TREASURY INSPECTOR GENERAL FOR TAX ADMINISTRATION

Employees Sometimes Did Not Adhere to E-mail Policies Which Increased the Risk of Improper Disclosure of Taxpayer Information

October 14, 2016

Reference Number: 2017-30-010

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
E-mail Address / TIGTACommunications@tigta.treas.gov
Website / http://www.treasury.gov/tigta

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

1-800-366-4484

By Web:

www.treasury.gov/tigta/

Or Write:

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

Information you provide is confidential and you may remain anonymous.

EMPLOYEES SOMETIMES DID NOT ADHERE TO E-MAIL POLICIES WHICH INCREASED THE RISK OF IMPROPER DISCLOSURE OF TAXPAYER INFORMATION

Highlights

Final Report issued on October 14, 2016

Highlights of Reference Number: 2017-30-010 to the Deputy Commissioner for Operations Support and the Deputy Commissioner for Services and Enforcement.

IMPACT ON TAXPAYERS

Personally Identifiable Information (PII) is a specific type of sensitive information which may include tax return and return information. Laws require that the IRS protect PII and tax return and return information (taxpayer PII/tax return information) for different reasons, including the protection of privacy and because the loss, theft, or unauthorized disclosure places individuals at serious risk for identity theft. Additionally, the proper protection of taxpayer PII and tax return information helps maintain taxpayer confidence and the IRS's reputation for privacy protection, which are critical for the IRS to perform its mission.

WHY TIGTA DID THE AUDIT

This audit was initiated because electronic mail (e-mail) is a prevalent form of communication in the IRS. Employees who have frequent contact with taxpayers, *i.e.*, revenue officers and revenue agents, need to ensure that appropriate steps to safeguard e-mails are being taken. The overall objective was to determine whether Small Business/Self-Employed (SB/SE) Division employees are following e-mail policies and properly safeguarding taxpayer PII/tax return information contained in e-mail correspondence.

WHAT TIGTA FOUND

TIGTA reviewed a random sample of 80 SB/SE Division employees' e-mails sent during four weeks in May and June 2015, and determined that 39 (49 percent) employees sent a total of 326 unencrypted e-mails containing 8,031 different taxpayers' PII/tax return information internally to other IRS employees or externally to non-IRS e-mail accounts. TIGTA identified 275 unencrypted e-mails that contained taxpayer PII/tax return information that were sent internally to other IRS employees. These e-mails were sent inside the IRS internal information system firewall, and therefore pose less risk of improper disclosure or improper access. TIGTA also identified 51 unencrypted e-mails that contained taxpayer PII/tax return information that were sent externally to non-IRS e-mail accounts. These employees failed to follow Internal Revenue Manual (IRM) requirements and risked exposing the information to unauthorized persons.

Additionally, 20 e-mails sent by six employees to personal e-mail accounts involved official IRS business. SB/SE Division employees may not be aware of the restriction on using personal e-mail because the *Standards for Using Email* IRM does not include this restriction.

The IRS Enterprise e-Fax (EEFax) capability was implemented in early 2013 without encryption capability. TIGTA identified 193 unencrypted e-mails that contained taxpayer PII/tax return information that were routed to the EEFax servers via the e-mail system. Because the EEFax does not use encryption, its use could result in the interception and disclosure of taxpayer PII/tax return information.

WHAT TIGTA RECOMMENDED

TIGTA recommended that the IRS consider the feasibility of a systemic solution to ensure that PII/tax return information is encrypted, and until such time consider requiring the default Outlook setting for certain employees to encrypt sent e-mail messages; ensure that managers are aware of e-mail violations and take appropriate disciplinary action; update the IRM to include that no IRS employee may use a personal e-mail account to conduct official business of the Government; and request an information technology update to allow encrypted messages to be sent to the EEFax server.

In response to the report, IRS officials agreed with the recommendations and plan to take corrective actions.

TREASURY INSPECTOR GENERAL
FOR TAX ADMINISTRATION

DEPARTMENT OF THE TREASURY

WASHINGTON, D.C. 20220

October 14, 2016

MEMORANDUM FOR Deputy Commissioner for Operations Support
Deputy Commissioner for Services and Enforcement

FROM: Michael E. McKenney
Deputy Inspector General for Audit

SUBJECT: Final Audit Report – Employees Sometimes Did Not Adhere to E-mail Policies Which Increased the Risk of Improper Disclosure of Taxpayer Information (Audit # 201530035)

This report presents the results of our review to determine whether Small Business/ Self-Employed Division employees are following electronic mail (e-mail) policies and properly safeguarding Personally Identifiable Information and tax return and return information contained in e-mail correspondence. The audit was included in our Fiscal Year 2016 Annual Audit Plan and addresses the major management challenge of Tax Compliance Initiatives.

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

Copies of this report are also being sent to the Internal Revenue Service managers affected by the report recommendations. If you have any questions, please contact me or Matthew A. Weir, Assistant Inspector General for Audit (Compliance and Enforcement Operations).

Table of Contents

Abbreviations

DLP	Data Loss Prevention
EEFax	Enterprise e-Fax
IRM	Internal Revenue Manual
IRS	Internal Revenue Service
IT	Information Technology
PGLD	Privacy, Governmental Liaison, and Disclosure
PII	Personally Identifiable Information
SB/SE	Small Business/Self-Employed
SBU	Sensitive But Unclassified
SPIIDE	Safeguarding Personally Identifiable Information Data Extracts

