times when the employee is unable to determine the identity of the taxpayer whose information was inadvertently disclosed. For example, an employee may be stuffing notices into envelopes and realize, after the fact, a notice is missing and must have been stuffed into an envelope addressed to another taxpayer that had already gone out with the mail.

Taxpayers are not always contacted when the only information disclosed is tax account information

In 10 (10 percent) of the 98 incidents, tax account information was disclosed but the IRS closed the incident without notifying taxpayers that their tax account information had been disclosed. This happened because IRS procedures did not include tax account information in its definition of Personally Identifiable Information. Projected to the population of 4,081 inadvertent disclosures processed in Fiscal Years 2009 and 2010, there may have been 408 incidents where the IRS disclosed tax account information but the IRS did not notify the affected individuals.

This could occur when someone who has a relationship or prior relationship with a taxpayer (e.g., a spouse, former spouse, or business partner) calls the IRS asking for the taxpayer's account information. The assistor follows all IRS procedures to authenticate the caller, only later to find that the caller is not the taxpayer. The Incident Management Program codes this type of incident Orange, "Incident does not contain Personally Identifiable Information, so there is no risk of identity theft or other harm." An Executive Summary Report will not be prepared for this type of incident and the incident will be closed.

However, Personally Identifiable Information includes any information about an individual maintained by an agency, including any other information that is linked or linkable to an individual, such as:

- Medical.
- Educational.
- Financial.
- Employment.

Therefore, tax account information is Personally Identifiable Information. Assistors authenticate taxpayers by asking their name, Social Security Number, address, date of birth, and filing status. A caller with a relationship to the taxpayer may know all this information. However, the caller may be calling without the taxpayer's knowledge or permission to obtain information about the

taxpayer's tax account. While these individuals may not intend to steal or assume the taxpayer's identity, the taxpayer is at risk of other harm. For example, an ex-spouse or business partner may be calling to obtain information on the taxpayer's current income. Once this information is obtained, these individuals may use this information for any number of purposes, including legal actions that could potentially harm the taxpayer.

In August 2009, private investigators were sentenced after being convicted for illegally obtaining confidential medical records, tax records, and employment information by posing as the subjects of their investigations who had legitimate claim to the records. From January 2004 to May 2007, employees from a private investigation company posed as the people they were investigating to trick the targets into releasing sensitive information (e.g., Social Security Number, verifications, tax returns, and medical histories) and selling this information to other private investigators, law firms, and others. [14]

Private investigators used illegal methods to illegally obtain confidential information from Federal agencies.

OMB guidance instructs agencies to consider a number of possible harms associated with the loss or compromise of information. Harm may include the:

- Effect of a breach of confidentiality or fiduciary responsibility.
- Potential for blackmail, the disclosure of private facts, mental pain, and emotional distress.
- Disclosure of address information for victims of abuse.
- Potential for secondary uses of the information which could result in fear or uncertainty.
- Unwarranted exposure leading to humiliation or loss of self-esteem.

Taxpayer's account information is valuable information. Nevertheless, IRS procedures do not require that the taxpayer be notified when another individual has attempted to access his or her tax account information, but no other Personally Identifiable Information was disclosed. The IRS should notify taxpayers when someone else has accessed their tax accounts to ensure taxpayers are aware of the incident and can take appropriate actions.

[14] United States Attorney's Office: Western District of Washington, News Release, *TEN INDICTED FOR PRETEXTING IN "OPERATION DIALING FOR DOLLARS": Defendants Would Adopt Various Identities to Get Confidential Tax, Medical and Employment Info* (December 6, 2007), *available at* **http://www.justice.gov/usao/waw/press/2007/dec/torrella.html**

There are limited procedures for the IRS to contact taxpayers who unknowingly may be victims of identity theft

The IRS will notify a taxpayer (victim) by letter when someone may have attempted to use his or her Social Security Number for incidents resulting from the following:

- Phishing and refund schemes.
- Verified false returns.
- Mixed entity research.
- Certain unpostable returns.

**********1**********1**********. The incident was coded Orange and the Incident Management Program did not notify the taxpayer. Projected to the population of 4,081 inadvertent disclosures processed in Fiscal Years 2009 and 2010, there may have been 41 incidents in which the IRS became aware that a taxpayer's identity may have been stolen by an individual but the IRS did not notify the taxpayer.

The information was also not reported to the IRS's Identity Theft Program because Disclosure Notification Process procedures do not require it. When the IRS learns that a taxpayer's identity may have been stolen, the information should be referred to the Identity Theft Program for resolution, including determining if an identity theft indicator should be placed on the taxpayer's account.

We have reported that the IRS needs to take more actions to address employment-related and tax fraud identity theft.[15] The use of another person's Social Security Number to obtain employment is often done in conjunction with a name different from Social Security Administration records. This is known as a Social Security Number/name mismatch. In these instances, the IRS and the Social Security Administration do not associate the income and benefits with the lawful taxpayer. The number of Wage and Tax Statements (Form W-2) with Social Security Number/name mismatches is substantial.

Serious problems develop for lawful taxpayers when both their name and Social Security Numbers are used by others to gain employment.

