TREASURY INSPECTOR GENERAL FOR TAX ADMINISTRATION

While the Data Loss Prevention Solution Is Being Developed, Stronger Oversight and Process Enhancements Are Needed for Timely Implementation Within Budget

September 22, 2014

Reference Number: 2014-20-087

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
3 = Other Identifying Information

Phone Number / 202-622-6500
E-mail Address / TIGTACommunications@tigta.treas.gov
Website / http://www.treasury.gov/tigta

WHILE THE DATA LOSS PREVENTION SOLUTION IS BEING DEVELOPED, STRONGER OVERSIGHT AND PROCESS ENHANCEMENTS ARE NEEDED FOR TIMELY IMPLEMENTATION WITHIN BUDGET

Highlights

Final Report issued on September 22, 2014

Highlights of Reference Number: 2014-20-087 to the Internal Revenue Service Chief Technology Officer.

IMPACT ON TAXPAYERS

The protection of sensitive and personal information is more important than ever with electronic communications becoming increasingly prevalent. Safeguarding Personally Identifiable Information in the possession of the IRS is essential to retaining the trust of taxpayers.

WHY TIGTA DID THE AUDIT

This audit is included in our Fiscal Year 2014 Annual Audit Plan and addresses the IRS major management challenge of *Security of Taxpayer Data and Employees*. The overall objective was to determine whether the Safeguarding Personally Identifiable Information Data Extracts (SPIIDE) Project is developing a data loss prevention (DLP) and protection solution for implementation in accordance with applicable policies and procedures and within budget to safeguard sensitive taxpayer data.

WHAT TIGTA FOUND

The SPIIDE Project team is progressing in its development and implementation of the DLP solution. The team has completed key required enterprise life cycle deliverables and has been identifying and addressing security weaknesses as they are detected. Notwithstanding these achievements, the SPIIDE Project team continues to face challenges to timely implement the DLP solution to protect from disclosing Personally Identifiable Information and data that should not be exiting IRS networks.

Based on its new projected implementation date of December 31, 2014, the IRS will have taken more than four years to build and develop its DLP solution. Because of the length of time taken, TIGTA believes that stronger management oversight is needed to ensure that the DLP solution meets its new implementation date within budget. In addition, the IRS could not provide support to validate SPIIDE Project spending, which it reports to be more than $9.6 million of the $11.4 million budgeted through Fiscal Year 2014.

Lastly, DLP solution processes and procedures can be enhanced while the DLP solution is still being developed. While TIGTA determined that the DLP Operations team correctly classified 99 (94 percent) of 105 sampled e-mail events, TIGTA also found that 17 (57 percent) of the 30 appropriately classified e-mail events were potential incidents that were not forwarded to all appropriate incident responders. These incidents should have been forwarded to and/or accepted by the Office of Privacy, Governmental Liaison, and Disclosure. That office should have then advised the affected parties of the disclosure and offered credit monitoring services in 11 of the 17 potential incidents.

WHAT TIGTA RECOMMENDED

TIGTA recommended that the Chief Technology Officer ensure that the SPIIDE Project team reconciles the DLP solution funding and expenses and resolves discrepancies identified during the audit. TIGTA also recommended that the Director, Privacy, Governmental Liaison, and Disclosure, revise the disclosure acceptance criteria to ensure that all potential Personally Identifiable Information disclosure incidents are reported.

In their response, IRS management agreed with all but two recommendations. The IRS partially agreed with one recommendation and disagreed with the recommendation to revise its disclosure acceptance criteria. TIGTA agrees with the rationale for the partial agreement, but believes that the acceptance criteria should be revised to protect against disclosures.

