



*Additional Security Is Needed for the  
Taxpayer Secure Email Program*

**February 4, 2011**

**Reference Number: 2011-20-012**

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

Redaction Legend:

1 = Tax Return/Return Information

---

*Phone Number* | 202-622-6500

*Email Address* | [TIGTACommunications@tigta.treas.gov](mailto:TIGTACommunications@tigta.treas.gov)

*Web Site* | <http://www.tigta.gov>



## HIGHLIGHTS

### **ADDITIONAL SECURITY IS NEEDED FOR THE TAXPAYER SECURE EMAIL PROGRAM**

## Highlights

### **Final Report issued on February 4, 2011**

Highlights of Reference Number: 2011-20-012 to the Internal Revenue Service Chief Technology Officer; Commissioner for Large Business and International Division; Chief of the Office of Appeals; and Director of the Office of Privacy, Information Protection and Data Security.

### **IMPACT ON TAXPAYERS**

Internal Revenue Service (IRS) employees and taxpayers are required to work together to ensure the security of taxpayers' sensitive data transmitted in email messages. If employees and taxpayers do not follow the required security policies, the risks to taxpayers' sensitive data are increased. The data could be intercepted and accessed by unauthorized individuals or inadvertently sent to the wrong recipient.

### **WHY TIGTA DID THE AUDIT**

This audit was initiated because the IRS relaxed its long-standing internal policy prohibiting employees from transmitting Sensitive But Unclassified (SBU) data to taxpayers in emails. The objective of the review was to determine whether IRS controls, policies, and procedures for sensitive email messages to taxpayers adequately protected taxpayers' data, guarded against email threats to the IRS network, and ensured email practices were compliant with Federal regulations.

### **WHAT TIGTA FOUND**

Although some controls for the Secure Email With Taxpayers program are in place, such as the installation of antivirus software on employees' computers, other security controls were not implemented. The IRS has not implemented an automated control to detect and prevent SBU data in unencrypted emails from being transmitted outside the IRS. In addition, some employees and taxpayers are not

encrypting their emails that contain SBU data. These violations of the program were not reported to IRS management. Furthermore, IRS procedures and training lacks adequate guidance for employees to report the violations. In addition, the IRS does not timely correct persistent medium-risk security vulnerabilities detected on email servers.

### **WHAT TIGTA RECOMMENDED**

TIGTA recommended that the Large Business and International Division and Office of Appeals coordinate with the Office of Privacy, Information Protection, and Data Security to develop additional procedures for employees participating in the Secure Email With Taxpayers program to address how, when, and to whom employee and taxpayer secure email violations should be reported; update guides and training materials to include these procedures; amend the Memorandum of Understanding to apprise the taxpayer of the specific risks associated with transmitting unencrypted email with SBU data; and issue a memorandum to all employees advising them of the disciplinary actions that will be taken against employees who violate IRS email policies by sending unencrypted emails to taxpayers who have not signed a Memorandum of Understanding to participate in the program.

TIGTA also recommended that the Associate Chief Information Officer, Cybersecurity, ensure data leakage prevention software is implemented by April 2012, and update the annual Information Systems Security briefing to include the new Secure Email With Taxpayers procedures. Lastly, TIGTA recommended the Associate Chief Information Officer, Enterprise Operations, ensure medium-risk vulnerabilities detected on email servers are appropriately tracked and, if the vulnerabilities cannot be corrected within two months, follow security requirements to post the vulnerabilities to the appropriate Plan of Actions and Milestones.

In their response to the report, IRS officials agreed with six of the recommendations and partially agreed with three. For the three partially agreed recommendations, TIGTA continues to believe that the IRS should fully implement the recommendations.



TREASURY INSPECTOR GENERAL  
FOR TAX ADMINISTRATION

DEPARTMENT OF THE TREASURY  
WASHINGTON, D.C. 20220

February 4, 2011

**MEMORANDUM FOR** CHIEF TECHNOLOGY OFFICER  
COMMISSIONER, LARGE BUSINESS AND INTERNATIONAL  
DIVISION  
CHIEF, OFFICE OF APPEALS  
DIRECTOR, OFFICE OF PRIVACY, INFORMATION  
PROTECTION AND DATA SECURITY

*Michael R. Phillips*

**FROM:**

Michael R. Phillips  
Deputy Inspector General for Audit

**SUBJECT:**

Final Audit Report – Additional Security Is Needed for the Taxpayer  
Secure Email Program (Audit # 201020021)

This report presents the results of our review to determine whether Internal Revenue Service (IRS) controls, policies, and procedures for sensitive email messages to taxpayers adequately protected taxpayers' data, guarded against email threats to the IRS network, and ensured email practices were compliant with Federal regulations. This audit was included in the Treasury Inspector General for Tax Administration Fiscal Year 2010 Annual Audit Plan and was part of our statutory requirement to annually review the adequacy and security of IRS technology.

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

Copies of this report are also being sent to the IRS managers affected by the report recommendations. Please contact me at (202) 622-6510 if you have questions or Alan R. Duncan, Assistant Inspector General for Audit (Security and Information Technology Services), at (202) 622-5894.



*Additional Security Is Needed  
for the Taxpayer Secure Email Program*

*Table of Contents*

**Background** .....Page 1

**Results of Review** .....Page 3

    Some Controls Have Been Implemented to Mitigate the  
    Risks of the Secure Email With Taxpayers Program.....Page 3

    An Automated Control to Detect Sensitive But Unclassified  
    Data in Unencrypted Emails Transmitted Outside the  
    Internal Revenue Service Has Not Been Implemented.....Page 4

Recommendation 1:.....Page 5

    Additional Procedures and Training to Protect Taxpayers’  
    Sensitive Data Transmitted in Emails Should Be Developed  
    and Implemented.....Page 5

Recommendations 2 and 3: .....Page 8

Recommendations 4 and 5: .....Page 9

Recommendations 6 and 7: .....Page 10

    Medium-Risk Vulnerabilities on Email Servers Are Not  
    Timely Corrected .....Page 10

Recommendation 8:.....Page 12

    Some Unauthorized Employees Are Sending and Receiving  
    Sensitive Data in Emails .....Page 12

Recommendation 9:.....Page 13

**Appendices**

    Appendix I – Detailed Objective, Scope, and Methodology .....Page 15

    Appendix II – Major Contributors to This Report.....Page 19

    Appendix III – Report Distribution List .....Page 20

    Appendix IV – Management’s Response to the Draft Report .....Page 21



*Additional Security Is Needed  
for the Taxpayer Secure Email Program*

---

*Abbreviations*

EOPS	Enterprise Operations
IRS	Internal Revenue Service
LB&I	Large Business and International Division
MOU	Memorandum of Understanding
NIST	National Institute for Standards and Technology
SBU	Sensitive But Unclassified



## *Additional Security Is Needed for the Taxpayer Secure Email Program*

---

### *Background*

Electronic mail (email) presents one of the highest security risks to an organization's sensitive data and computer network. For example, most computer viruses are spread through email attachments and emails with links to malicious web sites. Computer viruses can destroy data on computers, disrupt computer operations, and degrade network performance. In addition, sensitive data transmitted in emails could be intercepted by unauthorized individuals or inadvertently sent to the wrong recipient.

The Internal Revenue Service (IRS) relies on email to communicate within the organization. Most managers and employees have access to email and can send sensitive data to other employees using the Secure Enterprise Messaging System.<sup>1</sup> The most common type of sensitive information processed by the IRS is Sensitive But Unclassified (SBU) information, which includes taxpayers' tax and financial data as well as Personally Identifiable Information.