While Social Security Number/name mismatches are a significant problem for the IRS and the Social Security Administration, the more serious problem develops for the lawful taxpayer when both their name and Social Security Number are used by someone else to gain employment. No action is taken to stop someone from continuing

[15] *Outreach Has Improved, but More Action Is Needed to Effectively Address Employment-Related and Tax Fraud Identity Theft* (Reference Number 2008-40-086, dated March 25, 2008).

to commit employment-related identity theft using another person's Social Security Number and name.

The IRS does not actively try to identify or stop an individual from committing identity theft. Moreover, the IRS does not notify the employer of the problem of their employee using someone else's identity. Because the IRS and the Social Security Administration will assume the information on the Forms W-2 is accurate, the earnings resulting from the identity theft will be attributed to the lawful taxpayers for determining both Social Security benefits and tax liabilities. The IRS generally does not pursue the taxes that may be due on income earned using a stolen identity.

We have also reported that the IRS does not notify the taxpayer when there is evidence that the taxpayer's identity has been stolen.[16] The IRS has stated that the Social Security Administration has a program in place called the Employee No-Match Letter that requests correct information from individuals. The IRS believes its involvement would possibly be a duplication of the Social Security Administration's efforts.

Taxpayers are not always timely notified when their Personally Identifiable Information has been inadvertently disclosed

From our sample of 98 incidents, the IRS mailed notification letters to taxpayers for 27 of the reported incidents. In only 7 (26 percent) of 27 incidents, the notifications were mailed within 45 days of the date the incident was reported to or identified by the IRS. See Figure 2 for a breakdown of the number of days between the date the IRS was notified or identified the incident and the date the notifications were mailed.

Figure 2: Analysis of Days Between the Date the IRS Was Notified or Identified and the Date the Notification Letters Were Mailed

Number of Days	1-45 Days	46-75 Days	76-100 Days	101-150 Days	More Than 150 Days	Total Incidents
Number of Incidents	7	7	6	3	4	27

Source: Our analysis of 98 cases selected for the statistical sample.

For these 27 incidents, the time from the date the incident was reported or identified to the date the notification letter was mailed ranged from 20 to 226 days–with a median of 68 days and an average of 86 days. The IRS has established a business measure for the Disclosure Notification Process to notify potentially affected individuals with a median lapse time of 45 days from the date reported to the CSIRC to the date the notification letter is mailed.

[16] *Procedures Need to Be Developed for Collection Issues Associated With Individual Taxpayer Identification Numbers* (Reference Number 2010-40-040, dated March 29, 2010).

Through Fiscal Year 2010, the population of incidents the IRS used to determine the median included only the incidents input on the CSIRC *and* notification letters mailed within a fiscal year (October 1 through September 30). If the notification letter was mailed in a subsequent fiscal year, it was not counted in either fiscal year.

The IRS is also not measuring the total time associated with processing the disclosures reported through the Office of Taxpayer Correspondence or other IRS offices or functions. For example, incidents reported through the Office of Taxpayer Correspondence are tracked from the date they are input into the CSIRC. This does not include the days the employees in the Office of Taxpayer Correspondence work the incidents.

The IRS needs a measure to determine if all incidents are reported timely. This will ensure taxpayers are alerted to the risk in sufficient time to take precautions against identity theft or other harm.

Recommendations

The Deputy Commissioner for Operations Support should:

Recommendation 1: Educate employees on the importance of obtaining sufficient information on individuals whose Personally Identifiable Information was disclosed so they can be notified of the disclosure and can take the necessary steps to protect themselves from identity theft or other harm. The information should be documented when learning of a disclosure rather than after the fact and include enough information to identify the taxpayer whose information was disclosed and to whom it was disclosed.

> ***Management's Response:*** IRS management agreed with this recommendation. The IRS recently implemented a Think Data Protection campaign, which consists of a series of targeted employee communications using various media reaching across the IRS, designed to education employees on the importance of protecting sensitive information and reporting any losses or disclosures. In addition, the business units will continue to emphasize the data that should be gathered and reported when an incident occurs.

Recommendation 2: Revise procedures to: 1) ensure the definition of Personally Identifiable Information includes tax account information so taxpayers whose tax account information has been disclosed will be appropriately notified of a disclosure and 2) include instructions to forward disclosure incidents to the IRS's Identity Theft Program when the Incident Management Program learns that a taxpayer may already have been a victim of identity theft.

> ***Management's Response:*** IRS management agreed with this recommendation. During the assessment of a reported incident and the determination of whether notification is appropriate, the IRS applies the OMB's definition of Personally Identifiable Information. While the incidents noted in the report do not meet the definition of a disclosure of Personally Identifiable Information, the IRS will study the

possible expansion of the notification process to address these situations. As part of this process, the IRS will strengthen procedures to coordinate with the appropriate function to ensure identity theft is addressed. To date, the IRS has no evidence of an inadvertent disclosure that has led to a taxpayer becoming a victim of identity theft.

Office of Audit Comment: The IRS stated that it applies the OMB's definition of Personally Identifiable Information and that the incidents noted in the report do not meet the definition of a disclosure of Personally Identifiable Information.