TREASURY INSPECTOR GENERAL
FOR TAX ADMINISTRATION

DEPARTMENT OF THE TREASURY
WASHINGTON, D.C. 20220

September 22, 2014

MEMORANDUM FOR CHIEF TECHNOLOGY OFFICER

FROM: Michael E. McKenney
Deputy Inspector General for Audit

SUBJECT: Final Audit Report – While the Data Loss Prevention Solution Is Being Developed, Stronger Oversight and Process Enhancements Are Needed for Timely Implementation Within Budget (Audit # 201420024)

This report presents the results of our review of the Internal Revenue Service's data loss prevention solution. The overall objective of this review was to determine whether the Safeguarding Personally Identifiable Information Data Extracts Project is developing a data loss prevention and protection solution for implementation in accordance with applicable policies and procedures and within budget to safeguard sensitive data. This audit is included in our Fiscal Year 2014 Annual Audit Plan and addresses the major management challenge of Security for Taxpayer Data and Employees.

Management's complete response is included in Appendix VI.

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 Kent Sagara, Acting Assistant Inspector General for Audit (Security and Information Technology Services).

Table of Contents

Abbreviations

CSIRC	Computer Security Incident Response Center
DAR	Data-at-Rest
DIM	Data-in-Motion
DIU	Data-in-Use
DLP	Data Loss Prevention
IFS	Integrated Financial System
IPS	Integrated Procurement System
IRM	Internal Revenue Manual
IRS	Internal Revenue Service
OMB	Office of Management and Budget
OPR	Office of Professional Responsibility
Ops	Operations
PGLD	Privacy, Governmental Liaison, and Disclosure
PII	Personally Identifiable Information
SBU	Sensitive But Unclassified
SPIIDE	Safeguarding Personally Identifiable Information Data Extracts
SSN	Social Security Number
TIC	Trusted Internet Connection
TIGTA	Treasury Inspector General for Tax Administration
TIN	Taxpayer Identification Number

Background

The protection of sensitive and personal information is more important than ever with electronic communications becoming increasingly prevalent. Safeguarding Personally Identifiable Information (PII) in the possession of the Federal Government and preventing its breach are essential to retaining the trust of the American public. This responsibility is shared by officials accountable for administering operational, privacy, and security programs. PII is any information that, by itself or in combination with other information, may be used to uniquely identify an individual. For the Internal Revenue Service (IRS), PII primarily consists of Social Security Numbers (SSN), names, addresses, dates and places of birth, bank account numbers, e-mail addresses, telephone numbers, and mother's maiden names. The Office of Management and Budget (OMB) and the Department of the Treasury (Treasury) Chief Information Office released several memoranda to address the issue of safeguarding PII across all Federal agencies.

In a February 2011 report,[1] the Treasury Inspector General for Tax Administration (TIGTA) reported that the IRS had not implemented a recommended enterprise data leakage prevention system before approving the Secure Email With Taxpayers program because the IRS, along with 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. In addition, the report linked the importance of the recommended data leakage system with the Administration's Trusted Internet Connection (TIC)[2] initiative, which is one of three priorities to improve cybersecurity and the security of Federal information systems. The TIC initiative aims to improve agencies' security posture and incident response capabilities through enhanced monitoring and situational awareness of all external network connections.

In response to the OMB memoranda, the IRS Cybersecurity's Architecture and Implementation Branch is leading the Safeguarding Personally Identifiable Information Data Extracts (SPIIDE) Project to promote secure practices in electronic communications (e-mails and Internet access) on the IRS network to protect Sensitive But Unclassified (SBU) data. Taking a phased approach, the SPIIDE Project team plans to build a system environment to implement the Symantec's Data Loss Prevention (DLP) commercial off-the-shelf software solution that is capable of identifying and tracking a number of the IRS's defined PII datasets. The DLP solution is designed to give the IRS an enterprise view into where its most sensitive data are stored, who has access to the data, and where and by whom the data are sent to outside the IRS network. By using this information, the IRS can spot broken business processes and reduce the overall risk of exposure. The DLP solution is a system that will take a data-centric approach to security, in which policies

[1] Treasury Inspector General for Tax Administration, Ref. No.2011-20-012, *Additional Security Is Needed for the Taxpayer Secure E-Mail Program* p. 5 (Feb. 2011).
[2] See Appendix V for a glossary of terms.

can be developed around the content that should be protected and then deployed across multiple data states or functionalities, such as identifying, monitoring, and preventing. The DLP solution consists of three components: Data-in-Motion (DIM), Data-at-Rest (DAR), and Data-in-Use (DIU).

