

---

---

*TREASURY INSPECTOR GENERAL FOR TAX ADMINISTRATION*  
*Office of Inspections and Evaluations*



*The Program to Protect Hardcopy Personally  
Identifiable Information Is a Work-in-Progress*

**September 12, 2008**

**Reference Number: 2008-IE-R002**

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](mailto:inquiries@tigta.treas.gov)  
*Web Site* | <http://www.tigta.gov>



TREASURY INSPECTOR GENERAL  
FOR TAX ADMINISTRATION

DEPARTMENT OF THE TREASURY

WASHINGTON, D.C. 20220

September 12, 2008

**MEMORANDUM FOR DEPUTY COMMISSIONER, OPERATIONS SUPPORT**

**FROM:** Philip Shropshire   
Acting Deputy Inspector General for Inspections and Evaluations

**SUBJECT:** Final Inspection Report – The Program to Protect Hardcopy Personally Identifiable Information Is a Work-in-Progress (Inspection #200810IE008)

This report presents the results of our inspection to determine what actions the Internal Revenue Service (IRS) is taking to protect hardcopy personally identifiable information (PII)<sup>1</sup> that is shipped from office to office and how the IRS responds when a disclosure of hardcopy PII potentially occurs.

*Impact on the Taxpayer*

Every year, the IRS mails hardcopy PII in millions of packages and letters by commercial carriers and the United States Postal Service. While the overwhelming majority of commercially shipped packages reach their destinations without incident, the few packages that are compromised present opportunities for identity theft. Taxpayer confidence that information sent to the IRS is properly protected from identity theft is critical to the voluntary compliance system.

---

<sup>1</sup> Personally identifiable information (PII) refers to information that 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. Hardcopy PII is in paper or other physical form rather than in electronic format, such as on a laptop.



## *The Program to Protect Personally Identifiable Information Is a Work-in-Progress*

### Synopsis

In recent years the public has become increasingly aware that their PII can be compromised while in the possession of a third party. Identity theft victims have shared their stories of how their lives have been turned into chaos. Several highly publicized data breaches, generally involving electronic data files, have taken place in both the private and public sectors. The IRS is responsible for protecting electronic PII for its employees and millions of taxpayers. Additionally, the IRS still has millions of paper records with PII that must be shipped from one location to another.

The IRS ships packages primarily via the United States Postal Service and the United Parcel Service (UPS). In Fiscal Year 2007, the IRS sent over 150 million pieces of mail to taxpayers through the United States Postal Service and more than 3 million packages were shipped via UPS. While some UPS packages are damaged, misdirected or lost, disclosures from these types of incidents are minimal. However, to the taxpayers whose PII is compromised, the potential for identity theft is a valid concern.

The IRS established the Privacy, Information Protection and Data Security Office ([PIPDS] hereafter referred to as the Office) to protect sensitive data by reducing the risk of inadvertent disclosures. Since its establishment in July 2007, the Office has investigated over 300 potential data breaches to determine whether taxpayer notification is appropriate. They have also hired a consulting firm to review procedures associated with shipping documents between IRS offices. The Office also has studied and developed recommendations to reduce the use of Social Security Numbers (SSN) when appropriate. Finally, the Office is spearheading the Operation R.E.D. (Review, Encrypt, Decide) initiative, designed to remind IRS employees how to protect PII.

We recognize that many problems with hardcopy PII protection have been long-term problems and will not be easily solved. The Office has identified these problems and either has plans or has already initiated actions to address them. Our inspection identified some areas where additional actions could improve operations.

First, we found that hardcopy PII cases could not be readily distinguished from electronic PII or mixed media incidents in the incident reporting database. Second, not all packages contain a list of items shipped, and package originators do not always monitor package delivery and initiate appropriate actions if packages are lost. Third, formal procedures to improve how packages are assembled and shipped have not been issued. Fourth, the study on shipping hardcopy PII being conducted by a consulting firm did not include shipments to Federal Records Centers.

### Recommendations

We recommend that the Director of PIPDS collaborate with the Director, Computer Security Incident Response Center (CSRC), to develop a new incident code that clearly separates



*The Program to Protect Personally Identifiable Information Is a  
Work-in-Progress*

---

hardcopy PII loss from other types of losses; require originators to maintain a list of the package contents to enable the IRS to identify lost items and whom to notify; reinforce the need for mandatory monitoring of all packages by the originator to ensure receipt; and initiate follow-up actions as appropriate. Also, the PIPDS Director should monitor actions to ensure that planned enhancements to shipping procedures are made formal and perform a risk assessment on the shipment of documents to Federal Records Centers.