We believe that tax account information, which is financial information, is included in the definition of Personally Identifiable Information. OMB M-07-16 defines Personally Identifiable Information as "information which can be used to distinguish or trace an individual's identity, such as their name, Social Security Number, biometric records, etc. 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, mother's maiden name, etc."

The Guide to Protecting the Confidentiality of Personally Identifiable Information (The U.S. Department of Commerce, Special Publication 800-122, April 2010) states that Personally Identifiable Information is any information about an individual maintained by an agency. This includes any information that is linked or linkable to an individual, such as medical, educational, financial, and employment information.

In addition, the IRS stated in its response that to date, it has no evidence of an inadvertent disclosure that has led to a taxpayer becoming a victim of identity theft. We reported that in one incident sampled, **********1**********
**********1**********.

Recommendation 3: Implement a timeliness measure to ensure taxpayers are timely notified and to gauge the overall performance of the Disclosure Notification Process, and include the time the incident is being processed by the Office of Taxpayer Correspondence or other IRS offices or functions before it is reported to the CSIRC.

Management's Response: IRS management agreed with this recommendation. Current reporting measures the elapsed time between the CSIRC report date and notification letter date. Based on this measure, the IRS has demonstrated positive performance in Fiscal Year 2011, averaging a 20-day response time through April 21, 2011. The IRS will expand its current metrics to include a broader organizational measure that incorporates the elapsed time between initial incident reporting and taxpayer notification dates.

Multiple Information Systems and Manual Processes Increase the Risk That Not All Incidents Are Considered and Controlled

There is no assurance that all disclosure incidents reported were considered and processed. A test of 4,800 disclosure incidents reported on the CSIRC identified 898 missing reports. Management controls should provide reasonable assurance that all disclosures are appropriately recorded and considered. Systems used to record and track disclosures need to be complete and accurate. The Disclosure Notification Process management information systems need to be improved to ensure all incidents are considered and appropriately processed, and that the IRS has sufficient data to effectively monitor the Process and ensure it is meeting all the objectives of the Incident Management Program.

Disclosure incidents are processed using three systems–the CSIRC email portal, the Incident Tracking System, and the E-Trak System–during the Disclosure Notification Process. The Office of Taxpayer Correspondence uses a fourth system, the System for Tracking and Analysis of Correspondence Impact, to track the incidents that are reported to that office.

- Each system is independent of the others and does not communicate with the others.
- Data are manually keyed into the Incident Tracking System and the E-Trak System from the emails generated by the CSIRC portal.
- Three different numbering schemes are used to track the incidents. Only the Incident Response number generated by the Incident Tracking System is used by the E-Trak System. This makes it difficult to ensure all incidents are being considered and timely processed.

The IRS does not reconcile the various systems to ensure the databases are complete and all incidents are processed. Because of the lack of reconciliation, the reliability of the databases is at risk.

Testing of the System for Tracking and Analysis of Correspondence Impact showed that all incidents reported to the Office of Taxpayer Correspondence were appropriately reported to the CSIRC. However, reconciliations completed on the other three systems identified missing records.

The CSIRC Portal and Incident Tracking System

Seventeen percent of CSIRC portal disclosure incident reports were not controlled on the Incident Tracking System.

A test of 4,800 CSIRC portal disclosure incident email reports identified that 898 (19 percent) incidents were not on the Incident Tracking System. After researching the systems, the IRS was later able to find 86 of the 898 records. The actions taken on the remaining 812 (17 percent) of the 4,800 disclosure incidents reported through the CSIRC portal could not be determined.

The CSIRC portal disclosure incident email reports are not tracked, controlled, or maintained for review. CSIRC portal submissions are not stored in their own database. They are simply emails generated by the Portal form submission. The emails are reviewed and those that are considered disclosure incidents are entered into the Incident Tracking System. When the Incident Management Program employee determines the incident does not meet the definition of a disclosure, the employee emails the individual reporting the incident that disclosure criteria has not been met and no further action is being taken. Although the incident email is received by the "Disclosure of Sensitive Data" mailbox, the response emails to the reporting employee are from the Incident Management Program employee's personal mailbox application and archived from the analyst's mailbox.

The IRS does not quantify the total number of CSIRC disclosure incident email reports received, the total number not meeting the disclosure criteria, or the total number meeting the criteria and elevated to be entered into the Incident Tracking System. There are no controls to ensure an incident report email is not deleted. The IRS cannot be assured all emails are reviewed. There are also currently no managerial or quality reviews of the CSIRC portal disclosure incidents reported to ensure the decisions are appropriate. This increases the risk that some affected taxpayers might not be notified about an inadvertent disclosure of their Personally Identifiable Information.

The Incident Tracking System and the E-Trak System

A comparison of 4,321 Disclosure of Sensitive Data Incident Report Numbers in the Incident Tracking System to the E-Trak System identified 3 (0.7 percent) incident records were not on the E-Trak System.

- Three incidents were not transmitted from the Incident Tracking System to the Incident Management Program mailbox to be worked and input to the E-Trak System. The IRS has since input the incidents to the E-Trak System and is attempting to contact the employees and managers to obtain additional information.