Background

Internal Revenue Code § 6103 generally protects the confidentiality of taxpayers' tax return and return information. Under Federal law, Internal Revenue Service (IRS) employees or officers are subject to criminal penalty provisions and the taxpayer can bring civil action against the United States for the unauthorized inspection or disclosure of returns or return information.[1] If any officer or employee of the United States knowingly, or by reason of negligence, inspects or discloses any return or return information with respect to a taxpayer in violation of any provision of § 6103, the taxpayer may bring a civil action for damages against the United States in a district court of the United States.[2] The Internal Revenue Code makes it unlawful for any officer or employee of the United States or any person described in § 6103(n) (or an officer or employee of any such person), or any former officer or employee, willfully to disclose to any person, except as authorized in this title, any return or return information. Any violation shall be a felony punishable upon conviction by a fine in any amount not exceeding $5,000, or imprisonment of not more than five years, or both, together with the costs of prosecution, and if such offense is committed by any officer or employee of the United States, he or she shall, in addition to any other punishment, be dismissed from office or discharged from employment upon conviction for such offense.[3]

Sensitive But Unclassified (SBU) information is any information that requires protection due to the risk and magnitude of loss or harm to the IRS or the privacy to which individuals are entitled under 5 United States Code § 552a (the Privacy Act), which could result from inadvertent or deliberate disclosure, alteration, or destruction.[4] Personally Identifiable Information (PII) is a specific type of sensitive information which may include tax return and return information. The Internal Revenue Manual (IRM)[5] provides a detailed list of information the IRS deems to be PII, including the personal data of taxpayers, as well as personal information of employees, contractors, applicants, and visitors to the IRS.[6]

It is important that taxpayer PII/tax return and return information (taxpayer PII/tax return information) be protected because the loss, theft, or unauthorized disclosure of taxpayer PII/tax return information places individuals at serious risk for identity theft and invasion of privacy. Additionally, the proper protection of taxpayer PII/tax return information helps maintain taxpayer confidence and the IRS's reputation for privacy protection, which are critical for the

[1] Internal Revenue Code §§ 7213, 7213A, and 7431.
[2] Internal Revenue Code § 7431(a)(1).
[3] Internal Revenue Code § 7213(a)(1).
[4] Internal Revenue Manual 1.10.3.2.1(1) (Nov. 12, 2015).
[5] The primary, official source of instructions to staff related to the organization, administration, and operation of the IRS.
[6] IRM 1.10.3.2.1(2) (Nov. 12, 2015). Detailed examples are located in IRM 10.8.1.4.14.1.3 (Jul. 8, 2015).

IRS to perform its mission. Encryption is the process of transforming plain or clear text information into an unreadable text, so the data being transmitted can only be opened by the end user for whom the data are intended. IRS employees should never include taxpayer PII/tax return information in electronic mail (e-mail) messages or attachments unless an IRS-approved encryption technology is used.[7]

The IRS uses the Secure Enterprise Messaging System (Secure Messaging) to send Microsoft Outlook[8] messages that contain taxpayer PII/tax return information.[9] Secure Messaging enables IRS employees to digitally encrypt internal e-mail messages and attachments for transmission between IRS employees. Secure Messaging enrollment is an automated process for all IRS local area network accounts with an Exchange mailbox. Alternatively, IRS employees may encrypt files to be e-mailed as attachments using encryption technology software approved by the IRS's Information Technology (IT) function. However, IRS employees may not send taxpayer PII/tax return information by e-mail outside the IRS unless an IT function-approved exception is obtained.

Employees should never consider e-mail to be secure and should not include taxpayer, SBU, or PII/tax return information in e-mail messages or attachments unless they use IRS-approved encryption technology.[10] Taxpayer PII/tax return information may be transmitted to other IRS employees provided the recipient has a need to know the information and release is otherwise consistent with statutory requirements.[11] Subject lines are not encrypted and should not contain taxpayer PII/tax return information. Employees can receive e-mail containing taxpayer PII/tax return information from taxpayers or their representatives; however, taxpayer PII/tax return information may not be sent to parties outside of the IRS, including other Government agencies, taxpayers, or their representatives even if specifically authorized by the taxpayer. Any exceptions to sending taxpayer PII/tax return information externally must have the approval of the IT function Office of Cybersecurity Policy and Program Management. Employees are also discouraged from sending their own PII/tax return information to their home e-mail address, but if they do, they are required to encrypt any attachments containing their own PII/tax return information.[12]

In the IRS Small Business/Self-Employed (SB/SE) Division, e-mail is a prevalent form of communication. SB/SE Division employees who have frequent contact with taxpayers, *i.e.*, revenue officers and revenue agents, need to ensure that appropriate steps to safeguard e-mails are being taken. The casual nature of e-mail results in a higher risk of taxpayer PII/tax

[7] Messages distributed by electronic means from one computer user to one or more recipients via a computer network.
[8] E-mail software commonly used by the IRS.
[9] IRM 1.10.3.2.1(4) (Nov. 12, 2015).
[10] IRM 1.10.3.2.1(3) (Nov. 12, 2015).
[11] IRM 11.3.1.14.2(1)(c) (Mar. 29, 2011).
[12] *Keep all PII – even your own – secure when sending it via e-mail*; IRS Headlines article published Apr. 6, 2009.

return information and sensitive information of taxpayers and IRS employees being accessed by unauthorized persons.

This review was performed with information obtained from the SB/SE Division Headquarters in Washington, D.C., and in Austin, Texas, during the period September 2015 through April 2016. 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

Unencrypted E-mails Contained Taxpayers' Personally Identifiable Information and Tax Return Information

We reviewed a random sample of 80 SB/SE Division employees' e-mails sent during May and June 2015 and determined that 39 (49 percent) employees sent a total of 326 unencrypted e-mails containing 8,031 different taxpayers' PII/tax return information.[13] Based on our sample results, we estimate that 11,416[14] SB/SE Division employees sent 95,396 unencrypted e-mails with taxpayer PII/tax return information for 2.4 million taxpayers during the four-week period of our sample.[15] If this four-week period is typical, we estimate that more than 1.1 million unencrypted e-mails with taxpayer PII/tax return information of 28.2 million taxpayers could be sent annually.[16] These unencrypted e-mails violated IRM requirements and potentially compromised the security of taxpayer information. Employees sent unencrypted e-mails with taxpayer PII/tax return information internally to other IRS employees or externally to non-IRS e-mail accounts. However, the majority of these unencrypted e-mails (275 of the 326) were sent internally to other IRS employees, which poses less risk of improper disclosure or improper access than those that were sent externally.