*Response*

IRS management generally agreed with our recommendations. The CSIRC database has the necessary capability for data loss reporting and tracking processes. PIPDS will continue to update reporting and tracking processes to support identifying trends and develop mitigation strategies. Also, a review of the Document Transmittal, Form 3210, will be included in the current SSN Elimination and Reduction initiative, and the effectiveness of the document transmittal process will be evaluated during a shipping process risk assessment. The assessment is being conducted to provide further insight and validation for the enhancements identified to strengthen shipping procedures and other improvement opportunities. The Director, PIPDS will continue to work with key stakeholders to implement the procedural improvements to strengthen IRS shipping procedures. Management also agreed to expand the scope of the shipping process risk assessment to include shipping tax returns and other taxpayer and employee hard copy data from IRS facilities to the Federal Record Centers. Management's complete response to the draft report is included as Appendix IV.

Please contact me at (202) 927-7048 if you have questions or Kevin Riley, Acting Director, Inspections and Evaluations, at (972) 249-8355.



---

*The Program to Protect Personally Identifiable Information Is a  
Work-in-Progress*

---

## *Table of Contents*

<b>Background</b> .....	Page 1
<b>Results of Review</b> .....	Page 3
The Office of Privacy, Information Protection and Data Security Has Significant Accomplishments in Less Than a Year of Operation.....	Page 3
<u>Recommendation 1:</u> .....	Page 6
<u>Recommendations 2 and 3:</u> .....	Page 8
<u>Recommendation 4:</u> .....	Page 9
Summary .....	Page 11
<b>Appendices</b>	
Appendix I – Detailed Objective, Scope, and Methodology .....	Page 12
Appendix II – Major Contributors to This Report .....	Page 14
Appendix III – Report Distribution List .....	Page 15
Appendix IV – Management’s Response to the Draft Report .....	Page 16



*The Program to Protect Hardcopy Personally Identifiable  
Information Is a Work-in-Progress*

---

## *Abbreviations*

CSIRC	Computer Security Incident Response Center
FISMA	Federal Information Security Management Act of 2002
IRS	Internal Revenue Service
OMB	Office of Management and Budget
OPIP	Office of Privacy and Information Protection
PII	Personally Identifiable Information
PIPDS	Privacy, Information Protection, and Data Security
R.E.D.	Review, Encrypt (and/or safeguard), Decide
SSN	Social Security Number
UPS	United Parcel Service



---

*The Program to Protect Hardcopy Personally Identifiable Information Is a Work-in-Progress*

---

## *Background*

Many Americans each year suffer the financial and emotional trauma caused by identity theft. While the risk has greatly increased because of electronic record-keeping, the concern about protecting hardcopy personally identifiable information (PII)<sup>1</sup> is not new. As early as 1977, the Government Accountability Office<sup>2</sup> reported that the IRS tax return mailing procedures and practices needed more stringent controls. Some of those same issues are relevant today.

*“... the problem of identity theft has become more complex and challenging for the general public, the government, and the private sector.”*

The President's Identity Theft Task Force  
“Combating Identity Theft: A Strategic Plan”  
April 2007

To address the concern about the Federal Government's protection of personal information, the President's Task Force on Identity Theft was established by Executive Order 13,402<sup>3</sup> on May 10, 2006. It was charged with developing a strategic plan for the Federal Government to combat identity theft and recommending actions for the public and private sectors should take. Consumers wrote to the Task Force, urging the public and private sectors to do a better job of protecting their Social Security Numbers (SSNs), and many discussed the challenges raised by the overuse of SSNs as identifiers.

According to the Task Force's strategic plan, identity theft depends on access to consumer data. Data compromises can expose consumers to the threat of identity theft or related fraud, damage the victim's reputation, and carry financial costs for everyone involved. Although the strategic plan was not released until April 2007, an interim recommendation suggested that the Office of Management and Budget (OMB) issue data breach guidance to all agencies. In September 2006, the OMB issued guidance to Federal agencies for responding to data breaches. On May 22, 2007, the OMB issued a memorandum requiring agencies to develop and implement a breach notification policy within 120 days.

Hardcopy PII maintained by the Internal Revenue Service (IRS) is subject to the Privacy Act of 1974 and the Federal Information Security Management Act of 2002 (FISMA). The Privacy Act

---

<sup>1</sup> Personally identifiable information (PII) refers to information that 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. Hardcopy PII is in paper or other physical form rather than electronic format, such as on a laptop.

<sup>2</sup> IRS' Security Program Requires Improvements to Protect Confidentiality of Income Tax Information GGD-77-44 July 11, 1977.

<sup>3</sup> Executive Order No. 13,402, 3 C.F.R. 225-228 (2007), *amended by* Executive Order No. 13,414, C.F.R. 250 (2007).



*The Program to Protect Hardcopy Personally Identifiable  
Information Is a Work-in-Progress*

---

prohibits disclosure of records without consent of the individual to whom the record pertains. The FISMA requires each agency to follow National Institute of Standards and Technology<sup>4</sup> guidance and standards by implementing procedures for detecting, reporting, and responding to security incidents. The FISMA also requires agencies to notify and consult with the Federal Information Security Incident Center, law enforcement agencies, and the agency Inspector General on any reported incidents.