A comparison of 4,081 E-Trak System disclosure incidents to the Incident Tracking System showed only 1 incident was not recorded on the Incident Tracking System. This incident was erroneously input into the Incident Tracking System (i.e., it did not meet the criteria for a disclosure) and was subsequently deleted from the Incident Tracking System. However, the E-Trak System was not updated to show the reason for the deletion.

A new process is being implemented so that incidents reported will automatically populate a database, reducing the risk that all incidents are not controlled.

The IRS is currently in the process of replacing the CSIRC portal and Incident Tracking System. Submission of the CSIRC online reporting form will automatically populate a database generating an incident notification email to the Incident Management Program to control on the E-Trak System. This will reduce the risk that all reported incidents are not controlled. However, controls

will need to be implemented to ensure all reported incidents are accounted for as meeting or not meeting disclosure criteria and provide for a quality review of criteria decision accuracy.

The IRS should evaluate whether the current systems could be integrated or if systems can be developed that allow for automatic updating and sharing information. This would reduce the need to reconcile between the systems. In addition, the information from all the systems should be used to measure the Disclosure Notification Process and assess how it can be improved. The information could also be useful in identifying trends in incidents. Management information is essential to make sound business decisions. Data must be accurate and complete.

Multiple systems and manual processes reduce management's ability to effectively oversee the Disclosure Notification Process

There is no single system that tracks incidents from the time they occur and are reported to the time the incidents are evaluated and closed. The IRS uses four independent systems to capture disclosure incident-related information. This requires the use of time-consuming manual data entry, which is susceptible to transcription errors, to process the incidents. Detailed incident information cannot be easily organized, categorized, and accessed for trend analysis to enhance management oversight.

None of the systems communicate with each other so the IRS does not have the ability to determine, for example:

- The total number of disclosure incidents reported and how many resulted in notifications.
- The causes of the disclosures.
- The responsible office for the disclosure.
- The most common types of disclosures.

Further, the IRS is not tracking whether incidents are being reported within 1 hour, as required. As more time elapses between the disclosure incident and reporting, there is a greater likelihood that the incident report will not include key data elements such as the individual's name and Social Security Number. This is because the reporting person may not acquire and maintain the affected individual's key information. Without the key data elements, the IRS cannot properly notify individuals who have had their information compromised.

Currently, any type of incident trend analysis would be very laborious because detailed incident information is stored in various systems, collected at different points in time, and not easily accessible. However, the data would be useful for management to analyze the Disclosure Notification Process and determine if it is meeting its objectives and goals and if the Process could be more efficient or effective. The information could also be useful in educating employees on how to avoid making inappropriate disclosures.

Disclosures related to taxpayer correspondence are to be reported first to the Office of Taxpayer Correspondence so that systemically generated notice issues can be quickly identified and resolved

In our sample of 98 incidents, 41 (42 percent) incidents were reported through the Office of Taxpayer Correspondence. Not all of these cases were related to systemic issues. For example, these cases typically involved letters addressed to an incorrect taxpayer or a letter for one taxpayer that was erroneously included in the same envelope with another taxpayer's letter. An example of a systemic issue is a computer program accidentally printing one taxpayer's information on another taxpayer's notice.

The Office of Taxpayer Correspondence reviews the reported incidents, obtains additional data from the individual who reported the incident, and for the incidents considered disclosures inputs them into the CSIRC. The Office of Taxpayer Correspondence took an average of 39 days—from 2 to 84 days—to process the 41 incidents in our sample that originated in the Office of Taxpayer Correspondence. This time is not included in the IRS's business measure for Disclosure Notification Process timeliness.

The IRS should evaluate the information it has on disclosure incidents reported through the Office of Taxpayer Correspondence to determine if the issues are predominantly systemic and whether incidents related to individual notices should continue to be reported first to the Office of Taxpayer Correspondence.

Recommendation

Recommendation 4: The Deputy Commissioner for Operations Support should implement sufficient controls to ensure that all incidents are accurately documented, controlled, and considered and develop a management information system sufficient to oversee disclosure incidents. This would include an evaluation of whether one system can be developed to track incidents from IRS notification to closure. If multiple systems must be used, consideration should be given to automatic updates between the systems to limit the need for manual reconciliations.

> ***Management's Response:*** IRS management agreed with this recommendation. The IRS will be implementing the Threat Incident Response Center and consolidating data from all systems for the most serious incidents. Routing reconciliations between systems have found minimal differences between CSIRC reports and the risk assessment-tracking database.

Appendix I

Detailed Objective, Scope, and Methodology

The overall objective of this review was to determine whether the IRS is making appropriate decisions to promptly and properly notify taxpayers of inadvertent disclosures of their tax information. To accomplish this objective, we:

I. Determined what IRS procedures and processes are in place to identify inadvertent disclosures and to notify taxpayers.

   A. Reviewed all applicable laws and regulations to gain a clear understanding and ensure the IRS is appropriately adhering to them.

   B. Reviewed IRS internal procedures and processes, including manuals, user guides, and the IRS intranet.

   C. Met with the appropriate IRS personnel to discuss and document the processes used to identify inadvertent disclosures and notify taxpayers that their Personally Identifiable Information has been disclosed.