- The DIM monitors data moving across the IRS's information technology perimeter and identifies PII in e-mails and attachments that are in the process of being sent from the IRS. Once identified, the system can prevent inappropriate dissemination of the PII based upon policy. While the system is being developed, the SPIIDE Project team will not prevent e-mails from being sent out until the DIM capability is fully implemented and National Treasury Employees Union (hereafter referred to as Union) negotiations are completed. The IRS plans to implement only the DIM component in its initial release.
- The DAR discovers and identifies PII residing across the IRS's vast information technology infrastructure and determines whether it has adequate protection. The DAR scans PII stored on network databases, storage devices, and SharePoint sites. The DAR is scheduled for implementation in Release 2.
- The DIU monitors data being created and manipulated on users' workstations and prevents the unintended or malicious distribution, storage, or alteration. The DIU, installed on users' laptops, identifies PII that is stored on thumb drives and compact disks as well as in e-mails. The DIU tags PII in e-mails as it is being typed and is more preventive rather than reactive when compared to the DIM. The DIU is scheduled for implementation in Release 3.

This review was performed at the Information Technology organization's Cybersecurity office in New Carrollton, Maryland, during the period December 2013 through June 2014. We conducted this performance audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objective. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objective. Detailed information on our audit objective, scope, and methodology is presented in Appendix I. Major contributors to the report are listed in Appendix II.

Results of Review

The SPIIDE Project team is progressing in its development and implementation of the DLP solution. They have completed key required enterprise life cycle deliverables through the current milestone and have been identifying and addressing security weaknesses as they are identified, such as defining user roles and responsibilities to ensure that separation of duties exists and creating individual user accounts with minimum required privileges rather than the team using the default administrator account that provided privileged accesses and permissions to the system. The SPIIDE Project team has also conducted several e-mail monitoring tests of the DLP solution to determine whether the system is identifying disclosures of PII as expected and is updating the policy to reduce the number of false positives.

The IRS paid more than $3.7 million to purchase user seat licenses and maintenance for the DLP solution for use by all of the Treasury. This amount was far less than the initial bid of $5.9 million for licenses and maintenance that Symantec offered the IRS for the same number of users, despite not effectively using all of them. Specifically, the IRS bought 110,000 individual user seat licenses and maintenance for the DIM component it is developing and the other two DLP solution components (the DIU and the DAR) that are not scheduled for implementation. In addition, the IRS bought 30,000 individual user seat licenses and maintenance for all three DLP solution components for the Treasury to use, although to date only two agencies have inquired about the licenses and none have requested to use them. According to the new executive assigned to the SPIIDE Project, the reason for the limited use is that other agencies within the Treasury have run into similar development and implementation challenges as those experienced by the IRS. The IRS is now providing guidance to the other agencies in the Treasury and instituting a process that can be repeated for future implementation of the remaining DLP solution components. For example, the IRS is considering adding policies to the DLP solution that will include identifying bank account numbers that are leaked from its networks.

Notwithstanding the above achievements, the SPIIDE Project team continues to face challenges to timely implement the DLP solution to protect PII from disclosure and loss of data. Stronger management oversight is needed to ensure that the DLP solution meets its new implementation date within budget. In addition, DLP solution processes and procedures can be enhanced to improve the effectiveness of the DLP solution.

Stronger Management Oversight Is Needed to Ensure That the Data Loss Prevention Solution Meets Its New Implementation Date Within Budget

Based on its new projected implementation date, the IRS will have taken more than four years to build and develop the DLP solution and implement one (the DIM) of the three components to

protect PII since the SPIIDE Project was first chartered in March 2010. In a February 2011 TIGTA report, the IRS planned to fully implement the DLP solution in April 2012 and later changed the date to July 2012. In April 2013, the SPIIDE Project team requested and received Executive Steering Committee approval to rebaseline the implementation of the DLP solution by December 31, 2014. Because of the length of time taken to implement the DLP solution, we believe that the IRS is at risk of not fulfilling a recommended DLP solution capability, which is included in the Administration's TIC initiative for improving cybersecurity and the security of Federal information systems.