Because of the nature of IRS work processes, a tremendous volume of taxpayer and employee PII is at risk. The IRS ships packages from office to office primarily via the United States Postal Service and the United Parcel Service (UPS). In Fiscal Year 2007 more than 3 million packages were shipped via UPS and an additional 10,000 by Federal Express. While some UPS packages are damaged, misdirected or lost, disclosures from these types of incidents are minimal.

This inspection was performed at the IRS National Headquarters in Washington, D.C., and in the Office of Privacy, Information Protection, and Data Security ([PIPDS] hereafter referred to as the Office) during the period April through May 2008. This review was performed in accordance with the President's Council on Integrity and Efficiency Quality Standards for Inspections. Detailed information on our inspection objective, scope, and methodology is presented in Appendix I. Major contributors to the report are listed in Appendix II.

---

<sup>4</sup> The National Institute of Standards and Technology (NIST) is a part of the U.S. Department of Commerce and is responsible for developing standards that other Federal agencies are required to follow.



---

*The Program to Protect Hardcopy Personally Identifiable  
Information Is a Work-in-Progress*

---

## *Results of Review*

The Social Security Administration reports that identity theft is one of the fastest growing crimes in the United States. Several widely publicized incidents have amplified the need to prevent inadvertent information disclosures and to respond quickly when disclosures occur. The OMB provided the Executive Branch with guidance on protecting PII.

In response to this quickly evolving environment, the IRS established an office to oversee the protection of private information and data. As part of its current initiatives, the Office is studying all reported incidents of potential disclosure and how hardcopy data is shipped to various destinations. It has assessed how PII is used, how it might be inadvertently disclosed, how to limit such disclosures, and how it can better respond when disclosures occur. Additionally, the Office is studying ways to eliminate the use of SSNs when feasible. Finally, it is spearheading an agency-wide review called Operation R.E.D. (Review, Encrypt, and Decide) to remind employees of their role in properly safeguarding information.

Less than a year after its creation, the Office has had significant accomplishments. It has investigated over 300 potential data breaches to determine whether taxpayer notification is appropriate. It also has studied and developed recommendations to reduce the use of SSNs when appropriate. We recognize that many problems with hardcopy PII protection have been long-term problems, and these will not be solved easily. The Office has identified these problems and has plans, or has already initiated actions, to address them.

Our inspection identified some areas where additional actions could improve operations. First, we found that hardcopy PII cases could not be readily distinguished from electronic PII or mixed media incidents in the incident reporting database. Second, not all packages contain a list of items shipped, and package originators do not always monitor package delivery and initiate appropriate actions if packages are lost. Third, formal procedures to improve how packages are assembled and shipped have not been issued. Fourth, the study on shipping hardcopy PII being conducted by a consulting firm did not include shipments to Federal Records Centers.

### ***The Office of Privacy, Information Protection and Data Security Has Significant Accomplishments in Less Than a Year of Operation***

The IRS established the Office in July 2007. It reports directly to the Deputy Commissioner, Operations Support, and functions at the same organizational level as the Chief Information Officer, the Chief Financial Officer, the Human Capital Officer, and the Chief, Agency-Wide Shared Services. As of April 2008, the Office had a staff of about 40 employees.



*The Program to Protect Hardcopy Personally Identifiable Information Is a Work-in-Progress*

The organizational mission of this Office is: ***“To preserve and enhance public confidence by advocating for the protection and proper use of identity information.”***

The Office has two components: Privacy and Information Protection (OPIP); and Online Fraud Detection and Prevention (OFDP). Our inspection was limited to the OPIP, which performs its mission through two staffs designed to focus on specific technical areas in privacy and identity protection.

Recent major accomplishments of OPIP include developing assessment and notification procedures to evaluate the significance of reported disclosures, studying the causes of disclosures during shipping, and studying methods to reduce or eliminate the use of SSNs when feasible. Below is a description of these areas.

**Breach Notification Policy**

The OPIP developed its breach notification process based on OMB guidance. It created a process to assess reported potential disclosures, determine the likelihood that a disclosure did occur, and make recommendations on whether individual taxpayers must be notified. An OPIP team receives incident reports from the Computer Security Incident Response Center (CSIRC) of potential information breaches. The team performs a risk assessment on each incident, summarizes the facts developed, and recommends whether individual taxpayers should be notified that their PII might have been disclosed. In cases where notification is recommended, those cases are forwarded for review and, if the Identity Theft and Incident Management Executive Advisory Committee<sup>5</sup> concurs with the decision, taxpayers are notified. The level of risk associated with a potential disclosure incident is summarized in Figure 1.