To protect taxpayers' sensitive data transmitted in email messages, IRS procedures require the email system provide appropriate security to the network where the system resides and to the data stored and transmitted by the email system in accordance with the standards and guidelines developed by the National Institute for Standards and Technology (NIST).<sup>2</sup> The NIST recommends agencies implement automated tools, such as a network data leakage prevention tool, to monitor transfers of Personally Identifiable Information, and to monitor inbound and outbound communications for unauthorized activities.

Prior to November 2007, the IRS maintained a long-standing policy that prohibited sending SBU data in emails to taxpayers or a taxpayer's representative, such as a Power of Attorney. IRS procedures directed employees to not send SBU data by email to parties outside of the IRS or the Department of the Treasury, even if the other party uses encryption software. The IRS cited the risks to taxpayers' privacy as the reason for its policy.

The IRS relaxed its email policy in November 2007 when its Security Services and Privacy Executive Steering Committee approved the Large Business and International (LB&I) Division to begin a Secure Email With Taxpayers pilot. This pilot began with 12 volunteer corporate taxpayers and ended in September 2008 with 35 corporate taxpayers.

In October 2008, the Security Services and Privacy Executive Steering Committee approved the LB&I Division's request to incorporate the Secure Email With Taxpayers pilot in its standard

---

<sup>1</sup> The Secure Enterprise Messaging System allows users to digitally encrypt email messages and attachments that contain Sensitive But Unclassified data.

<sup>2</sup> NIST Special Publication 800-45, *Guidelines on Electronic Mail Security*, February 2007, and NIST 800-122, *Guide to Protecting the Confidentiality of Personally Identifiable Information*, April 2010.



---

*Additional Security Is Needed  
for the Taxpayer Secure Email Program*

---

operating procedures. During our review, over 200 taxpayers were enrolled in the LB&I Division's Secure Email With Taxpayers program.

In February 2009, the IRS changed its official internal policy on transmitting SBU data by email to taxpayers. The policy was revised as follows:

*“IRS employees may never send SBU data by electronic mail to taxpayers or their representatives unless they are using a technology and methodology that has been approved by the Security Services and Privacy Executive Steering Committee and the Senior Executive Team.”*

The Security Services and Privacy Executive Steering Committee also approved the IRS Office of Appeals to begin a Secure Email With Taxpayers pilot in June 2009. The pilot is limited to only the employees in the Appeals Team Case Leader groups that process large dollar taxpayer cases routed from the LB&I Division. The Office of Appeals employees and the employees in the LB&I Division usually communicate with the same taxpayers. The technology, processes, and procedures for the Office of Appeals pilot emulate what was developed and implemented by the LB&I Division.

The Security Services and Privacy Executive Steering Committee has no plans to allow other IRS business units to transmit emails with SBU data to taxpayers and emphasized the Office of Appeals' participation is still in the pilot phase. In addition, the Committee considers the Secure Email With Taxpayers program to be a “limited” program because only the LB&I Division and the Office of Appeals are authorized to participate and, within these business units, only some employees are authorized to participate. In this report, we use Secure Email With Taxpayers program to refer to the LB&I Division's program and the Office of Appeals' pilot.

We focused this review on the technical and manual controls that the IRS implemented to protect taxpayers' data, guard against email threats to the IRS computer network, and ensure email practices are compliant with Federal regulations and IRS policies. This review was performed at the offices of the LB&I Division and the Office of Appeals in Washington, D.C., and Dallas, Texas, and at the Modernization and Information Technology Services organization's Office of Cybersecurity, Computer Security Incident Response Center, End User Equipment and Services office, and Enterprise Operations office in New Carrollton, Maryland. We also performed work in the Enterprise Operations office in Austin, Texas. We performed this review during the period January through July 2010. 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.



---

*Additional Security Is Needed  
for the Taxpayer Secure Email Program*

---

*Results of Review*

***Some Controls Have Been Implemented to Mitigate the Risks of the Secure Email With Taxpayers Program***

The Secure Email With Taxpayer program represents a departure from the traditional means of communicating with taxpayers, such as regular mail and telephone contact. With advances in supporting technologies and the increased use of email by taxpayers to conduct business, we acknowledge this program will enhance customer service with taxpayers and provide a more expedient and efficient way to trade information. During our review, over 200 corporate taxpayers were enrolled in the LB&I Division's Secure Email With Taxpayers program.

In order to participate in the Secure Email With Taxpayers program, the IRS requires taxpayers to sign a Memorandum of Understanding (MOU) agreeing to work together to ensure the joint security of the data transmitted in emails. The MOU is an important control that has been implemented for the Secure Email With Taxpayers program because it sets up the parameters for the program as well as the responsibilities for both parties. For example, the MOU states,

*“It is the intention of both parties to this MOU that encrypted emails be used for the transmission of sensitive or confidential tax-related information...”*

Encryption provides the technological protection of the email and all data files attached to the emails while being transmitted by either party. The taxpayer is required to have a compatible secure email system with encryption capability to participate in the program.

Another important aspect of the MOU is the identification of authorized individuals allowed to send and receive emails under this program. The specific names of IRS employees authorized to send and receive emails are required to be listed in an attachment to the MOU. Once the MOU is signed by both parties, only listed individuals are authorized to participate in the Secure Email With Taxpayers program. Allowing only the specific individuals to send and receive emails ensures that the confidentiality of data are maintained, especially since some taxpayers participating in this program are large and mid-sized businesses and are being represented by attorneys, accountants, and administrative personnel. In addition, the IRS has effective controls to remove employees' email accounts from the email system when an employee separates from the IRS.

We also found that the LB&I Division and Office of Appeals provided guides on secure communication to their employees with instructions on how to exchange digital signature certificates between the IRS and taxpayers' email systems. These step-by-step guides explain how to securely communicate using email and caution employees not to type sensitive



---

*Additional Security Is Needed  
for the Taxpayer Secure Email Program*

---

information in the subject line of the email or in the name of a file attachment because these parts are not encrypted.

Lastly, we found that antivirus software is installed and operating properly on 98 percent of the IRS's computer workstations. This security software was installed long before the Secure Email With Taxpayers program was initiated and is critical because the workstation is the last line of defense in detecting and removing viruses.

Although the IRS implemented some controls, additional actions are needed to protect taxpayers' sensitive data and the IRS computer network.

***An Automated Control to Detect Sensitive But Unclassified Data in Unencrypted Emails Transmitted Outside the Internal Revenue Service Has Not Been Implemented***

As previously stated in this report, the IRS must implement automated controls, such as a data leakage prevention tool, to detect and prevent SBU data from inappropriately leaking from the IRS, including sensitive data transmitted in emails.

The IRS is currently acquiring an enterprise data leakage prevention system. This key control was not implemented prior to approving the LB&I Division's Secure Email With Taxpayers pilot because the IRS, along with the Department of the Treasury, determined the data loss prevention solutions in the marketplace at that time were not mature or robust enough to address the IRS's needs. The Co-Chairman of the Security Services and Privacy Executive Steering Committee also cited the following reasons for approving the program without a data loss prevention system in place.

- The MOU signed by the taxpayer affords a sufficient level of protection. The taxpayer accepts the risks when signing the MOU.
- The taxpayers involved in the Secure Email With Taxpayers program are business professionals and have email systems capable of encrypting the emails.