Management control challenges have affected the implementation of the DLP solution

The SPIIDE Project team has and continues to face challenges to timely implement the DLP solution. These challenges include insufficient funding and dedicated resources, changes in project leadership and lack of experience, and project administration and execution issues with the development and implementation of the DLP solution.

- The DLP solution continues to compete for limited IRS information technology program funding and resources with other higher priority projects and initiatives, such as the Affordable Care Act,[3] the Customer Account Data Engine 2, and each annual filing season from 2012 through 2014. As a result of the funding and resource demands: 1) the SPIIDE Project team lost a project manager and two of four contracted subject matter experts; 2) the development, integration, and test environment was not initially funded and delayed the start of the DLP solution pilot by nine months; and 3) functions in the IRS Information Technology organization were delayed in reviewing architecture plans and performing operational implementation maintenance and work, *e.g.*, system administrators were not readily available to replace and test a computer motherboard that crashed, on the DLP solution.
- The SPIIDE Project team lacked consistent leadership, team members, and experience in developing and implementing the DLP solution. The DLP solution has had at least three project managers during its development. In addition, we reviewed the SPIIDE Project team's list of lessons learned, which indicated issues with stakeholder communications, the need for longer commitments from team members, team members' limited knowledge of the enterprise life cycle process and requirements management, inadequate relationships with process owners, poor planning when requesting necessary equipment, and insufficient lead time for contractors to obtain background clearances. For example, beginning in February 2011, the SPIIDE Project team experienced approximately a five-month delay with contract negotiations and waiting for contractor

[3] Pub. L. No. 111-148, 124 Stat. 119 (2010) (codified as amended in scattered sections of the U.S. Code), as amended by the Health Care and Education Reconciliation Act of 2010, Pub. L. No. 111-152, 124 Stat. 1029.

background clearances, only to discover that the contractors, ******3****** ********3********, were not qualified and had to be replaced.

- Due to miscommunication between the SPIIDE Project team and the Office of Privacy, Governmental Liaison, and Disclosure (PGLD), a live data waiver, a requirement for testing when using real taxpayer data, was allowed to expire, which delayed further testing of the DLP solution in February 2014. Operating without a live data waiver violated IRS policy. Internal Revenue Manual (IRM) 10.8.8.1, *Live Data Protection*, requires that the use of live data is prohibited without approval from the PGLD office. This provision applies to all offices, business, operating, and functional units within the IRS, and is to be applied when live data are used to accomplish the IRS's mission. This manual also applies to individuals and organizations having contractual arrangements with the IRS, including employees, contractors, vendors, and outsourcing providers that use or operate information technology systems containing IRS live data.
- In September 2013, the IRS hired an executive in its Cybersecurity office with experience in implementing the DLP solution. Among his responsibilities for the SPIIDE Project is to help provide guidance for its development and implementation efforts. The executive offered some insight into why the SPIIDE Project encountered and continues to encounter delays. For example, the responsibility for the expected data output should lie with the business owners rather than the SPIIDE Project team, and the processes, roles, and responsibilities that are now being developed should have been in place earlier.
- Efforts to involve the Union should have begun earlier to negotiate the process for addressing employees involved with outbound unencrypted e-mails. The process can be laborious and involve bargaining experts who represent the Union as well as IRS management and attorneys.

To provide perspective regarding the length of time used to implement the DLP solution, we identified and contacted two other Government agencies, the U.S. Postal Service and the Department of State, that have implemented the solution. They shared with us that they were able to implement their DLP solution through a "plug and play," rather than building a system environment, in approximately six and 24 months, respectively. The IRS's response to the other Government agencies "plug and play" was that it was not a viable option. Officials shared with us that they have tax systems that could/would most likely be negatively affected if drivers were automatically installed by "plug and play" software. While both agencies implemented the DIM first, the U.S. Postal Service was able to start blocking e-mails within three months after implementation and has subsequently implemented the DAR component. Both agencies initially identified SSNs in their search criteria; however, the U.S. Postal Service includes credit card numbers and threatening words. We shared our observations of the other agencies with the SPIIDE Project team.