**Figure 1: Risk Levels**

<b>RISK ASSESSMENT LEVEL</b>	<b>RISK CODE</b>	<b>DESCRIPTION</b>
Level One	Green	Risk of identity theft or other harm is unlikely.
Level Two	Yellow	Risk of identity theft or other harm is possible.
Level Three	Red	Risk of identity theft or other harm is likely.
Level Four	Blue	The information could compromise National Security, Grand Jury, or Criminal Investigation.

*Source: Derived by IRS Privacy, Information Protection and Data Security from OMB guidance.*

<sup>5</sup> See Appendix IV for a list of the Committee members.



---

*The Program to Protect Hardcopy Personally Identifiable  
Information Is a Work-in-Progress*

---

Notification groups have been established to issue letters specifically designed for this program. The letters offer individuals credit monitoring provided through Equifax<sup>6</sup> for 1 year. This offer does not extend to businesses, but other avenues are being explored that would not preclude notification to businesses if financial data was breached. In addition, a dedicated toll-free number has been established to handle taxpayers' inquiries related to personal information disclosure cases. All other IRS Customer Service Representatives have been instructed about where to route personal information disclosure calls.

Additionally, in January 2008, the IRS created an indicator code for application to the accounts of taxpayers who have been determined to be the victims of identity theft, regardless of how it occurred. The IRS expects that by January 2009 this code will allow legitimate returns to be properly processed and will prevent questionable returns from being associated with the taxpayers' accounts. In the fall of 2008, the IRS will also implement new indicator codes to place on the accounts of three additional taxpayer groups: 1) self-identified victims of identity theft who have not yet experienced a problem with their tax accounts; 2) IRS-identified victims of identity theft; and 3) individuals who have received breach notification letters from the IRS.

We reviewed the 63 potential disclosure incidents reported during the period January 2008 through March 2008 and found that 21 of the cases involved hardcopy PII being shipped by the IRS via UPS. Fourteen of the 21 cases were categorized as Code Red incidents (risk of identity theft or other harm is likely), and the decision was made to notify the 90 affected individuals and offer them credit monitoring services.

The largest number of individuals affected by a hardcopy incident, however, is likely to be those initiated by an IRS computer application. For example, on December 11, 2007, an incident was reported in which 9,951 letters were mailed to taxpayers containing account information for a taxpayer other than themselves. These taxpayers were notified of the disclosure and were offered credit monitoring services.

When performing our review, we found that for CSIRC the "hardcopy only" PII cases could not be readily distinguished from the electronic PII cases or mixed media incidents. For information purposes and trend analyses, the capability to separate the two types of cases could be beneficial and would eliminate a manual process. The OPIP maintains a separate database intended to facilitate this type of analysis while programming changes are being pursued for the CSIRC reports. A revision to the report intake form is also underway.

---

<sup>6</sup> Equifax is a consumer credit reporting agency. It is not a government entity.



---

*The Program to Protect Hardcopy Personally Identifiable  
Information Is a Work-in-Progress*

---

## ***Recommendation***

**Recommendation 1:** We recommend that the Director, Privacy, Information Protection and Data Security collaborate with the Director, Computer Security Incident Response Center to develop a specific category code to segregate the hardcopy PII losses from other data losses.

**Management's Response:** IRS management will continue to update reporting and tracking processes to support identifying trends and develop mitigation strategies. Management found that the CSIRC database has the capability to segregate hardcopy PII losses from other data losses.

## **Shipping Hardcopy PII**

The inadvertent disclosure of PII during shipping has been identified as a priority. The OPIP has contracted with a consulting firm to complete an Enterprise-wide Risk and Compliance Assessment on shipping by August 2008. The IRS shipped more than 3 million packages with UPS and millions more pieces domestically through the United States Postal Service during Fiscal Year 2007. This mail included over 150 million letters and notices mailed to taxpayers in addition to tax returns and files shipped between IRS offices, many containing hardcopy PII.

According to IRS officials, in FY 2007, 183 packages sent via UPS were reported lost or damaged in shipment. However, two were determined to contain office supplies and did not pose any disclosure risk. Of the 181 packages for which disclosure might have been an issue, 21 were identified by IRS employees and of these, 18 were recovered and 3 remain unaccounted for. UPS notified the IRS of 160 lost or damaged packages that it identified. The status of the 160 packages is shown in Figure 2 on the next page.



*The Program to Protect Hardcopy Personally Identifiable Information Is a Work-in-Progress*

**Figure 2: Status of UPS Packages**

<b>NUMBER OF PACKAGES</b>	<b>RESULTS OF INVESTIGATION</b>
77	The packages were sent to the UPS mail facility and were jointly reviewed by the UPS and the IRS's Postal and Transport Policy staff.
28	The packages were empty upon discovery and the shipping label or UPS billing invoice did not include a named individual shipper or receiver; however, there was enough information to determine that they were being shipped to and from large IRS offices. Neither the IRS nor UPS know the extent of potential disclosure from these packages.
26	The packages were damaged and the contents returned to the IRS.
17	Packages were sent to the UPS mail facility but were identified by the IRS and forwarded to the correct destinations.
12	Shippers or receivers were identified and notified of the loss and the documents were recovered.