   D. Identified systems used to capture the incidents of inadvertent disclosure and to notify taxpayers.

II. Determined whether the IRS is accurately controlling all reported disclosure incidents. We identified all disclosure incidents on the following systems with the CSIRC[1] portal email date for the period October 1, 2008, to September 30, 2010. We assessed the reliability of computer system data by performing electronic testing of required data elements and interviewing agency officials knowledgeable about the data. We identified deficiencies in the completeness of the data and made a recommendation to address those deficiencies. We performed the following comparisons to validate whether all incidents were accurately controlled.

   A. Compared 4,800 disclosure incident emails submitted through the CSIRC portal to 4,321 Incident Tracking System[2] disclosure incidents.

   B. Compared 4,321 Incident Tracking System disclosure incidents to 4,081 E-Trak System[3] disclosure incidents.

[1] The CSIRC is the centralized reporting facility for all computer security privacy incidents.
[2] The Incident Tracking System provides an automated process to capture, process, and track incident data and generate reports.
[3] The E-Trak System is an off-the-shelf case-tracking tool used to respond to a public law.

C. Compared 1,779 System for Tracking and Analysis of Correspondence Impact disclosure incidents to 4,321 Incident Tracking System disclosure incidents.

D. Compared 4,081 E-Trak System disclosure incidents to 4,321 Incident Tracking System disclosure incidents.

III. Determined whether appropriate decisions were made for notifying the taxpayer of inadvertent disclosures of tax information.

A. Selected a statistical sample of 98 closed incidents from the population of 4,081 E-Trak System disclosure incidents using a confidence rate of 95 percent, a precision rate of 5 percent, and an error rate of 7 percent. The error rate was established from a probe sample of 15 randomly selected disclosure incidents resulting in 1 (7 percent) of 15 incidents where the individual should have been notified of Personally Identifiable Information disclosure.

B. Reviewed the sampled records and associated data in the IRS Incident Management archived shared drawer and from the Office of Taxpayer Correspondence to determine if appropriate decisions were made.

C. Using the sample from Step III.A., reviewed the Integrated Data Retrieval System[4] to determine whether the identity theft indicator had been input on the account.

IV. Determined whether taxpayers were notified timely of inadvertent disclosures.

A. Identified the business measure used to indicate timeliness of notification.

B. Using the sample from Step III.A., identified 27 incidents with notifications mailed to taxpayers.

C. Reviewed the selected records to identify the length of time from the date the incident was reported to or identified by the IRS and the date the notification letter was mailed to the taxpayer.

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 the following internal controls were relevant to our audit objective: the Incident Management Program policies and procedures aimed at timely reaction and appropriate responses to occurrences of IRS data losses, thefts, breaches and disclosures. We evaluated the internal controls by interviewing

[4] The IRS computer system capable of retrieving or updating stored information. It works in conjunction with a taxpayer's account records.

management and reviewing policies, reports, and procedures; selecting and comparing the disclosure incidents identified on four systems used to process disclosure incidents; and evaluating the response decision and timely notification of a statistical sample of 98 disclosure incidents.

Appendix II

Major Contributors to This Report

Michael E. McKenney, Assistant Inspector General for Audit (Returns Processing and Account Services)
Augusta R. Cook, Director
Paula W. Johnson, Audit Manager
Lynn Faulkner, Lead Auditor
Jackie Forbus, Senior Auditor
Jerome Antoine, Auditor
Kevin O'Gallagher, Information Technology Specialist

Appendix III

Report Distribution List

Commissioner C
Office of the Commissioner – Attn: Chief of Staff C
Deputy Commissioner for Services and Enforcement SE
Chief Technology Officer OS:CTO
Commissioner, Small Business/Self-Employed Division SE:S
Commissioner, Wage and Investment Division SE:W
Deputy Chief Information Officer for Operations OS:CTO
Deputy Commissioner of Operations, Wage and Investment Division SE:W
Deputy Commissioner of Services, Wage and Investment Division SE:W
Director, Privacy, Information Protection, and Data Security OS:P
Chief Information Officer OS:CTO:CIO
Associate Chief Information Officer, Cybersecurity OS:CTO:C
Associate Chief Information Officer, Strategy and Planning OS:CTO:SP
Director, Communications, Liaison, and Disclosure, Small Business/Self-Employed Division SE:S:CLD
Director, Customer Account Services, Wage and Investment Division SE:W:CAS
Director, Cybersecurity Operation OS:CTO:O
Director, Privacy and Information Protection OS:P:PIP
Director, Strategy and Finance, Wage and Investment Division SE:W:S
Director, Taxpayer Correspondence, Wage and Investment Division SE:W:OTC
Director, Governmental Liaison and Disclosure, Small Business/Self-Employed Division SE:S:CLD:GLD
Chief, Program Evaluation and Improvement, Wage and Investment Division SE:W:S:PRA:PEI
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 Liaisons:
- Chief Technology Officer OS:CTO
- Commissioner, Small Business/Self-Employed Division SE:S
- Director, Privacy, Information Protection, and Data Security OS:P
- Senior Operations Advisor, Wage and Investment Division SE:W:S

Appendix IV

Outcome Measures

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

Type and Value of Outcome Measure:

- Taxpayer Privacy and Security – Potential; 653 taxpayer accounts affected[1] (see page 6).