The IRS now believes the enterprise-level data leakage prevention solutions currently available for purchase have the capability of working with security software already in place and can handle the large amount of electronic information generated by a large organization. The IRS is in the early stages of the acquisition and expects to have a data leakage prevention control fully implemented by April 2012, which would be 4 years after the LB&I Division Secure Email With Taxpayers pilot was approved.

Without an automated control to identify and prevent unencrypted emails with sensitive data from leaving the IRS, sensitive data could be exposed to unauthorized access and disclosure. Until the data leakage prevention solution is fully implemented, the IRS must rely solely on the effectiveness of manual controls. For example, the IRS must have effective procedures and



---

*Additional Security Is Needed  
for the Taxpayer Secure Email Program*

---

training to ensure employees follow the security policies and report violations of the program to ensure sensitive data are adequately protected.

### ***Recommendation***

**Recommendation 1:** The Associate Chief Information Officer, Cybersecurity, should continue with the acquisition of a data leakage prevention system to ensure full deployment by April 2012. This data leakage prevention system should include the ability to identify and stop unencrypted emails containing sensitive data, such as Social Security Numbers, from leaving the IRS domain.

**Management's Response:** The IRS agreed with this recommendation. The IRS stated that it would deploy a data leakage prevention solution through the Safeguarding Personally Identifiable Information Data Extracts project. The Safeguarding Personally Identifiable Information Data Extracts project will implement Data-In-Motion components to address this issue. In addition, the project will also coordinate the deployment of Incident Response workflows with respective organizations including the Office of Privacy, Information Protection and Data Security. The final scope for policy, rules, and corrective actions will be determined with input from the Treasury Inspector General for Tax Administration and other stakeholders. The IRS set an implementation date of July 1, 2012.

### ***Additional Procedures and Training to Protect Taxpayers' Sensitive Data Transmitted in Emails Should Be Developed and Implemented***

The Department of the Treasury<sup>3</sup> requires its bureaus to develop formal, documented procedures to monitor and control email. These manual procedures are needed to mitigate the security risks of the Secure Email With Taxpayers program and are critical in light of the previous finding. The IRS must develop and implement procedures and training for employees to identify and report violations of the program. Examples of Secure Email violations include employees, taxpayers, or taxpayers' representatives transmitting unencrypted emails with SBU data or unauthorized employees or taxpayers participating in the program. As previously stated, the requirement for the taxpayer and the IRS to sign an MOU is one of the most significant manual controls established to date.

To evaluate program compliance, we selected 97 of the 582 program employees and reviewed emails that were sent or received. We found some employees authorized<sup>4</sup> to participate in the

---

<sup>3</sup> Treasury Directive Publication 85-01, *Treasury Information Technology Security Program*, November 3, 2006.

<sup>4</sup> Employees are authorized to participate in this program when the employee's name is listed on an attachment to the MOU and the MOU is signed by the taxpayer.



*Additional Security Is Needed  
for the Taxpayer Secure Email Program*

Secure Email With Taxpayers program were not encrypting some of their emails that contained SBU data.

- Nine (9 percent) of the 97 authorized employees sent a total of 20 unencrypted emails containing SBU data to 9 taxpayers. An MOU was not in place for three of the taxpayers, which indicates the employee was not authorized to send SBU data to these taxpayers.

\*\*\*\*\*1\*\*\*\*\*  
 \*\*\*\*\*  
 \*\*\*\*\*  
 \*\*\*\*\*

We also found employees authorized to participate in the Secure Email With Taxpayers program were receiving unencrypted emails that contained SBU data.

- Thirty-five (36 percent) of the 97 authorized employees received 128 unencrypted emails with SBU data from 38 taxpayers. An MOU had not been executed for 14 of these taxpayers, indicating the employee was not authorized to receive SBU emails from these taxpayers.

\*\*\*\*\*1\*\*\*\*\*  
 \*\*\*\*\*  
 \*\*\*\*\*

We did not contact the taxpayers to determine why they did not encrypt their emails or sign an MOU with the IRS. However, officials in the LB&I Division and the Office of Appeals informed us that some taxpayers and their representatives have been sending SBU data in emails long before the Secure Email With Taxpayers program started. The IRS officials also stated they were unaware of procedures requiring them to stop or report taxpayers who send emails with SBU data to IRS employees.

These violations of the program were not reported to the LB&I Division or the Office of Appeals Team Managers or Team Coordinators or to the Modernization and Information Technology Services organization’s Computer Security Incident Response Center. Furthermore, none of the 22 LB&I Division or Office of Appeals Team Managers or Team Coordinators that we interviewed were aware of any reported violations of the Secure Email With Taxpayers program. These IRS officials informed us they did not receive procedures requiring them to report secure email violations of the type we found in our review.

Other IRS officials in the National Headquarters Office informed us that the IRS is not responsible for reporting or stopping taxpayers from sending unencrypted SBU data in emails. They believe the IRS is responsible only after receiving the data, and that taxpayers are fully aware of the risks because, while not explicit in the MOU, the risks are discussed with each taxpayer prior to signing the MOU. However, we disagree with this rationale. If taxpayers’



*Additional Security Is Needed  
for the Taxpayer Secure Email Program*

sensitive data are lost or stolen as a result of the Secure Email With Taxpayers program, we believe the brunt of the criticism and negative publicity would be directed at the IRS. Second, and more importantly, of the above 38 taxpayers that sent unencrypted email to IRS employees, 8 (21 percent) were not the actual taxpayer; they were the taxpayers' representative such as a Power of Attorney or Public Accountant. In these instances, the taxpayers are most likely unaware their sensitive data were transmitted insecurely. The IRS should take all reasonable actions to ensure the taxpayers' data are protected, including responding to an unencrypted email with SBU data reminding the taxpayer to encrypt the email and requesting that taxpayers who receive unencrypted emails with SBU data from IRS employees report this violation to a designated IRS official. These actions would provide accountability for program compliance and ensure the security of the program is maintained.

The IRS's internal procedures, guides, and training briefings do not provide adequate guidance or instructions to employees to report violations of unencrypted emails with SBU data from employees or taxpayers. We found the procedures require employees to report inadvertent disclosures of sensitive information to the Computer Security Incident Response Center using that office's online Security Incident Reporting form. However, the form instructs employees to report emails sent to the wrong party. None of the above email violations that we found were sent to the wrong party. Furthermore, the Security Incident Reporting form instructs employees to use the Wage and Investment Division's Erroneous Taxpayer Correspondence Reporting form to report emails sent to the wrong party, as does the Office of Privacy, Information Protection and Data Security web site. The Erroneous Taxpayer Correspondence Reporting form does not include a category for unencrypted emails with SBU data sent to or received from taxpayers.

We also found the LB&I Division's Secure Communications With Taxpayers guide and Office of Appeals Secure Email Messaging training presentation lack specific procedures for employees to report violations of the Secure Email With Taxpayers program. Lastly, the IRS's two mandatory annual briefings on information security are required for all employees and are prepared by the Office of Privacy, Information Protection and Data Security and by the Office of Cybersecurity. However, the Information Protection and Disclosure briefing prepared by the Office of Privacy provides general guidance and penalties for failing to protect sensitive data, but this briefing and the Office of Cybersecurity's Information System Security briefing do not include procedures for reporting violations of the Secure Email With Taxpayers program.