The designed capabilities of the DLP solution can be improved

When the IRS's DLP solution is implemented, it will not be as robust in its capabilities as the solution can provide, especially when identifying more SSNs that could exit the IRS network undetected. Specifically, the SPIIDE Project team included policies in the DLP solution to identify PII using only SSNs, based on a specific pattern, and only in association with key words or phrases (*i.e.*, Social Security Number, SSN, SS#) in unencrypted outbound e-mails. However, we determined the IRS could add another common term, Taxpayer Identification Numbers (TIN), independently or in association with SSNs, to further enhance the DLP solution capabilities.

We conducted research of TIGTA's Data Center Warehouse, which receives selected downloads of IRS computer data, and identified four major IRS databases[4] that use the heading "TIN" as a key word in identifying taxpayer SSNs. During the audit, we conducted an independent testing of the DLP solution to determine whether the DLP solution is capable of identifying unencrypted e-mails containing PII. We designed 43 e-mails containing TIN as the key word. The DLP solution did not identify any of the e-mails because policies were not created to identify that key word.

In addition, during the independent testing, we created 32 e-mails that met the narrow policy criteria currently used by the DLP solution. These e-mails contained the ADOBE portable document format, jpeg, Excel, and Word documents with the key word SSN and a nine-digit number separated by hyphens, periods, no spaces, and spaces as separators. The DLP solution correctly identified 28 (88 percent) of the 32 e-mails. However, for the remaining four e-mails, the DLP solution failed to identify the SSNs in Excel documents because the key word "SSN" was placed in comment boxes in the spreadsheets rather than inside the cells.

We discussed the four exceptions with the SPIIDE Project team, and they stated that the DLP solution version 11.6 the IRS purchased could not detect embedded comments in Microsoft Office 2007 files. They further stated that the Symantec vendor corrected the issue in version 12. The SPIIDE Project team plans to upgrade to version 12 after full deployment, if funding is available. The upgrade will need to be discussed with the Enterprise Life Cycle Project Management Office because it may be considered a major system change, which will require the SPIIDE Project team to coordinate work with the IRS's Enterprise Operations function, rework enterprise life cycle and other project documentation, and perform additional testing and all other maintenance release tasks.

Guidelines and recommendations as well as other factors, such as impact and dependency for other systems, also needed to be considered when implementing a DLP solution. The National Institute for Standards and Technology Special Publication 800-122, *Guide to Protecting the*

[4] The four IRS databases were the Integrated Data Retrieval System, the Integrated Collection System, the Automated Collection System, and the Examination Returns Control System. These computer systems are capable of retrieving, updating, or providing employees with access to stored taxpayer information.

Confidentiality of Personally Identifiable Information,[5] recommends that agencies implement automated tools, such as a network data leakage prevention tool, to monitor transfers of PII and to monitor inbound and outbound communications for unauthorized activities. In addition, the Government Accountability Office's *Standards for Internal Control in the Federal Government*[6] provides that application controls should be designed to help ensure completeness, accuracy, authorization, and validity of all transactions during application processing. Controls should be installed as an application interfaces with other systems to ensure that all inputs are received and are valid and that outputs are correct and properly distributed.

The IRS is developing a partial DLP solution to identify potential disclosures of PII associated with the key word "SSN" in its outbound unencrypted e-mails. Without a more robust DLP solution in place, the IRS lessens its ability to effectively and accurately discover or prevent PII data leakage, maintain confidentiality of data, ensure public trust of conducting business electronically, and prevent disclosure and loss of information. However, once implemented, the IRS plans to add additional polices to the DIM that will identify passwords, credit card numbers, and bank account numbers.