- 275 unencrypted e-mails were sent internally to other IRS employees, which contained 8,010 different taxpayers' PII/tax return information. Because these e-mails were sent inside the IRS internal firewall, there is limited risk of access from external third parties.[17] There is potential that these e-mails could be sent to internal recipients that should not have access to the taxpayers' PII/tax return information in the e-mail.

[13] The employees in our sample included revenue agents, revenue officers, tax examiners, secretaries, or contact representatives.
[14] The point estimate projection is based on a two-sided 95 percent confidence interval. We are 95 percent confident that the point estimate is between 8,764 and 14,090. See Appendix IV for additional information on our sampling methodology.
[15] The projection is based on a two-sided 95 percent confidence interval. We are 95 percent confident that the estimate of unencrypted e-mails is between 51,239 and 139,553 and the estimate of taxpayers that may have been affected is between 8,031 and 5,950,157.
[16] The projection is based on a two-sided 95 percent confidence interval. We are 95 percent confident that the estimate of unencrypted e-mails is between 614,867 and 1,674,631 and the estimate of taxpayers that may have been affected is between 96,372 and 71,401,886.
[17] An information security firewall is an integrated collection of security measures designed to prevent unauthorized electronic access to a networked computer system.

- 51 unencrypted e-mails were sent externally to non-IRS e-mail accounts, including:
  - 28 e-mails sent directly to taxpayers.
  - 14 unencrypted e-mails sent to taxpayers' representatives, which contained 7 taxpayers' PII/tax return information.
  - 3 unencrypted e-mails sent to other Government agencies or a third party, which contained three taxpayers' PII/tax return information.
  - 6 unencrypted e-mails sent to employees' personal e-mail addresses, ****1***** **********1**********.

The IRS has established penalties, ranging from admonishment to removal, for employees who send unencrypted e-mails with taxpayer PII/tax return information; however, there was no evidence provided that these penalties were enforced.[18] Based on additional statistical analysis, we estimate that 3.9 percent[19] of all SB/SE Division employee e-mails contain one or more violations, with most being internal e-mails (3.3 percent).[20]

On May 22, 2015, the IRS IT function Cybersecurity organization deployed the Safeguarding Personally Identifiable Information Data Extracts (SPIIDE) automated Data Loss Prevention (DLP) tool. This tool monitors outgoing external unencrypted e-mail traffic (including attachments) and external unencrypted web traffic to identify and block taxpayer Social Security Numbers. The SPIIDE DLP tool does not monitor encrypted e-mails or e-mails that are sent internally within the IRS; therefore, it would not have identified the internal unencrypted e-mails with taxpayer Social Security Numbers or other taxpayer PII/tax return information.

At the time of our review, the SPIIDE DLP tool only identified Social Security Numbers, so any other PII/tax return information would not be detected or blocked. Examples of taxpayer PII/tax return information that would not be detected include: Employer Identification Numbers, taxpayer names, addresses, telephone numbers, *etc*. Of the 51 unencrypted e-mails containing taxpayer PII/tax return information that were sent to external non-IRS e-mail accounts, 28 were sent after the SPIIDE DLP tool was deployed. While none of these e-mails contained Social Security Numbers, they did contain prohibited taxpayer PII/tax return information such as taxpayers' names, **********1**********, and specific details about the tax returns. Our sample did include one e-mail that contained an attachment with the employee's own Social Security Number. In this instance, the SPIIDE DLP tool worked as expected and successfully blocked the transmission of the unencrypted e-mail message with a Social Security Number from being sent outside of the IRS network.

[18] IRS Guide to Penalty Determinations, Aug. 13, 2007.
[19] The jackknife estimate projection is based on a two-sided 95 percent confidence interval. We are 95 percent confident that the jackknife estimate is between 2.11 percent and 5.72 percent.
[20] The jackknife estimate projection is based on a two-sided 95 percent confidence interval. We are 95 percent confident that the jackknife estimate is between 1.58 percent and 5.03 percent.

Employees did not always encrypt internal e-mails when required

Secure Messaging enables the user to digitally encrypt internal e-mail messages and attachments for transmission between IRS employees. IRS employees must use Secure Messaging for e-mail that contains SBU data.[21] In order to send a secure message, both the sender and the recipient must have Secure Messaging installed. This configuration allows authorized employees to transmit SBU information to other authorized employees within the system once they have been enrolled and received training.[22] SBU data may be transmitted to other employees provided the recipient has a need to know the information and the release of the information is otherwise consistent with statutory requirements. However, e-mail subject lines are not encrypted and should not contain SBU information.[23]

We identified 275 unencrypted internal e-mails, containing 8,010 taxpayers' PII/tax return information, which were sent by 32 (40 percent) of the 80 employees we reviewed. The number of unencrypted e-mails with taxpayer PII/tax return information sent by the 32 employees ranged from one to 44. Figure 1 shows the range of unencrypted e-mails sent by these employees and the number of taxpayers whose PII/tax return information was at risk for exposure.

Figure 1: Range of Unencrypted Internal E-mails With PII/Tax Return Information Sent by Sampled Employees

Employees	Unencrypted Internal E-mails Sent With PII/Tax Return Information	Number of Taxpayers' PII/Tax Return Information in These E-mails
20	1-5	1,039
3	6-10	648
6	11-30	78
3	31-44	6,245
Total: 32	**275**	**8,010**

Source: Treasury Inspector General for Tax Administration review of a random sample of SB/SE Division employees' sent e-mails.