***Although we did not find evidence of unencrypted emails being intercepted or instances where emails were sent to the wrong recipient, the risk of unauthorized disclosure is increased when employees do not report secure email violations or adhere to the MOU requirements.***

We did not find evidence of unencrypted emails being intercepted by unauthorized individuals, nor were our tests designed to uncover this type of illegal activity. However, the risks to taxpayers' sensitive data are increased when employees do not report secure email violations and



---

*Additional Security Is Needed  
for the Taxpayer Secure Email Program*

---

IRS management does not establish and reinforce clear procedures and training on secure email policies.

## ***Recommendations***

**Recommendation 2:** The LB&I Division and the Office of Appeals should coordinate with the Office of Privacy, Information Protection and Data Security to develop and enforce additional procedures for employees participating in the Secure Email With Taxpayers program. The procedures should address how, when, and to whom employee and taxpayer secure email violations should be reported and that appropriate actions will be taken against employees who do not encrypt sensitive email messages to taxpayers.

**Management's Response:** The IRS partially agreed with this recommendation. The LB&I Division will take the lead and coordinate with the Office of Privacy, Information Protection and Data Security to ensure the IRS's policy on privacy and security incorporates the use of secure email with taxpayers. The LB&I Division will also ensure its web site is consistent with guidance set forth by the Office of Cybersecurity on secure email with taxpayers. In addition, the LB&I Division and the Office of Appeals will advise its employees participating in the Secure Email With Taxpayers program of their responsibilities on how, when, and to whom they should report secure email violations. Lastly, the Office of Appeals will update its web site to link to the appropriate IRS policy on privacy and security for the Secure Email With Taxpayers program.

Within the IRS's response transmittal, the IRS stated its disciplinary procedures are appropriate for addressing email violations without the need for further delineation in the Secure Email procedures.

**Office of Audit Comment:** The IRS's disciplinary procedures state the penalty for an employee who fails to maintain security for Personally Identifiable Information is admonishment up to a 14-day suspension. The penalty for a second offense is a 15-day suspension up to removal from the IRS. The penalty for the third offense is removal from the IRS. We believe these penalties should be delineated, or at least referenced, in the Secure Email procedures and would serve as a warning to employees who do not comply with encrypting email messages to taxpayers.

**Recommendation 3:** The LB&I Division and the Office of Appeals should update guides and training materials to include the new reporting procedures.

**Management's Response:** The IRS agreed with this recommendation. The IRS stated that the Director, Business Systems Planning, LB&I Division, will update IRS training materials and guides to include all current and any new reporting procedures and policies relating to the Secure Email program. In addition, the Office of Appeals will update its web site to link to the approved IRS training materials and guides.



---

*Additional Security Is Needed  
for the Taxpayer Secure Email Program*

---

**Recommendation 4:** The LB&I Division and the Office of Appeals should coordinate to amend the MOU to apprise the taxpayer of the specific risks associated with transmitting unencrypted emails with SBU data and provide specific actions that will be taken when taxpayers or their representatives do not comply with the terms of the MOU. For example, the IRS could potentially terminate the MOU if the taxpayer or taxpayer's representatives repeatedly fail to encrypt sensitive emails. These actions would provide accountability to taxpayers to comply with the MOU.

**Management's Response:** The IRS partially agreed with this recommendation and stated that the Director, Business Systems Planning, LB&I Division, will modify the existing Secure Email With Taxpayers MOU template to make taxpayers fully aware of the security risks if they choose to send unencrypted email. In addition, the LB&I Division and the Office of Appeals will issue the modified MOU to all its participants in the Secure Email program. Within the IRS's response transmittal, the IRS stated it will not amend the MOU to address taxpayers' noncompliance with the MOU.

**Office of Audit Comment:** We disagree with the IRS's decision to not amend the MOU to address taxpayers' noncompliance with the MOU. As stated in the report, many taxpayers are most likely unaware their sensitive information was transmitted insecurely because many of the violations we found were sent by the taxpayers' representatives, such as a Power of Attorney or Public Accountant. The IRS should take all reasonable actions to protect the taxpayers' sensitive data. These actions should include developing procedures and penalties to address taxpayers or taxpayer representatives who do not comply with the security terms of the MOU. The procedures and penalties should be explicitly stated in the MOU.

**Recommendation 5:** The Office of Privacy, Information Protection and Data Security should take actions to update the IRS's official internal procedures with the additional procedures developed by the LB&I Division and the Office of Appeals and post the procedures to its internal web site.

**Management's Response:** The IRS agreed with the recommendation and stated that the corrective actions have already been completed. The IRS stated that in August 2010, the Office of Privacy, Information Protection and Data Security updated its internal web site to reflect current IRS guidance and procedures for sending email containing Personally Identifiable Information within the IRS as well as to authorized non-IRS parties. The IRS also stated that its current guidance indicates the only approved process for sending secure email containing Personally Identifiable Information to taxpayers or their representatives is through the encryption solution utilized in the LB&I Division and the Office of Appeals Secure Email pilots, and only approved pilot participants could use this capability. The Office of Privacy, Information Protection and Data Security will continue to monitor the Secure Email pilots and programs and will update its internal web site, as appropriate, as new procedures are developed.



---

*Additional Security Is Needed  
for the Taxpayer Secure Email Program*

---

**Office of Audit Comment:** Although the IRS agreed with this recommendation, its corrective actions are not sufficient to address the recommendation. As stated in the report, the IRS's current procedures in its Internal Revenue Manual do not provide adequate guidance to employees on reporting violations of unencrypted emails with SBU data. The lack of a data leakage prevention system until July 2012 makes these procedures more critical. The IRS's Internal Revenue Manual is intended to provide the official procedures that employees are required to follow. These internal procedures should be updated with the additional procedures we recommended in Recommendation 2 above. The Internal Revenue Manual procedures should require the employees to report secure email violations and address how, when, and to whom employee and taxpayer secure email violations should be reported.

We reviewed the update to the Office of Privacy's web site that was completed in August 2010 and found the update does not include the additional procedures that we recommended the LB&I Division and the Office of Appeals develop. For example, the web site does not include new procedures regarding how, when, and to whom employee and taxpayer secure email violations should be reported.

**Recommendation 6:** The Office of Privacy, Information Protection and Data Security should update the Annual Information Protection and Disclosure Briefing to include the new Secure Email With Taxpayers procedures.

**Management's Response:** The IRS agreed with this recommendation. The IRS stated that the Office of Privacy, Information Protection and Data Security, will update the Annual Information Protection and Disclosure Briefing to indicate Secure Email With Taxpayers can occur only under agency/Modernization and Information Technology Services approved pilots and programs.

**Recommendation 7:** The Associate Chief Information Officer, Cybersecurity, should update the mandatory annual Information Systems Security briefing to include or reference the new Secure Email With Taxpayers procedures.

**Management's Response:** The IRS agreed with this recommendation. The Associate Chief Information Officer, Cybersecurity, will update the Information Systems Security supplemental briefing to include or reference the Secure Email With Taxpayers procedures. This supplemental briefing is a part of the mandatory security awareness training provided to all IRS employees annually.