DLP solution budget and expense figures could not be supported

The IRS could not provide support to validate that the SPIIDE Project spent more than $9.6 million of its budgeted $11.4 million through Fiscal Year 2014 to implement the DLP solution. As part of our review, we requested from the Information Technology Financial Management Services copies of all contracts and payment invoices, including dollar amounts reported on the Integrated Financial System (IFS) and Integrated Procurement System (IPS), associated with the SPIIDE Project. The IRS took approximately three months to provide 18 contracts and 118 invoices related to the project. This effort to provide supporting documentation and clarification involved several IRS organizations including the SPIIDE Project, Information Technology Financial Management Services, Chief Financial Officer, and Procurement offices.

We attempted to reconcile the budget and invoice expense totals by contract to the dollar amounts reported on the IFS and the IPS. We planned to conduct further analyses on any differences between the two amounts, if any were identified. However, due to the complexity and age of some of the contracts, *e.g.*, multiple projects under one contract dating back to 2006, and the obstacles encountered in obtaining and reconciling the budget and invoice expense amounts, we eventually opted to review one contract, totaling more than $3.5 million, in-depth until we were able to identify a process to quickly resolve the differences in the dollar amounts.

[5] National Institute of Standards and Technology, NIST SP 800-122, *Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)* (April 2010).
[6] Government Accountability Office (formerly known as the General Accounting Office), GAO/AIMD-00-21.3.1, *Internal Control: Standards for Internal Control in the Federal Government* (Nov. 1999).

For two months, we made repeated requests to resolve differences in the budgeted and expense amounts, which to date remain unresolved.

Based upon the limited scope of our review, we identified the following issues that were in multiple contracts and in the single contract reviewed. Contracts and invoices provided were not always associated with the SPIIDE Project and DLP solution. The IRS provided invoices that were not related to the DLP solution but instead were related to a different project. In contrast, it did not provide at least one contract and potentially other invoices associated with the SPIIDE Project. During our preliminary review to reconcile the budget and invoice expense totals, we located an invoice identified as a DLP solution expense, along with the contract number, but this contract was not one of the 18 contracts initially provided to us. Moreover, some of our calculated expense totals did not match the expense totals reported in the IFS, with differences ranging from $1,200 to more than $3.3 million, indicating the potential for unaccounted invoice expenses. Budget and invoice calculated expense totals did not reconcile to figures reported in the IFS and the IPS. We selected one contract for an in-depth review, and our results included the following:

- From four line items in the contract, we calculated $1,105,392.06 was budgeted for the SPIIDE Project. However, the amount for the same contract as reported in the IFS was $795,392, and in the IPS, it was $871,670.78. The difference between our amount and the IFS figure is due to one line item that was not included in the IFS. IRS personnel stated the line item in question should not be included in the total budget because it was not charged to the SPIIDE Project, despite the line item being clearly marked as such. In addition, we identified one invoice related to the SPIIDE Project that was charged to the line item that should not have been included.

  In the IPS, there were four budgeted amounts, but none matched the line item amounts in the contract we reviewed. IRS personnel stated it was possible that there were remaining funds never spent and later de-obligated. They stated it is a common practice to leave a small amount of funds on each line item just in case new expenses come in. IRS personnel never confirmed whether the funds were de-obligated and whether the de-obligated funds accounted for the differences between the IPS amounts and the contract amounts.

- Invoice amounts did not match payment amounts in the IFS. For example, an invoice for $22,595.61 was recorded in the IFS as $18,919.03 and was paid as $18,950.56. The invoice indicated that the payment was short $3,676.58, which is the difference in the invoice amount recorded in the IFS. However, there is no explanation in the IFS of why a different amount was actually paid. In another example, an invoice for $45,950.35 was recorded in the IFS for the same amount but $46,016.29 was paid. Although the difference was small, there was no explanation in the IFS for the change.

- Fees billed on invoices for the SPIIDE Project and other information technology projects were not proportionately allocated and charged in the IFS. For example, an invoice billed

for the SPIIDE Project and another project totaled $54,149.32, which included a 7.75 percent fee of $3,894.74. The subtotal including the fee for the SPIIDE Project should have been $29,301.84 but was recorded in the IFS as $29,141.66. The fee was also not correctly applied for the other project's expense. We observed similar concerns in 13 other invoices for which amounts in the IFS showed fees were misapplied for approximately $340.