Secure Messaging was not used to transmit the 275 e-mails, which resulted in vulnerable transmission of sensitive taxpayer information. Additionally, 14 of the 275 e-mails were sent with taxpayer PII/tax return information in the e-mail subject line, which cannot be encrypted and is prohibited. The taxpayer PII/tax return information in the e-mails included: taxpayer

[21] There are some exceptions which must be approved in writing by the IRS's Office of Cybersecurity.
[22] IRM 1.10.3.2.1(4) (Nov. 12, 2015).
[23] IRM 11.3.1.14.2(1)(c) (Mar. 7, 2008).

names, Social Security Numbers, Taxpayer Identification Numbers, addresses, ******1****** **********1**********. Encrypting internal e-mail does not guarantee that malicious internal users could not inappropriately access e-mails with taxpayer PII/tax return information and misuse the information for their own benefit. However, failure to encrypt internal e-mails with taxpayer PII/tax return information could result in compromised security from careless internal users who might inadvertently send it to unauthorized individuals. SB/SE Division employees who sent these e-mails did not follow IRM procedures and were not diligent about encrypting e-mails that contained taxpayer PII/tax return information.

Employees improperly sent e-mails with taxpayer PII/tax return information to external parties

IRS employees may not send e-mails with taxpayer PII/tax return information to parties outside of the IRS including other Government agencies, taxpayers, or their representatives.[24] Any exceptions must be approved by the IT function Office of Cybersecurity.[25] However, we identified 42 e-mails, containing different taxpayers' PII/tax return information, sent by six different SB/SE Division employees to either a taxpayer or his or her representative. Such e-mail transmissions are expressly prohibited. Moreover, 15 of the 42 e-mails were sent with taxpayers' PII/tax return information in the e-mail subject line, which cannot be encrypted and is prohibited. In addition, we identified three e-mails, containing three different taxpayers' PII/tax return information, sent by three different SB/SE Division employees to other Government agencies or third parties. The employees did not obtain an IT function-approved exception to transmit the data.

Although e-mail communication with taxpayers is common, SB/SE Division employees must not send e-mails with taxpayer PII/tax return information unless they obtain approval for the exception. SB/SE Division employees who sent these external e-mails failed to comply with IRM policy and jeopardized taxpayer information.

Employees sent unencrypted e-mails with taxpayer PII/tax return information to their personal e-mail accounts

Internal guidance was provided by the Office of Privacy, Information Protection, and Data Security [now Privacy, Governmental Liaison, and Disclosure (PGLD)] that stated if employees must send their own PII to their personal e-mail, they must encrypt it, although it recommended that employees not send such e-mails at all. Outside of an employee's own PII, no taxpayer PII/tax return information can ever be sent to a personal e-mail account.[26] For example, if an employee wants to send a copy of a personnel action to his or her personal e-mail, he or she must encrypt it with IRS IT function-approved encryption software and send it as an attachment.

[24] IRM 11.3.1.14.2(1)(d) (Mar. 7, 2008).
[25] IRM 11.3.1.14.2(1)(d) (Mar. 7, 2008).
[26] *Keep all PII – even your own – secure when sending it via e-mail;* IRS Headlines article published Apr. 6, 2009.

We identified six unencrypted e-mails sent by six different employees to personal e-mail accounts. **1** of the e-mails contained the employees' own PII and ********1******** **********1**********. The SB/SE Division employees who sent these e-mails failed to follow IRM requirements and risked exposing the information to unauthorized third parties.[27]

Microsoft Outlook offers users the option of encrypting all sent messages. The use of this option would automatically encrypt all internal e-mails with taxpayer PII/tax return information. Since IRS employees with an Exchange mailbox are automatically enrolled in Secure Messaging, all internal e-mails would be encrypted, which would greatly reduce the risk of sending unencrypted internal e-mails containing taxpayers' PII/tax return information. This option also provides an alert to the sender when the recipient is not capable of receiving encrypted messages, which could remind employees to remove any taxpayer PII/tax return information from the messages prior to sending them to external e-mail addresses.

Recommendations

The Deputy Commissioners for Operations Support and Services and Enforcement should:

Recommendation 1: Determine the feasibility of implementing a systemic solution to help ensure that e-mails with PII/tax return information are encrypted. Until such a solution is identified, consider requiring the default Microsoft Outlook setting to encrypt e-mail messages for compliance and enforcement employees who routinely send taxpayer information by e-mail and other employees who routinely send employee PII/tax return information, *e.g.*, human resource personnel.

> ***Management's Response:*** Management agreed with this recommendation and stated the SB/SE Division will work with the IT function to determine the feasibility of implementing a systematic solution and next steps needed. In the interim, the IRS will work to identify positions that routinely send taxpayer information by e-mail and issue interim guidance on implementing the default Microsoft Outlook encryption.

Recommendation 2: Provide additional training and issue a memorandum to remind employees that all internal and external e-mail with taxpayer PII/tax return information must be encrypted and include that:

- External e-mail with taxpayers' PII/tax return information requires written approval from the IT function Office of Cybersecurity.
- Employees sending their own PII, which is not related to their official duties, must encrypt the document containing the PII.

[27] Employees are also prohibited from using their personal e-mails to conduct official IRS business. This issue is discussed in the next section of this report.

Management's Response: Management agreed with this recommendation and stated the PGLD office issued interim guidance memorandums within the last year that addressed the use of e-mail. The following memorandums were issued:

1. Issued in June of 2016, the interim guidance PGLD-10-0616-0003, *Using IRS and Personal Email Accounts*, which addressed e-mail with taxpayers and the fact that no PII may be shared with taxpayers via e-mail (the exception being an IT function-approved secure e-mail program such as used in the Large Business and International Division). A message was sent to all IRS employees on June 22, 2016, advising of the issuance.

2. Issued in June of 2015 and then incorporated into IRM 10.5.1 (revision date June 15, 2016), the interim guidance titled *Interim Guidance on Sending Sensitive But Unclassified Information and/or Work-Related Documents to External Email Addresses,* which addressed employees sending their own PII to an external e-mail address. In combination with the beginning of the SPIIDE program, Service-wide meetings were held to go over the content in the interim guidance. The briefings also covered the requirements to encrypt e-mails that contain PII/SBU information and provided specific instructions for doing so.