### **Medium-Risk Vulnerabilities on Email Servers Are Not Timely Corrected**

The Modernization and Information Technology Services organization's Enterprise Operations office conducts monthly security assessments of its 70 email servers using the Windows Policy



---

*Additional Security Is Needed  
for the Taxpayer Secure Email Program*

---

Checker tool.<sup>5</sup> The monthly assessments conducted from September 2009 through February 2010 determined that each of the email servers failed between 73 and 79 medium-risk security checks each month. The number of failed security checks on each server was the same each month, indicating the same security vulnerabilities exist on the same servers each month and are not being timely corrected. Examples of the vulnerabilities that were not addressed include:

- The setting to prevent anonymous connections to the email server was not configured in compliance with IRS procedures. IRS procedures require the anonymous connection setting be configured to the default value “Null” to prevent the server from being accessed by any network user. This weakness could lead to exposure or corruption of sensitive corporate data.
- The settings to restrict access permissions to files, directories, and registry settings on the email servers were not configured to prevent unauthorized individuals from exploiting the email servers.
- The settings for passwords and audit logs were not configured to prevent or detect malicious activities. The audit logs were set to overwrite, and thereby delete, critical events that should be retained and reviewed in the logs. Registry settings for password length and expiration were incorrectly set for local user accounts on the email servers.

IRS policies require security weaknesses for medium-risk systems, such as the IRS’s email system, be posted on a Plan of Actions and Milestones<sup>6</sup> within 2 months of identification if the weakness cannot be fixed within 60 days. This action ensures the weaknesses receive adequate management oversight until corrected or until mitigating controls are implemented. However, the persistent medium-risk weaknesses that the IRS detected on its email servers were not posted to a Plan of Actions and Milestones because the IRS does not track these vulnerabilities to identify recurring weaknesses from month to month.

The Enterprise Operations office attributed the recurring security vulnerabilities on the email servers to system administrators focusing on other operational support responsibilities, including the daily maintenance and backup of the email system. The Enterprise Operations office also reported their office focused on correcting high-risk vulnerabilities, maintaining the IRS’s enterprise email infrastructure, and planning the implementation of the IRS’s new Secure Enterprise Messaging System. This focus diverted resources from correcting vulnerabilities found on the current email servers.

---

<sup>5</sup> An automated tool used to determine whether systems are adhering to security policies.

<sup>6</sup> The purpose of a Plan of Actions and Milestones is to assist agencies in identifying, assessing, prioritizing, and monitoring the progress of corrective efforts for security weaknesses found in programs and systems.



---

*Additional Security Is Needed  
for the Taxpayer Secure Email Program*

---

## **Recommendation**

**Recommendation 8:** To ensure persistent medium-risk vulnerabilities receive management oversight and timely corrective actions, the Associate Chief Information Officer, Enterprise Operations, should ensure the vulnerabilities detected on each email server during the monthly security assessments are appropriately tracked. If persistent medium-risk vulnerabilities cannot be corrected within 2 months, the Enterprise Operations office should follow IRS security requirements to post the vulnerabilities to the appropriate Plan of Actions and Milestones.

**Management's Response:** The IRS agreed with this recommendation and stated that the Associate Chief Information Officer, Enterprise Operations, will initiate tracking and correction of medium-risk vulnerabilities. A process will be implemented to ensure all medium-risk vulnerabilities that cannot be corrected within 60 days and high-risk vulnerabilities that cannot be corrected within 30 days of detection will be documented within a Plan of Actions and Milestones.

## **Some Unauthorized Employees Are Sending and Receiving Sensitive Data in Emails**

As previously stated in this report, the MOU provides the management control that only authorized employees, taxpayers, and taxpayers' representatives are sending and receiving emails under the Secure Email With Taxpayers program. To ensure this control's effectiveness, both the IRS and the taxpayer must be diligent in updating the list of authorized individuals who may conduct business for both the IRS and the taxpayer. The confidentiality of sensitive data is maintained when the email senders and recipients are known and authorized to send and receive emails.

To determine whether only authorized individuals are participating in the Secure Email With Taxpayers program, we selected a sample of 70 employees from the LB&I Division and the Office of Appeals who have not been authorized to participate in the program<sup>7</sup> and reviewed their historical emails. We found some of these employees are sending and receiving unencrypted emails to and from taxpayers or their representatives, most of whom are also not authorized to participate in the program.

- Seven (10 percent) of the 70 unauthorized employees in our sample sent a total of 21 unencrypted emails containing SBU data to 14 taxpayers. An MOU had not been executed for the 14 taxpayers.

---

<sup>7</sup> Employees are not authorized to participate in this program if there is no signed MOU on file or if the attachment to the signed MOU does not list their names as participants of the program.



*Additional Security Is Needed  
for the Taxpayer Secure Email Program*

As an example, we found one employee sent a total of eight unencrypted emails containing SBU data to four different taxpayers.

- Twenty-two (31 percent) of the 70 unauthorized employees received a total of 104 unencrypted emails containing SBU data from 64 taxpayers. An MOU was not in place for 58 of these taxpayers.

As examples, \*\*\*\*\*1\*\*\*\*\*  
\*\*\*\*\*1\*\*\*\*\*  
\*\*\*\*\*1\*\*\*\*\* Another employee received a total of 19 unencrypted emails with SBU data from 5 different taxpayers.

The employees above were not included in any MOU and violated the IRS policy that prohibits sending emails with SBU data unless participating in the Secure Email With Taxpayers program. We believe that many of these employees knowingly disregarded the Secure Email With Taxpayers program and do not fully understand the risk of unnecessarily exposing the release of taxpayer data. Without a systemic monitoring solution to prevent unencrypted emails from leaving the IRS (i.e., a data loss prevention solution cited in the previous finding), the IRS cannot stop these types of emails from occurring other than by relying on employee compliance.

The credibility and purpose of the program are undermined when non-participating employees send and receive unencrypted emails from taxpayers. The number of employees and taxpayers sending and receiving SBU emails without signing an MOU indicates that the most significant management control that the IRS has implemented is not effective at ensuring only authorized individuals are sending SBU emails to taxpayers. When unauthorized employees send and receive emails with SBU data to and from taxpayers, the risk of unauthorized disclosure of taxpayer data is increased.

**Recommendation**

**Recommendation 9:** The LB&I Division and the Office of Appeals should issue a memorandum to their employees reminding them of the Secure Email With Taxpayers policy and the actions that will be taken against unauthorized employees who violate the policy by sending or receiving emails with SBU data to or from taxpayers.

**Management's Response:** The IRS partially agreed with this recommendation. The IRS stated that the LB&I Division and the Office of Appeals will issue a memorandum or communication to all of their employees reminding them that only employees officially participating in the Secure Email program are permitted to transmit emails with SBU data to taxpayers. Within the IRS's response transmittal, the IRS stated that it believes any appropriate actions against noncompliant employees will fall under the normal disciplinary procedures.



*Additional Security Is Needed  
for the Taxpayer Secure Email Program*

---

**Office of Audit Comment:** To ensure compliance with the Secure Email policy, we believe the IRS should provide, or at least reference, the actions that will be taken against unauthorized employees who transmit SBU emails to or from taxpayers. Explicitly stating these penalties would serve as a warning to employees who have not been approved to send or receive SBU data to or from taxpayers.