*Source: IRS Postal and Transport Policy Staff.*

A couple of observations can be made from the loss of these packages. First, the evidence suggests that originators do not always complete the Document Transmittal, Form 3210. This form identifies the specific documents that are being shipped. IRS procedures require that originators follow up if a receipt copy of the Form 3210 is not received. Second, originators did not always use the tracking features provided by UPS to ensure that the package reached its destination.

According to the IRS staff responsible for postal and transport policy within the IRS, UPS packages are delayed or fail to reach their intended destination largely because:

- The package is improperly packed. This allows the contents to shift during shipment and can cause the packages to fall. If the box breaks, some or all of the contents can be visible to vendor employees.
- The outer label is the only source that identifies the shipping and receiving locations. In some cases the labels are torn off or are rendered unreadable.
- The package is improperly sealed, and this can lead to documents being separated from the package.



---

*The Program to Protect Hardcopy Personally Identifiable Information Is a Work-in-Progress*

---

Guidelines and shipping instructions for packages containing sensitive PII documents are available on the IRS web site and the IRS has published *Package Preparation Guidelines*.<sup>7</sup> In addition, the OPIP is working with over 50 contracted mailrooms to accept recommendations resulting from the shipping risk assessment.

During this inspection, we noted that shipments of tax returns and other documents to Federal Records Centers were not included in the shipping risk assessment. These shipments often include tax returns and usually contain PII. Due to unique requirements,<sup>8</sup> the OPIP is considering conducting a separate Federal Records Center shipment risk assessment. In 2004 and 2007, the Treasury Inspector General for Tax Administration and the Government Accountability Office<sup>9</sup> both reported that the IRS needed a better system to track case files because many could not be located.

## ***Recommendations***

We recommend that the Director, Privacy, Information Protection and Data Security:

**Recommendation 2:** Require originators to list identifying taxpayer data (excluding the SSN) on the Form 3210 (Document Transmittal) or other document that lists all items being sent to ensure that specific documents can be identified for notification when a loss occurs.

**Management's Response:** IRS management agrees that the IRS should continue to educate employees on existing shipping policies and procedures, including the use of the Form 3210. The effectiveness of the document transmittal process will also be evaluated during a shipping process risk assessment.

**Recommendation 3:** Implement requirements for: 1) mandatory monitoring of all shipments by the originator to ensure receipt or initiate follow-up actions as appropriate; 2) following the suggestions of the Postal and Transportation Policy unit to improve packing to prevent movement within the shipping box; 3) using duplicate UPS shipping labels, preferably with the tracking number securely attached to the inner package contents, which should be wrapped or double-boxed, and; 4) using shipping tape, in addition to the peel and stick adhesive strip supplied on the box, for those packages exceeding five pounds.

**Management's Response:** IRS management agrees that the IRS should continue to update policies and procedures to strengthen shipping controls. Because of the

---

<sup>7</sup> IRS Document 12506 [9-2007].

<sup>8</sup> Examples of some of the unique requirements are: special regulation boxes with specific labels, Standard Form 135, for determination of future disposition; and in the case of grand jury records, special red printed tape for grand jury records.

<sup>9</sup> *Better Procedures Are Needed to Locate, Retrieve, and Control Tax Records* (Reference Number 2004-10-186, dated September 2004) and *Tax Administration: The Internal Revenue Service Can Improve Management of Paper Case Files* (Reference Number GAO-07-1160, dated September 2007).



---

*The Program to Protect Hardcopy Personally Identifiable Information Is a Work-in-Progress*

---

importance of this topic, the IRS is conducting a shipping process risk to further provide insight and validation for these and other improvement opportunities. The Director, PIPDS, will continue to work with key stakeholders in various offices across the enterprise to implement procedural improvements to strengthen IRS shipping procedures.

**Recommendation 4:** Perform a risk assessment of the shipments of documents to the Federal Record Centers.

**Management's Response:** IRS management agreed with this recommendation. The scope of the shipping risk assessment will include the shipping of tax returns and other taxpayer and employee data from IRS facilities to the Federal Record Centers.

**Implementation of the Social Security Number Reduction and Elimination Plan**

The Office of Personnel Management is creating a Unique Identification Number to replace SSNs on official employment records. Implementation of the nine-digit number is expected by November 2008. The OPIP submitted a plan for SSN Elimination and Reduction to the Department of the Treasury in August 2007, issued the Internal Revenue Service Social Security Number Elimination and Reduction Implementation Plan on November 29, 2007, and expects to complete all the actions in the plan by March 2009.