- Other documents provided as support for invoice amounts were not useful, but the invoices were paid. For example, one invoice for $140,112.96 was paid, but the supporting documents attached to the invoice only supported $45,293.23. We inquired about the additional documentation but did not receive it. Also, in our preliminary review of all invoices, we identified numerous instances in which supporting documentation was lacking, such as timesheets to support the number of hours billed for each contractor.

While the dollar discrepancies above may be comparatively small, the results are for one of at least 19 contracts.[7] If similar results are found in other contracts, collectively, they could have a material effect on the budget and spending for the SPIIDE Project.

Specific requirements in IRM 1.35.3, *Receipt and Acceptance Guidelines*, provide that Federal agencies must adhere to 31 United States Code 3512, *Executive Agency Accounting and Other Financial Management Reports and Plans*, which requires agencies to establish and maintain systems of accounting and internal control to provide reliable accounting of the agency's activities. The systems must provide reasonable assurance that transactions are properly recorded and accounted for and are in compliance with laws and regulations. The accurate and timely recording of both receipt and acceptance is critical in assuring that the IRS's financial statements are materially correct. The IRM further requires the office that physically receives or accepts the goods or services must have and maintain documentation that supports recording the appropriate accounting entry. An invoice by itself is not sufficient documentation to support receipt or acceptance by the business unit.

During our discussions on the budget and expenses, IRS personnel could not explain the differences in the figures reported in the IFS and the IPS. ********3********** **3** **3** ***. The contracting officer's representative stated that there were four contracting officer's representatives who made entries to the contract because of employee turnover in business units that resulted from transfers and retirements. The contracting officer's representative further stated that the IPS does not have controls in place to restrict system access and that any contracting officer's representative can access any contracts to make a journal entry and make

[7] The 19 contracts are the 18 that the IRS provided to us and the one contract we identified during our attempt to reconcile the budget and invoice expense totals.

payments. In addition, the IPS does not have checks and balances to ensure that inputs are properly charged to the correct program, especially in contracts for multiple projects.

Because the DLP solution budget and expenses were not supported and accurately calculated in the contract we reviewed, the IRS is exposed to potentially spending more than what was budgeted for the SPIIDE Project.

Management actions: After the completion of our fieldwork and in discussions with executive management, the IRS stated that other internal management controls are in place to ensure that invoices are properly expensed and to prevent over spending. In addition, the IRS provided additional support and explanation on some of the issues previously identified; however, TIGTA did not have sufficient time to review the information in-depth for issuance of this report.

Stakeholder involvement was not clearly documented and maintained

The SPIIDE Project team could not provide sufficient documentation to support stakeholders' involvement in the development to implement the DLP solution. IRM 2.16.1.2.2.5.1, *Milestone Readiness Reviews*, requires the assurance that stakeholders and process owners participated in the development of a system. This can be supported by: 1) examining attendance lists and reviewer comment forms for each key deliverable, 2) resolving reviewer comments satisfactorily, and 3) completing the appropriate checklists for the current phase.

We reviewed the minutes from the SPIIDE Project team biweekly meetings for stakeholders' attendance and other key deliverables for the stakeholders' comments. The minutes only documented stakeholders who were invited to the meetings, rather than who attended the meetings and their expressed comments. The SPIIDE Project team stated that they provided the minutes from the meetings to the stakeholders, who subsequently provided comments that were incorporated into the key deliverables. However, the SPIIDE Project team did not maintain the original comments from the stakeholders.

Without documented stakeholders' comments, no assurance exists that stakeholders verified the DLP solution for its completeness, correctness, and consistency in the previous milestone phases.

Recommendations

To ensure that the SPIIDE Project meets its new DLP solution implementation date and budget requirements, the Chief Technology Officer should:

Recommendation 1: Associate fully implementing the DLP solution with meeting the recommended component requirement for the Administration's TIC initiative when competing for and securing additional funding and dedicated information technology resources.