---

*Additional Security Is Needed  
for the Taxpayer Secure Email Program*

---

## **Appendix I**

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

The overall objective of this review was to determine whether IRS controls, policies, and procedures for sensitive email messages to taxpayers adequately protected taxpayers' data, guarded against email threats to the IRS network, and ensured email practices were compliant with Federal regulations. To accomplish this objective, we:

- I. Determined whether IRS employees authorized and profiled to correspond with taxpayers using encrypted email are in fact encrypting the email messages to protect SBU data.
  - A. Interviewed project leaders and managers in the LB&I Division and the Office of Appeals and reviewed training guidance and local procedures to determine how the Secure Email With Taxpayers program<sup>1</sup> is administered and the level of oversight it receives.
  - B. Determined whether disciplinary actions have been taken against IRS employees for violating the Secure Email With Taxpayers program policies by interviewing managers to determine if secure email violations have occurred and were reported and if appropriate disciplinary actions were taken. We also determined whether employee security awareness training includes reminders of disciplinary actions for email abuse.
  - C. Determined the population of LB&I Division and Office of Appeals employees and taxpayers enrolled in the secure email program since the program began.
  - D. Selected a random sample of 97 LB&I Division and Office of Appeals employees who were authorized to participate in the Secure Email With Taxpayers program and a random sample of 70 employees from the same offices who were not authorized. We then requested a download of the employees' Outlook mailbox. On February 18, 2010, we requested that 6 months of email activity, September 2009 through February 2010, be included in each mailbox for each employee. However, we did not receive all the historical emails that we requested for all employees in our samples. We received a disparate percentage of historical emails for 109 (60 percent) of the 167 employees. For the remaining 58 employees, the IRS provided the employees' current mailbox as of February 2010, which was after we initiated our audit.

---

<sup>1</sup> The IRS refers to the Secure Email With Taxpayers program as a "limited" program because only LB&I Division and Office of Appeals employees listed on a signed MOU are authorized to send and receive Sensitive But Unclassified data in emails to and from taxpayers.



---

*Additional Security Is Needed  
for the Taxpayer Secure Email Program*

---

The Modernization and Information Technology Services' Enterprise Operations (EOPS) office experienced technical challenges in retrieving and combining the weekly backup tapes that contained the 6 months of emails we requested for our sample. The EOPS office informed us at the start of the review that retrieving the historical emails would be challenging. Because of these challenges, on March 11, 2010, we reduced our scope from 6 to 3 months of historical emails, which reduced the number of backup tapes from 24 to 12. On April 20, 2010, we reduced our request again to only one backup tape for each of the previous 3 months. We also agreed to perform the work to combine the weekly backup tapes into one file for each employee, allowing the EOPS office to concentrate on retrieving the tapes. However, the EOPS office continued to report that the labor-intensive process of retrieving the weekly backup tapes along with other competing data requests was straining their resources. On May 20, 2010, the EOPS office informed us our data request was causing employees to cancel scheduled time-off, work weekends, and impacting its other requests for data. On May 21, 2010, 88 days after our initial request, we asked the EOPS office to discontinue its efforts.

Although we could not evaluate all of the emails that employees sent to and received from taxpayers during the 6-month or 3-month period preceding our audit, we believe the email activity the IRS provided was sufficient to determine some employees were not encrypting some of their emails with SBU data.

**Sampling Methodology**

We compiled a list of all LB&I Division employees who were authorized to participate nationwide. The total population was 567 employees. To mitigate the IRS's anticipated technical challenges in retrieving the mailboxes, we selected participating employees in three LB&I Division offices, rather than a random sample of employees from across the Nation. We selected all 82 of the participating employees in the three largest offices, which were: Dallas, Texas (30 employees); New York, New York (27 employees); and Houston, Texas (25 employees). We also requested the mailboxes for all 15 Appeals employees authorized to participate nationwide. This sampling methodology was sufficient to identify a control weakness and prompt management to take corrective action.

We also selected 55 LB&I Division employees who were not authorized to participate from the same offices. We selected 20 employees from the Dallas office, 15 employees from the Houston office, and 20 employees from the New York office. Lastly, we selected 15 Office of Appeals employees, nationwide, who were not authorized to send and receive SBU data in emails to taxpayers because they were not listed on an MOU.



---

*Additional Security Is Needed  
for the Taxpayer Secure Email Program*

---

- E. Determined whether only authorized employees are using email to send and receive SBU data to and from taxpayers in compliance with IRS policies and procedures by reviewing unencrypted emails in the mailboxes.
- F. Evaluated the encryption used by the IRS to ensure compliance with Federal Information Processing Standard (FIPS Data Encryption Standard 46-3).
- II. Determined whether the IRS is retaining email correspondence in accordance with applicable Federal requirements and IRS procedures.
  - A. Reviewed the IRS email retention policy and procedures to determine whether procedures include an approved recordkeeping system, electronic records are retrievable, and the encryption key is stored with the emails to allow decryption.
  - B. Determined whether all offices reviewed are following the same policies and procedures and using the same email recordkeeping system.
- III. Determined whether the IRS has implemented adequate controls to ensure the email system is secure and malicious content is not delivered to IRS employees or taxpayers.
  - A. Reviewed the Secure Enterprise Messaging System Security Plan and evaluated the security controls that have been implemented.
  - B. Identified all email servers that process LB&I Division and Office of Appeals emails with taxpayers.
  - C. Confirmed that the IRS is regularly conducting scans and vulnerability assessments on the email servers to ensure the email applications are configured securely.
  - D. Determined whether the IRS is actively scanning incoming email for malicious content on the primary main servers before email is sent to the end users and is actively scanning outgoing mail for sensitive information leaving the IRS network by reviewing and evaluating the email policies and rules and interviewing key IRS officials. We also determined how often the rules are modified and whether the antivirus software is enabled and properly updated by reviewing security assessment reports that are run each week and presented to IRS executives. Lastly, we evaluated the process the IRS has implemented to handle “spam” and other bulk emails.
- IV. Determined whether the IRS is timely closing email accounts of employees participating in the Secure Email With Taxpayers program when the employees leave the IRS.
  - A. Determined whether the IRS has implemented a process to ensure employees’ email accounts are closed when an employee participating in the Secure Email With Taxpayers program leaves the IRS by interviewing LB&I Division and Office of Appeals secure email project leaders.



*Additional Security Is Needed  
for the Taxpayer Secure Email Program*

---

- B. Determined whether the email accounts of participating employees, who departed the IRS in the last 12 months, were properly deleted from the email system.



*Additional Security Is Needed  
for the Taxpayer Secure Email Program*

---

**Appendix II**

*Major Contributors to This Report*

Alan Duncan, Assistant Inspector General for Audit (Security and Information Technology Services)  
Kent Sagara, Director  
Allen Gray, Audit Manager  
Charles Ekunwe, Senior Auditor  
George Franklin, Senior Auditor  
Larry Reimer, Senior Auditor  
Suzanne Westcott, Senior Auditor



---

*Additional Security Is Needed  
for the Taxpayer Secure Email Program*

---

**Appendix III**

*Report Distribution List*

Commissioner C  
Office of the Commissioner – Attn: Chief of Staff C  
Associate Chief Information Officer, Cybersecurity OS:CTO:C  
Associate Chief Information Office, Enterprise Operations OS:CTO:EO  
Chief Counsel CC  
National Taxpayer Advocate TA  
Director, Office of Legislative Affairs CL:LA  
Director, Office of Program Evaluation and Risk Analysis RAS:O  
Office of Internal Control OS:CFO:CPIC:IC  
Audit Liaisons:  
    Commissioner, Large Business and International Division SE:LB  
    Chief, Office of Appeals AP  
    Director, Office of Privacy, Information Protection and Data Security OS:P  
    Director, Risk Management Division OS:CTO:SP:RM



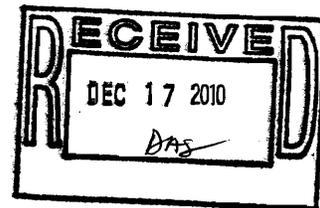
*Additional Security Is Needed  
for the Taxpayer Secure Email Program*

**Appendix IV**

*Management's Response to the Draft Report*



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



DEC 17 2010

MEMORANDUM FOR DEPUTY INSPECTOR GENERAL FOR AUDIT

FROM: Terrance V. Milholland *Terrance V. Milholland*  
Chief Technology Officer

SUBJECT: Draft Audit Report – Additional Security Is Needed for the Taxpayer Secure  
Email Program (Audit # 201020021) (e-trak# 2011-16800)

Thank you for the opportunity to review and respond to the subject draft audit report. The Secure Email with Taxpayer Program represents a departure from the traditional means of communicating with taxpayers, such as regular mail and telephone contact. We appreciate that the report acknowledged that the Internal Revenue Service (IRS) has controls in place for this program such as the installation of antivirus software on employee computers. We also thank you for acknowledging that with advances in supporting technologies and the increased use of email by taxpayers to conduct business, this program will enhance IRS's customer service with taxpayers and provide a more expedient and efficient way to exchange information.