The IRS is cataloging and assessing the collection, usage, and display of the SSNs in five core areas:

- Taxpayer notices.
- Human Resources systems.
- Internal management systems.
- Operational systems.
- Paper Loss/Hard Copy Documents, in addition to the FISMA inventory. The focus on Paper Loss/Hard copy will address the protection of documents during shipping and storage, and system errors, such as double stuffing (notices for more than one taxpayer are inserted into one envelope).

The project team will develop policies and procedures detailing the requirements for using SSNs, when necessary, and eliminating or reducing their use when not necessary. This would include using only the last four digits of the SSN, a unique identifier, or just a person's name in correspondence. The plan also proposes other alternatives to the SSN, such as barcodes and Personal Identification Numbers. The team also met with the Social Security Administration staff to better understand how to reduce the use of SSNs as personal identifiers. These efforts have resulted in a number of successes, including the partial masking of SSNs on 18 Automated



---

*The Program to Protect Hardcopy Personally Identifiable Information Is a Work-in-Progress*

---

Collection System<sup>10</sup> notices beginning in 2009. Two other SSN usage reductions occurred this year. The SSNs on Federal tax lien documents filed in public records were partially redacted, and they were also redacted on the economic stimulus payment notices sent to taxpayers.

**Operation R.E.D. (Review, Encrypt and/or Safeguard and Decide) Is in Progress**

On April 16, 2008, Commissioner Shulman introduced the Operation R.E.D. initiative. This is an agency-wide effort to remind IRS employees of existing policies and procedures about safeguarding and protecting sensitive information. By June 30, 2008, employees were required to have completed the following process:

- Reviewed their electronic files and paper holdings for sensitive information that is required to be secured.
- Encrypted (electronic) and safeguarded (paper) all sensitive information covered by a “need to know” (a continued business need to keep in their possession).
- Decided whether information they no longer need to know should be archived or destroyed.

Guidance for both managers and employees, including encryption and safeguarding instructions, has been published on the IRS intranet. The guidance includes reiterating IRS’s Clean Desk policy, and requires that protected data must be stored in a locked container when non-IRS personnel have area access during non-duty hours. Furthermore, when PII is in an unsecured area, including in an employee’s home, it must be stored in a locked container during non-duty hours. Finally, documents stored offsite, such as at the taxpayer’s office, must be in containers with bars and locks.

The guidance also suggests good document shipping practices. It states that when employees ship documents to another IRS facility, they should: 1) use UPS; 2) double wrap or double box the contents; 3) place shipping labels both inside the envelope or box and on the outside; and 4) monitor the tracking number to confirm receipt. Shipments of tax returns and information will be documented on Form 3210 and monitored to ensure that the shipment is received and acknowledged in a proper and timely manner. Every IRS office that ships tax returns and return information shall designate specific individuals to be responsible for monitoring the shipments.

In addition, employees are required to follow the recordkeeping requirements of the Internal Revenue Manual for Recordkeeping and Disclosures. The guidance also provides PII loss procedures and instructs employees to notify their manager, CSIRC, TIGTA, and the police, if applicable. Managers are required to certify that Operation R.E.D. was discussed with employees and that the employees were given time to complete Operation R.E.D. activities.

---

<sup>10</sup> A telephone contact system through which telephone assistants collect unpaid taxes and secure tax returns from delinquent taxpayers who have not complied with previous notices.



*The Program to Protect Hardcopy Personally Identifiable  
Information Is a Work-in-Progress*

---

**SUMMARY**

The Office of Privacy, Information Protection and Data Security has made significant achievements in a relatively short time period. The overwhelming majority of hardcopy PII that is shipped arrives without incident. However, for the packages that are compromised, the potential for identify theft is often high. The continued efforts to remind employees to safeguard hardcopy PII should help mitigate the risks of shipping documents between offices.



---

*The Program to Protect Hardcopy Personally Identifiable Information Is a Work-in-Progress*

---

## **Appendix I**

### *Detailed Objective, Scope, and Methodology*

The overall objective of this review was to determine what actions the Internal Revenue Service (IRS) is taking to protect hardcopy personally identifiable information (PII)<sup>1</sup> that is shipped from office to office and how the IRS responds when a potential disclosure of hardcopy PII occurs.

This review was conducted because the Inspector General has expressed concerns about the number of hardcopy PII loss incidents that have come to his attention over the past several months. While most attention to PII is rightfully on PII in electronic format, the IRS still transports large volumes of hardcopy PII outside of the agency's physical perimeter via commercial vendors (primarily via UPS) and the U.S. Postal Service.