3. Additional guidance has been provided in mandatory security awareness training.

Recommendation 3: Ensure that managers are aware of the violations for sending unencrypted e-mails with taxpayer PII/tax return information and that they take appropriate disciplinary action when violations occur.

Management's Response: Management agreed with this recommendation and stated the PGLD office will develop a Manager's Tool Kit that will include a reference to the Penalty Guide and how it applies to situations in which employees fail to encrypt e-mails. The SB/SE Division will begin notifying managers and their executives of incidents in which the SPIIDE DLP tool detects repeated unencrypted submission attempts by the same employee. Additionally, the Commissioner, SB/SE Division, will prepare an all manager e-mail to stress the importance of managerial awareness of the SPIIDE DLP tool.

Employees Improperly Used Personal E-mail Accounts to Conduct Official Business

Pursuant to a recent change in the law, no officer or employee of the IRS may use a personal e-mail account to conduct any official business of the Government.[28] There are two IRM sections that provide guidance to employees on the proper use of e-mail, the IT Security IRM

[28] Consolidated Appropriations Act of 2016, Pub. L. No. 114-113, § 402, 129 Stat. 2242, 3317 (2015) (codified at 26 USC §7801 note (IRS employees prohibited from using personal email accounts for official business)). .

and the *Standards for Using Email* IRM. The IT Security IRM states that non-IRS/Treasury accounts shall not be used for any Government or official purposes.[29] The *Standards for Using Email* IRM requires employees and contractors to use their personal e-mail accounts for all non-IRS official business; however, the IRM does not provide any guidance to employees about the restrictions on the use of their personal e-mail accounts to conduct official business.[30] We identified 20 e-mails sent by six employees to personal e-mail accounts that involved official IRS business. The following are the types of information included in these e-mails:

- **********1**********.[31]
- Employee performance appraisals.
- Team work and meeting schedules.
- Processing forms requesting computer access.
- Travel authorizations.
- Performance appraisal policies.
- Staffing/organization charts.
- Group work/inventory reports.
- IRS training presentations.
- IRS examination job aids.

These e-mails were sent prior to the enactment of the law prohibiting use of personal e-mail accounts to conduct official business, so they were not in violation of the law, but they did violate IRS procedures. However, because the *Standards for Using Email* IRM does not include specific guidance regarding employees' use of personal e-mail accounts to conduct official business, SB/SE Division employees may not have been aware of the restriction on using their personal e-mail. When SB/SE Division employees send official business e-mails to their personal e-mail addresses, there is a risk that confidential materials may be intercepted by unauthorized persons. The IRS should update the IRM to reflect the law, and notify and train employees about the policy.

[29] IRM 10.8.1.4.17.2.2.1 (July 8, 2015).
[30] IRM 10.8.1.4.17.7(3) (July 8, 2015).
[31] As previously discussed, **********1**********, which are included in the six unencrypted e-mails sent by six different employees to home e-mail accounts.

Recommendation

Recommendation 4: The Chief Technology Officer should update the *Standards for Using Email* IRM to include that no officer or employee of the IRS may use a personal e-mail account to conduct any official business of the Government. Additionally, provide training and issue a memorandum to instruct employees that they cannot send any work-related e-mails to their personal e-mail accounts.

> ***Management's Response:*** Management agreed with this recommendation and stated they will update IRM 1.10.3, *Standards for Using Email*, to include a statement that no officer or employee of the IRS may use a personal e-mail account to conduct any official business of the Government. Management stated that interim guidance memorandum PGLD-10-0616-0003 was issued on June 21, 2016, and it states that employees must always use their IRS e-mail accounts when using e-mail to conduct the official business of the IRS. Management also stated two mandatory briefing courses (Records Management Awareness, and Privacy Information Protection and Disclosure) provided training on the prohibition of using personal e-mail accounts to conduct official Government business. These briefings were required of all employees in Fiscal Year 2016.

Facsimiles Sent Using the Enterprise e-Fax Program Are Not Encrypted

The IRS implemented an automated system that allows all IRS employees to send facsimiles (fax) to any recipient from their IRS computer. This system, referred to as Enterprise e-Fax (EEFax), allows employees to use their e-mail accounts to send a message that is routed to the IRS's EEFax system, where the message and all qualified attachments are converted into a fax signal and transmitted onto an analog telephone line. The EEFax system infrastructure is located in two IRS Computing Centers in Memphis, Tennessee, and Martinsburg, West Virginia.[32] The system infrastructure in both locations resides within access-controlled computer room space and is connected to IRS-controlled network switching equipment.

IRS policy requires all e-mails with taxpayer PII/tax return information to be encrypted; however, EEFax system e-mail messages are not encrypted. Although these e-mails are routed to an explicit e-mail domain that belongs to the EEFax system and is located within IRS-controlled spaces, these e-mail messages are sent through Microsoft Outlook just like other internal e-mail messages that are required to be encrypted. After the e-mail is transmitted to the explicit e-mail domain, it is transmitted to the recipient over an analog telephone line similar to a

[32] IRS Computing Centers support tax processing and information management through a data processing and telecommunications infrastructure.

normal facsimile message. We identified 193 e-mails that contained taxpayer PII/tax return information that were routed to the EEFax system servers via the e-mail system.[33]

IRS EEFax system capability was implemented in early Calendar Year 2013 without the capability to send EEFax system e-mails with taxpayer PII/tax return information encrypted. In July 2015, the IRS completed an internal review that concluded that because the EEFax system does not use encryption, its use could result in the interception and disclosure of taxpayer PII/tax return information.[34] The review also determined that the required Risk Acceptance Request to approve the risk of sending e-mails with taxpayer PII/tax return information unencrypted using the EEFax system was never prepared. As a result, in October 2015, management approved the required forms; however, this action occurred more than five years after the system was implemented and in use by IRS employees. Furthermore, the approval of the Risk Acceptance Request did not mitigate the risk associated with sending unencrypted taxpayer PII/tax return information to the EEFax system servers.