The IRS's Modernization Information Technology Services organization is committed to continuously improving the security of our information technology process; your report recommendations will further improve our Secure Email with Taxpayer Program and processes. The attachment to this memo details our planned corrective actions. Of the nine report recommendations, we agree with six and partially agree with three.

We are addressing the corrective actions in which we partially agree. For recommendation #2, the IRS's Internal Revenue Manual (IRM) disciplinary procedures are appropriate for addressing email violations without the need for further delineation in Secure Email procedures. For recommendation #4, IRS will modify the Memorandum of Understanding (MOU) template to apprise the taxpayer of specific risks associated with transmitting unencrypted emails; however, we will not amend the MOU to address noncompliance. The taxpayer assumes the risk for unencrypted e-mails sent by the taxpayer. For recommendation #9, the IRS will reiterate its policy reminding employees that only employees officially participating in the Secure Email Program are permitted to transmit emails with Sensitive But Unclassified data to taxpayers. We believe any appropriate actions against noncompliant employees will fall under the normal IRM disciplinary procedures.



*Additional Security Is Needed  
for the Taxpayer Secure Email Program*

---

2

We value your continued support and the assistance and guidance your team provides. If you have any questions, please contact me at (202) 622-6800 or Darrin Brown, Senior Manager of Program Oversight, at (202) 283-4613.

Attachment



*Additional Security Is Needed  
for the Taxpayer Secure Email Program*

Attachment

Draft Audit Report – Additional Security Is Needed for the Taxpayer Secure Email Program  
(Audit # 201020021) (e-trak #2011-16800)

**RECOMMENDATION #1:** The Associate Chief Information Officer, Cybersecurity, should continue its acquisition of a data leakage prevention system to ensure full deployment by April 2012. This data leakage prevention system should include the ability to identify and stop unencrypted emails containing sensitive data, such as Social Security numbers, from leaving the IRS domain.

**CORRECTIVE ACTION #1:** We agree with this recommendation but based on current project plans we will now deploy by July 1, 2012. MITS CyberSecurity will lead the effort to acquire and deploy a Data Leakage Prevention solution through the Safeguarding Personally Identifiable Information Data Extracts (SPIIDE) project. SPIIDE will implement Data-In-Motion (DIM) components to address this issue. The project will also coordinate the deployment of Incident Response workflows with respective organizations including the Office of Privacy, Information Protection and Data Security (PIPDS). The final scope for policy, rules and corrective actions will be determined with input from TIGTA and other stakeholders.

**IMPLEMENTATION DATE:** July 1, 2012

**RESPONSIBLE OFFICIAL:** Associate Chief Information Officer, Cybersecurity

**CORRECTIVE ACTION MONITORING PLAN:** We enter accepted Corrective Actions into the Joint Audit Management Enterprise System (JAMES) and monitor them on a monthly basis until completion.

**RECOMMENDATION #2:** The LB&I Division and Office of Appeals should coordinate with the Office of Privacy, Information Protection and Data Security to develop and enforce additional procedures for employees participating in the Secure Email With Taxpayers program. The procedures should address how, when, and to whom employee and taxpayer secure email violations should be reported and that appropriate actions will be taken against employees who do not encrypt sensitive email messages to taxpayers.

**CORRECTIVE ACTION #2A:** We partially agree with the recommendation. The Large Business and International (LB&I) Division will take the lead and coordinate with the Office of Privacy, Information Protection and Data Security (PIPDS) to ensure the IRS's policy on privacy and security incorporates the use of secure email with taxpayers. The LB&I Division will also ensure its Web site is consistent with guidance set forth by Cybersecurity on secure email with taxpayers. In addition, the LB&I Division will advise its employees participating in the Secure Email for Taxpayers Program of their responsibilities on how, when and to whom they should report secure email violations.

**IMPLEMENTATION DATE:** August 15, 2011



---

*Additional Security Is Needed  
for the Taxpayer Secure Email Program*

---

Attachment

Draft Audit Report – Additional Security Is Needed for the Taxpayer Secure Email Program  
(Audit # 201020021) (e-trak #2011-16800)

---

**RESPONSIBLE OFFICIALS:** Director, Business Systems Planning (LB&I Division)

**CORRECTIVE ACTION MONITORING PLAN:** We enter accepted Corrective Actions into the Joint Audit Management Enterprise System (JAMES) and monitor them on a monthly basis until completion.

**CORRECTIVE ACTION #2B:** We partially agree with the recommendation. The Office of Appeals will update its Web site to link to the appropriate IRS policy on privacy and security for secure email with taxpayers. The Office of Appeals will also advise its employees participating in the Secure Email for Taxpayers Program of their responsibilities on how, when and to whom they should report secure email violations.

**IMPLEMENTATION DATE:** August 15, 2011

**RESPONSIBLE OFFICIAL:** Director, Business Systems Planning (Office of Appeals)

**CORRECTIVE ACTION MONITORING PLAN (#2a & #2b):** We enter accepted Corrective Actions into the Joint Audit Management Enterprise System (JAMES) and monitor them on a monthly basis until completion.

**RECOMMENDATION #3:** The LB&I Division and Office of Appeals should update guides and training materials to include the new reporting procedures.

**CORRECTIVE ACTION #3A:** We agree with the recommendation. The LB&I Division will update its training materials and guides to include all current and any new reporting procedures and policies relating to the Secure Email Program.

**IMPLEMENTATION DATE:** August 15, 2011

**RESPONSIBLE OFFICIAL:** Director, Business Systems Planning (LB&I Division)

**CORRECTIVE ACTION #3B:** We agree with the recommendation. The Office of Appeals will update its Web site to link to the approved IRS training materials and guides.

**IMPLEMENTATION DATE:** August 15, 2011

**RESPONSIBLE OFFICIAL:** Director, Business Systems Planning (Office of Appeals)



*Additional Security Is Needed  
for the Taxpayer Secure Email Program*

Attachment

Draft Audit Report – Additional Security Is Needed for the Taxpayer Secure Email Program  
(Audit # 201020021) (e-trak #2011-16800)

**CORRECTIVE ACTION MONITORING PLAN (#3a & #3b):** We enter accepted Corrective Actions into the Joint Audit Management Enterprise System (JAMES) and monitor them on a monthly basis until completion.

**RECOMMENDATION #4:** The LB&I Division and Office of Appeals should coordinate to amend the MOU to apprise the taxpayer of the specific risks associated with transmitting unencrypted emails with SBU data and provide specific actions that will be taken when taxpayers or their representatives do not comply with the terms of the MOU. For example, the IRS could potentially terminate the MOU if the taxpayer or taxpayer's representatives repeatedly fail to encrypt sensitive emails. These actions would provide accountability to taxpayers to comply with the MOU.