We reviewed all 63 incidents reported to the Incident Management Team in the period January 1, 2008 through March 31, 2008. We found that 21 of the 63 (33 percent) involved hardcopy PII that was shipped via UPS. To accomplish our objective, we:

- I. Determined what hardcopy PII includes and what is at risk.
  - A. Determined what hardcopy PII is mailed between IRS offices.
  - B. Determined what hardcopy PII is sent to taxpayers and/or their representatives.
- II. Determined what legislative, regulatory, and administrative requirements exist that address hardcopy PII.
  - A. Determined what general laws pertain to hardcopy PII.
  - B. Determined what IRS-specific laws pertain to hardcopy PII.
  - C. Determined what OMB requirements pertain to hardcopy PII.
- III. Determined the organizational context of hardcopy PII.
  - A. Determined the volume of annual mailings of notices and letters.
  - B. Determined the volume of annual shipment of small packages.
  - C. Determined the volume of annual hardcopy PII losses.

---

<sup>1</sup> Personally identifiable information (PII) refers to information that 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. Hardcopy PII is in paper or other physical form rather than electronic format, such as on a laptop.



*The Program to Protect Hardcopy Personally Identifiable  
Information Is a Work-in-Progress*

---

- IV. Determined IRS efforts to address hardcopy PII.
  - A. Determined the Office established to address protection of hardcopy PII.
  - B. Determined IRS policies and procedures regarding hardcopy PII.
  - C. Determined what current actions have been taken to address hardcopy PII.
- V. Determined the IRS Breach Notification Policy.
  - A. Determined the IRS policies and procedures regarding reporting breaches.
  - B. Determined how reported breaches are addressed.
  - C. Determined the breach notification process in place.



*The Program to Protect Hardcopy Personally Identifiable  
Information Is a Work-in-Progress*

---

**Appendix II**

*Major Contributors to This Report*

Kevin P. Riley, Acting Director, Office of Inspections and Evaluations  
Dolores Castoro, Lead Auditor  
Linda P. Lee, Program Analyst



*The Program to Protect Hardcopy Personally Identifiable  
Information Is a Work-in-Progress*

---

**Appendix III**

*Report Distribution List*

Commissioner C  
Office of the Commissioner – Attn: Chief of Staff C  
Chief, Privacy, Information Protection, and Data Security OS:P  
Chief Counsel CC  
National Taxpayer Advocate TA  
Director, Office of Legislative Affairs CL:LA  
Director, Office of Program Evaluation and Risk Assessment RAS:O  
Office of Internal Control OS:CFO:CPIC:IC  
Audit Liaison: Operations Support



*The Program to Protect Hardcopy Personally Identifiable Information Is a Work-in-Progress*

**Appendix IV**

*Management's Response to the Draft Report*



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

Treasury Inspector General  
for Tax Administration

Received

AUG 06 2008

August 4, 2008

MEMORANDUM FOR ACTING DEPUTY INSPECTOR GENERAL FOR INSPECTIONS  
AND EVALUATIONS



FROM: Director, Privacy, Information Protection and Data Security

SUBJECT: Draft Inspection Report – The Program to Protect Hardcopy  
Personally Identifiable Information Is a Work-in-Progress  
(Inspection #200810IE008)

Thank you for the opportunity to respond to the referenced draft report. Protecting Personally Identifiable Information (PII) is vital to the mission of the IRS and to the goal of maintaining the public's trust in this country's tax administration system. The IRS is the custodian of vast amounts of sensitive taxpayer and employee data, and the protection of this data is a top priority for the Service. This includes the protection of hardcopy data that may be lost during the shipping process when it is shipped from various IRS facilities.

To strengthen our enterprise-wide approach to identity protection and data security, the IRS established the Office of Privacy, Information Protection, and Data Security (PIPDS) in July 2007. PIPDS is led by a Senior Executive who reports directly to the Deputy Commissioner for Operations Support, which enables the office to reach across all IRS organizations and ensure that proper attention and discipline are given to the issues of privacy, identity theft, and data security.

**Data Protection Strategy**

With the increased focus on privacy issues in the Federal government and the growing threat of identity theft, the IRS has taken additional action to ensure that taxpayer information and other PII are properly protected. Our three-point plan for protecting sensitive information focuses on Prevention, Data Loss Management, and Accountability.



---

*The Program to Protect Hardcopy Personally Identifiable Information Is a Work-in-Progress*

---

2

In November 2007, we chartered a working group that includes representatives from all business divisions and functional units to identify opportunities to prevent hardcopy data losses at the IRS. In January 2008, the IRS developed a Data Loss Prevention Action Plan (Action Plan), which focuses on enterprise activities targeted at decreasing IRS data loss incidents. This plan includes some 35 actions, including enhanced information tracking and incident reporting, business process risk assessments, and employee training and awareness.

As part of the Action Plan, a cross functional group is currently analyzing our data loss reporting and tracking systems, including the Computer Security Incident Response Center (CSIRC) incident intake process, to make improvement recommendations. This effort will provide improved tracking and reporting of data loss incidents reported by IRS employees.