Recommendation

Recommendation 5: The Chief Technology Officer should update the EEFax system to allow encrypted messages to be sent to the EEFax system server.

> ***Management's Response:*** Management stated they will determine if it is feasible to upgrade the EEFax system given the known issues of unknown cost, level of effort, training, and certificate management. Such an upgrade would ensure that all outbound EEFax system encrypted e-mail traffic containing PII information is protected within the IRS e-mail infrastructure until the EEFax system server converts the encrypted e-mail to an industry standard format and transmitted over a standard unencrypted analog telephone line to a taxpayer provided facsimile number. If management determines it to be feasible, they will implement programming changes to accomplish this objective subject to budgetary constraints, limited resources, and competing priorities.

[33] A computer that carries out specific functions, *e.g.*, a file server stores files, a print server manages printers, and a network server stores and manages network traffic.
[34] The review was a risk assessment conducted by the IRS PGLD office.

Appendix I

Detailed Objective, Scope, and Methodology

The overall objective was to determine whether SB/SE Division employees are following e-mail policies and properly safeguarding taxpayer PII/tax return information contained in e-mail correspondence. To accomplish our objective, we:

I. Identified current IRS procedures and guidelines used by SB/SE Division employees for sending protected information in e-mail correspondence.

II. Evaluated the IRS's compliance with procedures and guidelines by reviewing a sample of employee mailboxes for a total of four weeks. The weeks were randomly selected between March 1, 2015, and June 25, 2015. The weeks we reviewed were May 4, 2015; May 11, 2015; May 25, 2015; and June 1, 2015. (The SPIIDE DLP tool was deployed on May 22, 2015, and the IRS was notified of this audit on June 25, 2015.)

A. Selected a random sample of 80 employee Microsoft Outlook mailboxes during the selected weeks to review for protected information misuse in e-mails.[1] We selected a random sample so that we could project the results to the population of 23,410 SB/SE Division employees. The random sample of 80 employees was based on a 95 percent confidence level, 50 percent error rate, and ± 5 percent precision factor. The Treasury Inspector General for Tax Administration's contracted statistician reviewed and assisted in developing the sampling plans and projections.

B. Reviewed the sample of employee mailboxes for sent e-mails.

1. For internal sent e-mails, determined if e-mails with protected information used Secure Messaging to encrypt messages with or without attachments and that protected information was not included in the subject line of the e-mails.

2. For approved external sent e-mails:

a. Determined if protected information was included in the message body or subject line.

b. If there were attachments with protected information, verified that attachments were encrypted using Guardian Edge Removable Storage.

c. Determined if approval was received and that rules were followed for sending the protected information externally.

[1] The original sample size was 145 employees. After applying an actual error rate from initial case review results, we reduced the sample size to 80 employees.

3. For any e-mails sent by employees with their own protected information, *i.e.*, personnel actions, to personal e-mail addresses, determined if the message body or subject line included protected information and verified that attachments were encrypted using Guardian Edge Removable Storage.
4. Determined if any e-mails were sent by employees with protected information (other than their own) to an outside e-mail address. (Outside e-mail addresses could include personal, taxpayers, taxpayer representative, or other.)

III. Determined if any of the external e-mails reviewed should have been identified by the SPIIDE DLP tool as intended.

Data validation methodology

During this review, we evaluated the reasonableness of the SB/SE Division population by comparing the Data Center Warehouse totals with the Treasury Integrated Management Information System data totals provided by the IRS. The comparison supported that the data were sufficiently reliable and could be used to meet the objective of this audit. We received employee Microsoft Outlook mailboxes from the IRS. By its nature, the data could not be validated; therefore, we relied on the integrity of the data obtained from the IRS.

Internal controls methodology

Internal controls relate to management's plans, methods, and procedures used to meet their mission, goals, and objectives. Internal controls include the processes and procedures for planning, organizing, directing, and controlling program operations. They include the systems for measuring, reporting, and monitoring program performance. We determined that the following internal controls were relevant to our audit objective: IRM and IRS policies related to safeguarding taxpayer PII/tax return information and the use of e-mail encryption tools when sending taxpayer PII/tax return information. We evaluated these controls by reviewing current IRM and IRS policies related to safeguarding taxpayer PII/tax return information and reviewing employees' use of e-mail encryption tools when sending taxpayer PII/tax return information.

Appendix II

Major Contributors to This Report

Matthew Weir, Assistant Inspector General for Audit (Compliance and Enforcement Operations)
Carl L. Aley, Director
Beverly K. Tamanaha, Audit Manager
Brian G. Foltz, Lead Auditor
Julian O'Neal, Senior Auditor

Appendix III

Report Distribution List

Commissioner
Office of the Commissioner – Attn: Chief of Staff
Commissioner, Small Business/Self-Employed Division
Director, Collection Policy, Small Business/Self-Employed Division
Director, Field Collection, Small Business/Self-Employed Division
Director, Office of Audit Coordination

Appendix IV

Outcome Measure

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

Type and Value of Outcome Measure:

- Taxpayer Privacy and Security – Potential; 2,350,071 taxpayers whose PII/tax return information was sent unencrypted in either internal or external e-mails during four weeks; this equates to 28,200,857 taxpayers for the full year (see page 4).

Methodology Used to Measure the Reported Benefit:

We selected a statistically valid sample of 80 SB/SE Division employees from a total population of 23,410 SB/SE Division employees who were employed between May and June 2015.[1] A total of 8,321 sent e-mails were reviewed from May 4, 2015, to May 17, 2015, and May 25, 2015, to June 7, 2015. We selected this type of sample so we could project our results to the population of employees for this time period and evaluate the effectiveness of the SPIIDE DLP tool.