**CORRECTIVE ACTION #4A:** We partially agree with the recommendation. The LB&I Division will modify the existing Secure Email for Taxpayers Memorandum of Understanding (MOU) Template to make the taxpayer fully aware of the security risks if they choose to send email unencrypted. In addition, the LB&I Division will issue the modified MOU to all its participants in the Secure Email Program.

**IMPLEMENTATION DATE:** August 15, 2011

**RESPONSIBLE OFFICIALS:** Director, Business Systems Planning (LB&I Division)

**CORRECTIVE ACTION #4B:** We partially agree with the recommendation. The Office of Appeals will issue the modified MOU to all its participants in the Secure Email Program.

**IMPLEMENTATION DATE:** August 15, 2011

**RESPONSIBLE OFFICIAL:** Director, Business Systems Planning (Office of Appeals)

**CORRECTIVE ACTION MONITORING PLAN (#4a & #4b):** We enter accepted Corrective Actions into the Joint Audit Management Enterprise System (JAMES) and monitor them on a monthly basis until completion.

**RECOMMENDATION #5:** The Office of Privacy, Information Protection and Data Security should take actions to update the IRS's official internal procedures with the additional procedures developed by the LB&I Division and Office of Appeals and post the procedures to its internal web site.

**CORRECTIVE ACTION #5:** We agree with this recommendation. In August 2010, the Office of Privacy, Information Protection and Data Security (PIPDS) updated its internal website to reflect current IRS guidance and procedures for sending email containing PII within IRS as well as to authorized non-IRS parties (other than taxpayers and their representatives). This guidance included that the only approved process for sending secure email containing PII to



*Additional Security Is Needed  
for the Taxpayer Secure Email Program*

Attachment

Draft Audit Report – Additional Security Is Needed for the Taxpayer Secure Email Program  
(Audit # 201020021) (e-trak #2011-16800)

taxpayers or their representatives was through the encryption solution utilized in the LB&I and Appeals Secure Email pilots and only approved pilot participants could use this capability. This guidance is consistent with IRM 1.10.3, Standards for Using Email and the encryption guidance contained in IRM 10.8.1, Information Technology (IT) Security, Policy and Guidance. PIPDS will continue to monitor the Secure Email pilots/programs and will update its internal website, as appropriate, as new procedures are developed.

**IMPLEMENTATION DATE:** Completed

**RESPONSIBLE OFFICIALS:** Director, Privacy, Information Protection and Data Security

**CORRECTIVE ACTION MONITORING PLAN:** N/A

**RECOMMENDATION #6:** The Office of Privacy, Information Protection and Data Security should update the Annual Information Protection and Disclosure Briefing to include the new Secure Email With Taxpayers procedures.

**CORRECTIVE ACTION #6:** We agree with this recommendation. The Office of Privacy, Information Protection and Data Security will update the Annual Information Protection and Disclosure Briefing to indicate secure email with taxpayers can only occur under agency/MITS approved pilots and programs.

**IMPLEMENTATION DATE:** July 1, 2011

**RESPONSIBLE OFFICIALS:** Director, Privacy, Information Protection and Data Security

**CORRECTIVE ACTION MONITORING PLAN:** We enter accepted Corrective Actions into the Joint Audit Management Enterprise System (JAMES) and monitor them on a monthly basis until completion.

**RECOMMENDATION #7:** The Associate Chief Information Officer, Cybersecurity, should update its mandatory annual Information Systems Security briefing to include or reference the new Secure Email With Taxpayers procedures.

**CORRECTIVE ACTION #7:** We agree with this recommendation. The ACIO, Cybersecurity will update the Information Systems Security supplemental briefing to include or reference the Secure Email With Taxpayers procedures. This supplemental briefing is a part of the mandatory security awareness training provided to all IRS employees annually.

**IMPLEMENTATION DATE:** August 1, 2011

**RESPONSIBLE OFFICIALS:** Associate Chief Information Officer, Cybersecurity



---

*Additional Security Is Needed  
for the Taxpayer Secure Email Program*

---

Attachment

Draft Audit Report – Additional Security Is Needed for the Taxpayer Secure Email Program  
(Audit # 201020021) (e-trak #2011-16800)

---

**CORRECTIVE ACTION MONITORING PLAN:** We enter accepted Corrective Actions into the Joint Audit Management Enterprise System (JAMES) and monitor them on a monthly basis until completion.

**RECOMMENDATION #8:** To ensure persistent medium-risk vulnerabilities receive management oversight and timely corrective actions, the Associate Chief Information Officer, Enterprise Operations, should ensure the vulnerabilities detected on each email server during the monthly security assessments are appropriately tracked. If persistent medium-risk vulnerabilities cannot be corrected within two months, the Enterprise Operations office should follow IRS security requirements to post the vulnerabilities to the appropriate Plan of Actions and Milestones.

**CORRECTIVE ACTION #8:** We agree with this recommendation. As identified in the Taxpayer Secure Email Program draft report (201020021), the IRS executes monthly Policy Checker and Vulnerability Scans on all email servers. To date, the primary focus has been the remediation of high-risk items. The Associate Chief Information Officer, Enterprise Operations will initiate tracking and correction of medium-risk vulnerabilities.

A process will be implemented to ensure all medium risk vulnerabilities that cannot be corrected within 60 days and high risk vulnerabilities that cannot be corrected within 30 days of detection will be documented within a Plan of Action and Milestones and entered into Trusted Agent FISMA for the GSS hosting the email systems.

**IMPLEMENTATION DATE:** April 1, 2011

**RESPONSIBLE OFFICIALS:** Associate Chief Information Officer, Enterprise Operations

**CORRECTIVE ACTION MONITORING PLAN:** We enter accepted Corrective Actions into the Joint Audit Management Enterprise System (JAMES) and monitor them on a monthly basis until completion.

**RECOMMENDATION #9:** The LB&I Division and Office of Appeals should issue a memorandum to their employees reminding them of the Secure Email With Taxpayers policy and the actions that will be taken against unauthorized employees who violate the policy by sending or receiving emails with SBU data to or from taxpayers.

**CORRECTIVE ACTION #9A:** We partially agree with the recommendation. The LB&I Division will issue a memorandum to all its employees reminding them that only employees officially participating in the Secure Email Program are permitted to transmit emails with Sensitive But Unclassified (SBU) data to taxpayers.

**IMPLEMENTATION DATE:** March 15, 2011



---

*Additional Security Is Needed  
for the Taxpayer Secure Email Program*

---

Attachment

Draft Audit Report – Additional Security Is Needed for the Taxpayer Secure Email Program  
(Audit # 201020021) (e-trak #2011-16800)

---

**RESPONSIBLE OFFICIALS:** Director, Business Systems Planning (LB&I Division)

**CORRECTIVE ACTION #9B:** We partially agree with the recommendation. The Office of Appeals will communicate to all its employees reminding them that only employees officially participating in the Secure Email Program are permitted to transmit emails with SBU data to taxpayers.

**IMPLEMENTATION DATE:** March 15, 2011

**RESPONSIBLE OFFICIAL:** Director, Business Systems Planning (Office of Appeals)

**CORRECTIVE ACTION MONITORING PLAN (#9a & #9b):** We enter accepted Corrective Actions into the Joint Audit Management Enterprise System (JAMES) and monitor them on a monthly basis until completion.