Methodology Used to Measure the Reported Benefit:

For the period October 1, 2008, to September 30, 2010, we reviewed a statistical sample of 98 incidents to determine whether the IRS accurately decided to notify the taxpayers that their Personally Identifiable Information was inadvertently disclosed. Our review determined the following:

- For 5 (5 percent) of the 98 decisions, the IRS did not notify the taxpayer their Personally Identifiable Information was disclosed because the IRS did not document or retain the necessary information to notify the affected taxpayer. Projected to the population of 4,081 inadvertent disclosures processed in Fiscal Years 2009 and 2010, there may have been 204 incidents where the IRS acknowledged Personally Identifiable Information had been disclosed but the IRS did not notify the affected taxpayers.
- For 10 (10 percent) of the 98 incidents, the IRS did not notify the taxpayers that their tax account information was disclosed because IRS procedures did not include tax account information as Personally Identifiable Information. Projected to the population of 4,081 inadvertent disclosures processed in Fiscal Years 2009 and 2010, there may have been 408 incidents where the IRS disclosed tax account information but the IRS did not notify the affected individuals.
- **********1**********1**********. Projected to the population of 4,081 inadvertent disclosures processed in Fiscal Years 2009 and 2010, there may have been 41 incidents where the IRS became aware that a taxpayer's identity may have been stolen by an individual but the IRS did not notify the taxpayer.

[1] Our projections are conservative. Each incident may affect more than one taxpayer that may have had Personally Identifiable Information disclosed but was not notified.

Type and Value of Outcome Measure:

- Taxpayer Privacy and Security – Potential; 815 disclosure records affected (see page 17).

Methodology Used to Measure the Reported Benefit:

We summed 812 incidents that were not transferred from the CSIRC[2] portal to the Incident Tracking System and 3 incidents that were not added to E-Trak System[3] from the Incident Tracking System.[4] Each incident may affect more than one taxpayer that may have had Personally Identifiable Information disclosed but the incident is not in the database for review.

[2] The CSIRC is the centralized reporting facility for all computer security privacy incidents.
[3] The E-Trak System is an off-the-shelf case-tracking tool used to respond to a public law.
[4] The Incident Tracking System provides an automated process to capture, process, and track incident data and generate reports.

Appendix V

Internal Revenue Service Employee Instructions on Reporting Inadvertent Disclosures

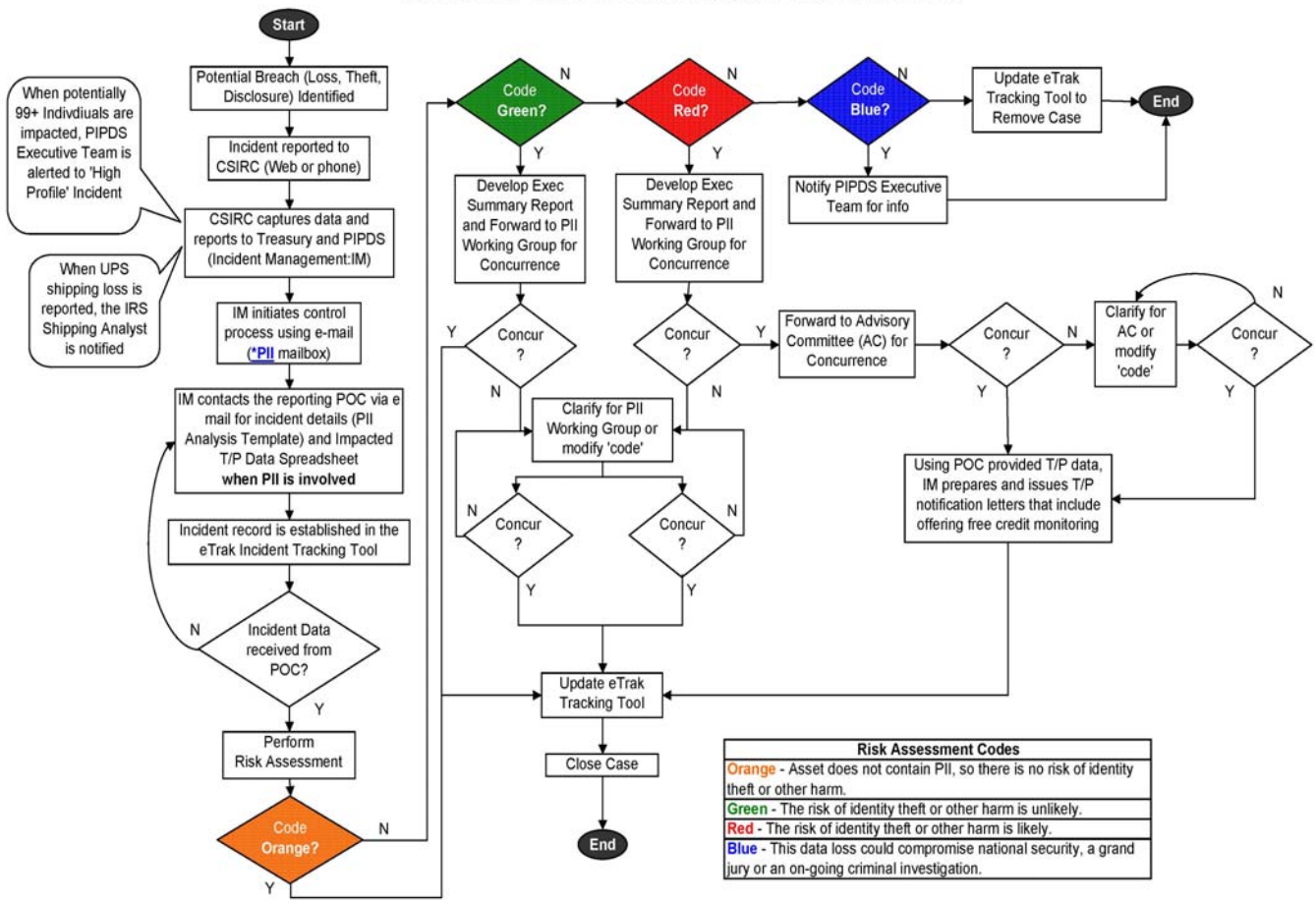
IRS employees, who become aware of an inadvertent disclosure of sensitive information, or the loss or theft of an information technology asset or hardcopy record or document containing sensitive information, *are required to report the incident* ***within 1 hour*** *to each of the following*, as applicable:

- His or her manager, in all instances.
- *The Office of Taxpayer Correspondence*, if the incident involves taxpayer correspondence, using the Servicewide Notice Information Program Erroneous Taxpayer Correspondence Reporting Form. The scope of this form has been expanded to include electronic communication like faxes, transcripts, and email messages. The Office of Taxpayer Correspondence will notify the CSIRC[1] as necessary after an initial analysis of the incident. This procedure minimizes the potential for inaccurate, incomplete, and duplicate reporting of incidents to the CSIRC, lessens the operational impact of reporting an incident, and focuses resources on correcting the error to prevent additional breaches/losses.
- *The CSIRC*, if the incident *does not* involve taxpayer correspondence (for example, a verbal disclosure, lost laptop, data disk, or packages lost during shipment), using the Computer Security Incident Reporting Form or by calling 1-866-216-4809.
- *The Treasury Inspector General for Tax Administration*, if the incident involves the loss or theft of an information technology asset (e.g., computers, laptops, routers, printers, removable media, CD/DVD, flash drive, floppy) or hardcopy records/documents, at 1-800-366-4484.
- *The Modernization and Information Technology Services organization Enterprise Services Help Desk*, if the incident involves the loss or theft of an information technology asset.

[1] The CSIRC is the centralized reporting facility for all computer security privacy incidents.

Appendix VI

Flowchart of the Disclosure Notification Process



Source: IRS Incident Management Program. IM = Incident Management Program. PII = Personally Identifiable Information. POC = Point of Contact. PIPDS = Privacy, Information Protection, and Data Security. T/P = Taxpayer. UPS = United Parcel Service.

Appendix VII

Management's Response to the Draft Report

DEPUTY COMMISSIONER

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

RECEIVED
MAY 10 2011

May 9, 2010

MEMORANDUM FOR DEPUTY INSPECTOR GENERAL FOR AUDIT

FROM: Beth Tucker
Deputy Commissioner for Operations Support

SUBJECT: Draft Audit Report – Some Taxpayers Were Not Appropriately Notified When Their Personally Identifiable Information Was Inadvertently Disclosed (Audit # 201040050)

Thank you for the opportunity to respond to the above referenced draft audit report. Protecting the sensitive data entrusted to the Internal Revenue Service (IRS) by taxpayers and employees is vital to maintaining the public's trust in the United States tax administration system, and is a top priority of the IRS. The IRS has made great strides in incident reporting, handling data breaches, assessing risk and notifying taxpayers.

The IRS has a consistent record of achievement and performance in protecting the information of the American public. IRS employees protect sensitive information while striking a balance between effective taxpayer interaction and data protection. Processes and systems are continually improved, and sophisticated technology is being used to secure data within the control of the IRS. The effective management of equipment and the implementation of high-end encryption minimize the potential impact of data incidents.

The IRS has an established process for reporting a data incident, analyzing the loss, responding quickly to prevent further impact, determining the risk to the taxpayer or employee and, as appropriate, notifying the taxpayer or employee of the loss. Over the last four years, the IRS has continually refined data incident procedures to increase understanding and expedite notification. A system of checks and balances has been instituted to ensure incidents are properly routed for analysis. New systems have been developed that allow for improved tracking of information related to incidents, increased coordination between IRS functions and expedited handling of incidents.

Data centric approaches to information protection have enhanced communications and mitigation plans to actively reduce the number of incidents. Regular communication between IRS business units increases coordination and security of information. Initiatives such as using secure electronic methods to ship documents between IRS offices instead of mail have increased the security of information and saved resources. An initiative designed to remove Social Security Numbers from IRS notices will also protect taxpayer information.