Our case review showed that 39 (49 percent) of 80 sampled employees sent at least one unencrypted e-mail that contained taxpayer PII/tax return information. A total of 326 unencrypted e-mails containing taxpayer PII/tax return information were sent during the time frame of our case review. This included:

- 275 e-mails sent internally within the IRS by 32 SB/SE Division employees, and those e-mails contained PII/tax return information of 8,010 taxpayers.
- 51 e-mails sent externally from the IRS by 15 SB/SE Division employees, and those e-mails contained PII/tax return information of 21 taxpayers.[2]

Based on our sample results, we estimate that for the four-week period of case reviews, SB/SE Division employees sent 95,396 unencrypted e-mails with taxpayer PII/tax return information. We also estimate that these e-mails could contain PII/tax return information of 2,350,071 taxpayers. If this four-week period of time is typical, we estimate that during the year,

[1] The initial population of 23,587 SB/SE Division employees was reduced by 177 employees who, by the nature of their job title, had a limited likelihood of contact with taxpayer-protected information.
[2] Eight employees sent unencrypted e-mails containing taxpayer-protected information internally within the IRS and externally from the IRS.

SB/SE Division employees sent 1,144,749 unencrypted e-mails that contained PII/tax return information of 28,200,857 taxpayers.[3] We could not reliably project estimates separately for internal and external e-mails. However, the majority of these unencrypted e-mails (275 of the 326) were sent internally to other IRS employees, which poses less risk of improper disclosure or improper access than those that were sent externally.

To project the results of our statistical sample, we used a 95 percent confidence level, 49 percent error rate, and an 11 percent precision factor. The jackknife estimate projection is based on a two-sided confidence interval.[4] We are 95 percent confident that the number of:

- Unencrypted e-mails sent for four weeks is between 51,239 and 139,553, and between 614,867 and 1,674,631 for the year.
- Taxpayers' PII/tax return information in the unencrypted e-mails for four weeks is between 8,031 and 5,950,157, and between 96,372 and 71,401,886 for the year.

[3] To make this calculation, we assumed a year contained an average of 48 workweeks to account for holidays and leave.

[4] Jackknife estimation is a general technique for estimating the bias and variance of any point estimate using resampling. Jackknife estimation computes many values of the point estimate by systematically leaving out one observation at a time and calculating the estimate from the remaining values.

Appendix V

Management's Response to the Draft Report

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

COMMISSIONER
SMALL BUSINESS/SELF-EMPLOYED DIVISION

SEP 07 2016

MEMORANDUM FOR MICHAEL E. McKENNEY
DEPUTY INSPECTOR GENERAL FOR AUDIT

FROM: Karen Schiller
Commissioner, Small Business/Self-Employed Division

SUBJECT: Draft Audit Report – Employees Sometimes Did Not Adhere to E-mail Policies Which Increased the Risk of Improper Disclosure of Taxpayer Information (Audit # 201530035)

Thank you for the opportunity to respond to the above referenced draft audit report. Ensuring the privacy and security of taxpayer information is a top priority for the IRS and a fundamental component of maintaining the public trust in the tax system and promoting voluntary compliance. As TIGTA noted in a report published last year (2015-20-079), among the most basic of taxpayers' and employees' rights is an expectation that the IRS will protect the confidentiality of personal, financial, and employment information. And, in that same report, TIGTA noted that the IRS takes the protection of taxpayer privacy very seriously.

While the title of this draft report refers to a risk of improper disclosure, it is important to note that your review did not identify any instances where Personally Identifiable Information (PII) that was sent unencrypted was sent to an unintended recipient. In your review of the emails of eighty IRS employees, you found a small number of emails containing PII which were not properly encrypted, but the majority of these emails were sent within the IRS firewall (from IRS employees to other IRS employees with a need-to-know the information). These communications, are within the extensive protections of the IRS firewall, and pose a minimal risk of disclosure or access. But, nonetheless, we agree that encryption provides an added layer of protection. Also, as TIGTA further notes, on the whole, the data in the emails TIGTA reviewed went to the proper recipient, and external issues were minimal, in that those that were sent externally were generally directed to the appropriate recipients (taxpayers and their representatives).

We appreciate your review of this topic, and welcome your recommendations for ways to further fortify our privacy and security protections in the electronic communications sphere. We are continuously looking for ways to appropriately balance the need to enable our workforce to communicate with each other and with taxpayers electronically, our taxpayers' expectations for more robust electronic communications, and the

overriding need to ensure that those communications are secure and guarded from external threats.

To that end, we have implemented some significant enterprise data protection initiatives. In addition to providing comprehensive instructions to staff, through the Internal Revenue Manual (IRM), we have established performance expectations to protect taxpayer information as outlined in our critical job elements from which managers monitor and annually evaluate employees. We support these added layers of protection by providing employees with guidance alerts and training, including mandatory briefings. This year, we issued two Interim Guidance memorandums and updated our mandatory briefings to include additional guidance regarding e-mail use and privacy protection.

In addition to our standard secure technology, we provide other tools to protect data including secure zip and messaging. In May 2015, the IRS deployed Safeguarding Personally Identifiable Information Data Extracts Data Loss Prevention (SPIIDE DLP) – a tool which blocks unencrypted email containing SSNs from exiting the IRS network. When an email is blocked, the manager of the employee sending the email is notified for follow up. TIGTA recognized the success of SPIIDE DLP in the audit report, when data showed the tool worked as expected by successfully blocking the transmission of an unencrypted e-mail message from being sent outside of the IRS Network.

TIGTA's review of email policies and practice provides us a good sense of where these comprehensive tools and procedures can be strengthened or expanded, and how to improve upon controls we already have in place. We are generally in agreement with the recommendations and have already taken steps to implement some of the corrective actions, and we are looking at additional steps that can be taken to solidify and strengthen this framework.