The IRS continues to evaluate the use of Social Security Numbers (SSNs) in our systems to identify opportunities to minimize or eliminate the use of SSNs where possible. For example we are analyzing our notice processes to determine where it is appropriate and feasible to mask the display of the full SSN on certain notices sent by the IRS to taxpayers.

We are evaluating key IRS business processes through our Business Process Risk Assessment program to identify and remediate vulnerabilities that could lead to the unauthorized disclosure or loss of sensitive information. Although shipping losses represent only a small fraction of the millions of documents shipped each year by the IRS, these losses can damage the public confidence in the IRS and put taxpayers and employees at risk of becoming victims of identity theft. Therefore, we initiated a review of the shipping process at the IRS to assess the risk of identity theft associated with current IRS procedures for shipping tax returns and other taxpayer and employee data externally and between IRS facilities. This assessment includes the development of strategies to mitigate the risk of hardcopy loss associated with the shipment of sensitive information.

We have taken several aggressive actions this year protect sensitive data, including the distribution of an educational DVD to IRS managers on how to safeguard sensitive information & information technology equipment. We have also recently completed a two-month Service-wide educational and awareness initiative focused on providing all employees with assistance and guidance in protecting sensitive information. In addition, we are promoting employee accountability for protecting information and assets by emphasizing employee rules of behavior, adherence to security policies, and application of consistent policy and sanctions.

**Recommendation 1:** We recommend that the Director, Privacy, Information Protection and Data Security collaborate with the Director, Computer Security Incident Response Center to develop a specific category code to segregate hardcopy PII losses from other data losses.



---

*The Program to Protect Hardcopy Personally Identifiable  
Information Is a Work-in-Progress*

---

3

**CORRECTIVE ACTION**

We agree that the IRS should continue to enhance its data loss reporting and tracking processes; however, after further review of this recommendation, we find that the CSIRC database already has this capability. We will continue to update our reporting and tracking processes to support identifying trends and develop mitigation strategies.

**IMPLEMENTATION DATE**

N/A

**RESPONSIBLE OFFICIAL**

N/A

**CORRECTIVE ACTION MONITORING PLAN**

N/A

***Recommendation 2:*** Require originators to list identifying taxpayer data (excluding the SSN) on the Form 3210 (Document Transmittal) or other document that lists all items being sent to ensure that specific documents can be identified for notification upon a loss.

**CORRECTIVE ACTION**

We agree that the IRS should continue to educate employees on executing existing shipping policies and procedures including the use of the document transmittal Form 3210 (Document Transmittal). Elimination and reduction of the use of SSNs on internal forms is part of our current SSN Elimination and Reduction plan, and we will include the review of the Form 3210 usage as part of this initiative. We will also evaluate the effectiveness of the document transmittal process as we carry out the business process risk assessment on shipping.

**IMPLEMENTATION DATE**

Ongoing

**RESPONSIBLE OFFICIAL**

Director, Privacy, Information Protection and Data Security

**CORRECTIVE ACTION MONITORING PLAN**

Not Applicable

***Recommendation 3:*** Implement requirements for: 1) mandatory monitoring of all shipments by the originator to ensure receipt or initiate follow-up actions as appropriate; 2) following the suggestions by the Postal and Transportation Policy unit to improve packing to prevent movement within the shipping box; 3) using duplicate UPS shipping



---

*The Program to Protect Hardcopy Personally Identifiable  
Information Is a Work-in-Progress*

---

4

labels, preferably with the tracking number securely attached to the inner package contents that should be wrapped or double-boxed, and, 4) using shipping tape in addition to the peel and stick adhesive strip supplied on the box for those packages exceeding five pounds.

**CORRECTIVE ACTION**

We agree that the IRS should continue to update our policies and procedures to strengthen shipping controls. As recognized in your report, the IRS identified multiple enhancements to strengthen shipping procedures during the development of the Data Loss Prevention Action Plan in January 2008, including the process enhancements reflected in the recommendation above. Because of the importance of this issue, we are conducting the business process risk assessment for shipping to provide further insight and validation for these and other improvement opportunities. The Director, PIPDS will continue to work with key stakeholders in various offices across the enterprise to implement the procedural improvements to strengthen IRS shipping procedures.

**IMPLEMENTATION DATE**

Ongoing

**RESPONSIBLE OFFICIAL**

Director, Privacy, Information Protection and Data Security

**CORRECTIVE ACTION MONITORING PLAN**

Not Applicable

***Recommendation 4:*** Perform a risk assessment on the shipments of documents to the Federal Record Centers.

**CORRECTIVE ACTION**

We agree, and will expand the scope of our business process risk assessment of the shipping process at the IRS to include the process for shipping tax returns and other taxpayer and employee data from IRS facilities to the Federal Records Centers.

**IMPLEMENTATION DATE**

December 2008

**RESPONSIBLE OFFICIAL**

Director, Privacy, Information Protection and Data Security

**CORRECTIVE ACTION MONITORING PLAN**

Not Applicable