Recently, a new data protection campaign was launched to keep IRS employees informed, prepared and practicing all aspects of data protection in their daily work activities. By communicating the importance of data protection through multiple channels and from the highest levels of the organization, the IRS commitment to protecting sensitive information is communicated to all employees.

To continue this momentum, we will focus on enhancing performance measures, improving processes and educating the IRS population on data protection. If you have any questions, please contact me at (202) 622-4255, or a member of your staff may contact Rebecca Chiaramida, Director, Privacy Information Protection & Data Security, at (202) 622-2988.

Attachment

Attachment

Draft Audit Report – Some Taxpayers Were Not Appropriately Notified When Their Personally Identifiable Information Was Inadvertently Disclosed (Audit # 201040050)

RECOMMENDATION 1: Educate employees on the importance of obtaining sufficient information on individuals whose Personally Identifiable Information was disclosed so they can be notified of the disclosure and can take the necessary steps to protect themselves from identity theft or other harm. The information should be documented when learning of a disclosure rather than after the fact and include enough information to identify the taxpayer whose information was disclosed and to whom it was disclosed.

CORRECTIVE ACTION: The IRS agrees with this recommendation. The IRS has recently implemented a Think Data Protection campaign, which consists of a series of targeted employee communications, using various media, reaching across the IRS, designed to educate employees on the importance of protecting sensitive information and reporting any losses or disclosures. Additionally, the business units will continue to emphasize the data that should be gathered and reported when an incident occurs.

IMPLEMENTATION DATE: This is projected to be accomplished no later than September 30, 2011.

RESPONSIBLE OFFICIAL: Director, Privacy, Information Protection & Data Security

CORRECTIVE ACTION MONITORING PLAN: Establish a timeline of necessary actions that incorporates expected outcomes and dates to successfully accomplish stated tasks.

RECOMMENDATION 2: Revise procedures to: (1) ensure the definition of Personally Identifiable Information includes tax account information so taxpayers whose tax account information has been disclosed will be appropriately notified of a disclosure; and (2) include instructions to forward disclosure incidents to the IRS's Identity Theft Program when the Incident Management Program learns that a taxpayer may already have been a victim of identity theft.

CORRECTIVE ACTION: The IRS agrees with this recommendation. During the assessment of a reported incident and the determination of whether notification is appropriate, the IRS applies the Office of Management and Budget's definition of Personally Identifiable Information (PII). While the incidents noted in the report do not meet the definition of a disclosure of PII, the IRS will study the possible expansion of the notification process to address these situations. As part of this process, the IRS will strengthen procedures to coordinate with the appropriate function to ensure identity theft is addressed. To date, the IRS has no evidence of an inadvertent disclosure that has led to a taxpayer becoming a victim of identity theft.

IMPLEMENTATION DATE: This is projected to be accomplished no later than September 30, 2011.

RESPONSIBLE OFFICIAL: Director, Privacy, Information Protection & Data Security

CORRECTIVE ACTION MONITORING PLAN: Establish a timeline of necessary actions that incorporates expected outcomes and dates to successfully accomplish stated tasks.

RECOMMENDATION 3: Implement a timeliness measure to ensure taxpayers are timely notified and to gauge the overall performance of the Disclosure Notification Process, and include the time the incident is being processed by the Office of Taxpayer Correspondence or other IRS offices or functions before it is reported to the Computer Security Incident Response Center (CSIRC).

CORRECTIVE ACTION: The IRS agrees with this recommendation. Current reporting measures the elapsed time between CSIRC report date and notification letter date. Based on this measure, the IRS has demonstrated positive performance in Fiscal Year 2011, averaging a 20-day response time through April 21, 2011. The IRS will expand its current metrics to include a broader organizational measure that incorporates the elapsed time between initial incident reporting and taxpayer notification dates.

IMPLEMENTATION DATE: This is projected to be accomplished no later than July 31, 2011.

RESPONSIBLE OFFICIAL: Director, Privacy, Information Protection & Data Security

CORRECTIVE ACTION MONITORING PLAN: Establish a timeline of necessary actions that incorporates expected outcomes and dates to successfully accomplish stated tasks.

RECOMMENDATION 4: The Deputy Commissioner for Operations Support should implement sufficient controls to ensure that all incidents are accurately documented, controlled, and considered and develop a management information system sufficient to oversee disclosure incidents. This would include an evaluation of whether one system can be developed to track incidents from IRS notification to closure. If multiple systems must be used, consideration should be given to automatic updates between the systems to limit the need for manual reconciliations.

CORRECTIVE ACTION: The IRS agrees with this recommendation. The IRS will be implementing the Threat Incident Response Center, consolidating data from all systems for the most serious incidents. Routine reconciliations between systems have found minimal differences between CSIRC reports and the risk assessment tracking database.

IMPLEMENTATION DATE: This is projected to be accomplished no later than September 30, 2011.

RESPONSIBLE OFFICIALS: Director, Privacy, Information Protection & Data Security

CORRECTIVE ACTION MONITORING PLAN: Establish a timeline of necessary actions that incorporates expected outcomes and dates to successfully accomplish stated tasks.