Attached is a detailed response outlining our corrective actions to address the recommendations. If you have any questions, please contact me, or a member of your staff may contact Bobby Hunt, Director, Operations Support at (240) 613-5163.

Attachment

Attachment

The Deputy Commissioners for Operations Support and Services and Enforcement should:

RECOMMENDATION 1:
Determine the feasibility of implementing a systemic solution to help ensure e-mails with PII/tax return information are encrypted. Until such a solution is identified, consider requiring the default Microsoft Outlook setting to encrypt e-mail messages for compliance and enforcement employees who routinely send taxpayer information by e-mail and other employees who routinely send employee PII/tax return information, *e.g.*, human resource personnel.

CORRECTIVE ACTIONS:
We agree with this recommendation.
1. SB/SE will work with IT to determine the feasibility of implementing a systematic solution and next steps needed.
2. In the interim, the IRS will work to identify positions that routinely send taxpayer information by email and issue interim guidance on implementing default Microsoft Outlook encryption.

IMPLEMENTATION DATES:
1. November 15, 2017
2. January 15, 2017

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

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

RECOMMENDATION 2:
Provide additional training and issue a memorandum to remind employees that all internal and external e-mail with taxpayer PII/tax return information must be encrypted and include that:
- External e-mail with taxpayers' PII/tax return information requires written approval from the IT function Office of Cybersecurity.
- Employees sending their own PII, which is not related to their official duties, must encrypt the document containing the PII.

CORRECTIVE ACTIONS:
We agree with this recommendation. Privacy, Governmental Liaison and Disclosure (PGLD) division issued IG memorandums within the last year that address the use of email.

1. Issued in June of 2016, the IG PGLD-10-0616-0003, *Using IRS and Personal Email Accounts,* addresses email with taxpayers and the fact that no PII may be shared with taxpayers via email (the exception being an IT approved secure email program such as used in Large Business &International Division). A message was sent to all IRS employees on June 22, 2016 advising of the issuance.
2. Issued in June of 2015 and then incorporated into IRM 10.5.1 (revision date 6/15/16), the IG titled *Interim Guidance on Sending Sensitive But Unclassified Information and/or Work-Related Documents to External Email Addresses* addressed employees sending their own PII to an external email address. In combination with the beginning of the SPIIDE program, service-wide 7114 meetings were held to go over the content in the IG. The briefings also covered the requirements to encrypt emails that contain PII/SBU information and provided specific instructions for doing so.
3. Additional guidance has been provided in mandatory security awareness training.

IMPLEMENTATION DATES:
1. Implemented
2. Implemented
3. Implemented

RESPONSIBLE OFFICIALS:
1. Director, PGLD (Director, Privacy Policy and Compliance (PPC))
2. Director, PGLD (Director, PPC)
3. Director, Technology Solutions, SB/SE

CORRECTIVE ACTION MONITORING PLAN:
N/A

RECOMMENDATION 3:
Ensure that managers are aware of the violations for sending unencrypted e-mails with taxpayer PII/tax return information and that they take appropriate disciplinary action when violations occur.

CORRECTIVE ACTIONS:
We agree with this recommendation.

1. PGLD will develop a Manager's Tool Kit that will include a reference to the Penalty Guide and how it applies to situations where employees fail to encrypt emails.
2. SB/SE will begin notifying managers and their executives of incidents in which the SPIIDE DLP tool detects repeated unencrypted submission attempts by the same employee.
3. The SB/SE Commissioner will prepare an all manager email to stress the importance of managerial awareness of SPIIDE DLP.

IMPLEMENTATION DATES:

1. November 15, 2016
2. January 15, 2017
3. January 15, 2017

RESPONSIBLE OFFICIALS:

1. Director, PGLD (Director, PPC)
2. Director, Technology Solutions, SB/SE
3. Director, Technology Solutions, SB/SE

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

RECOMMENDATION 4:
The Chief Technology Officer should update the *Standards for Using Email* IRM to include that no officer or employee of the IRS may use a personal e-mail account to conduct any official business of the Government. Additionally, provide training and issue a memorandum to instruct employees that they cannot send any work-related e-mails to their personal e-mail accounts.

CORRECTIVE ACTION:
We agree with this recommendation.

1. We will update IRM 1.10.3, *Standards for Using Email*, to include a statement that no officer or employee of the IRS may use a personal email account to conduct any official business of the government.
2. Interim Guidance memorandum PGLD-10-0616-0003 was issued on June 21, 2016, and states that employees must always use their IRS email accounts when using email to conduct the official business of the IRS.
3. Two mandatory briefing courses, Records Management Awareness and Privacy Information Protection & Disclosure, provided training on the prohibition of using

personal email accounts to conduct official Government business. These briefings were required of all employees in Fiscal Year 2016.

IMPLEMENTATION DATE:
1. November 15, 2016
2. Implemented
3. Implemented

RESPONSIBLE OFFICIAL(S):
1. Chief, Communications and Liaison, (C&L)
2. Director, PGLD (Director, PPC)
3. Director, PGLD (Director, PPC)

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

RECOMMENDATION 5:
The Chief Technology Officer should update the Enterprise Electronic Fax (EEFax) system to allow encrypted messages to be sent to the EEFax server.

CORRECTIVE ACTION:
We will determine if it is feasible to upgrade the EEFax system given the known issues of unknown cost, level of effort, training and certificate management. Such an upgrade would ensure that all outbound EEFax encrypted email traffic containing PII information is protected within the IRS email infrastructure until the EEFax server converts the encrypted email to an industry standard format and transmitted over a standard unencrypted analog phone line to a taxpayer provided facsimile number. If we determine it to be feasible, we will implement programming changes to accomplish this objective subject to budgetary constraints, limited resources, and competing priorities.

IMPLEMENTATION DATE:
October 15, 2020

RESPONSIBLE OFFICIAL:
Director, Unified Communications/UNS; Information Technology (IT)

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