> ***Management's Response:*** The IRS agreed with this recommendation. The IRS plans to implement the DLP DIM solution by August 2015 to the extent funding is provided.

Recommendation 2: Ensure that the SPIIDE Project team conducts a risk-based analysis on volume and impact on the system by adding a new criterion to the DLP solution that includes the key word "TIN." In addition, ensure that the DLP solution is upgraded to the most current version available to identify SSNs in embedded comments in the Microsoft Office 2007 application files, especially in the Excel spreadsheets.

> ***Management's Response:*** The IRS agreed with this recommendation. The SPIIDE Project team plans to conduct a risk-based analysis for adding a new criterion to the DIM solution for "TIN" in 2015. In addition, the IRS plans to upgrade the DLP solution plan in 2016 to the extent funding is provided.

Recommendation 3: Ensure that the SPIIDE Project team, with the assistance of the contracting officer's representative, reconciles the DLP solution funding and expenses and resolves discrepancies identified during the audit.

> ***Management's Response:*** The IRS agreed with this recommendation. The SPIIDE Project team plans to work with the contracting officer's representative to reconcile discrepancies identified during the audit, to the extent resources are available.
>
> ***Office of Audit Comment:*** IRS management's response specified that the SPIIDE Project team will work to reconcile the discrepancies identified during the audit as its corrective action; however, its implementation appears to be contingent upon the availability of resources. Because we identified and reported discrepancies that ranged from $1,200 to more than $3.3 million, we believe the IRS should resolve all discrepancies identified during the audit to ensure accurate reporting of DLP solution funding and expenses, without regard for the availability of resources.

Recommendation 4: Coordinate with the contracting officer's representative and Information Technology Financial Management Services to ensure that processes are in place and accounting entries are accurate as they pertain to the SPIIDE Project. This will assist the SPIIDE Project with properly accounting for dollars spent and provide assurance that sufficient funding remains to implement the initial release of the DLP solution by December 2014.

Management's Response: The IRS agreed with this recommendation. Information Technology Financial Management Services has internal management processes in place to ensure that invoices are properly expensed and to prevent over spending. Information Technology Financial Management Services plans to ensure that those processes are re-communicated to all applicable internal stakeholders.

Office of Audit Comment: IRS management's response addressed ensuring that processes were in place; however, it did not specifically address ensuring that accounting entries are accurate as they pertain to the SPIIDE Project. We reemphasize that all accounting entries should be accurate to ensure proper reporting of DLP solution funding and expenses in light of discrepancies identified in the audit.

Recommendation 5: Ensure that the SPIIDE Project team clearly documents and maintains sufficient information of stakeholder involvement in the future as the SPIIDE Project team continues to implement the DIM and other DLP solution components.

Management's Response: The IRS agreed with this recommendation. The SPIIDE Project team documented stakeholder involvement with the DLP Working Group and the information is stored on the SPIIDE Project SharePoint Site.

Office of Audit Comment: IRS management's response showed the corrective action for this recommendation was implemented on February 24, 2014. During the audit, we made repeated requests to the SPIIDE Project team for documentation of stakeholder involvement, which included the DLP Working Group minutes; however, no additional documentation was provided to demonstrate stakeholder involvement. As such, we are concerned that the recommendation has not been sufficiently addressed.

Data Loss Prevention Solution Processes and Procedures Can Be Enhanced

The Symantec DLP solution generates a new potential PII disclosure event with a preset status of "New" and severity of high, medium, low, or informational. The DLP Operations (Ops) team[8] receives event alerts from the DLP solution and analyzes the event data and artifacts to determine if a PII disclosure incident or attempted disclosure occurred. The event is resolved as a false positive or a nonincident, or it is categorized as a potential incident and referred to proper authorities for further investigation. If the event is a false positive, the DLP Ops team dismisses it, resolves it as a false positive, and provides a reason for the type of error. If the event is a nonincident, the DLP Ops team resolves it as such, provides the reason (which includes personal use, such as employees e-mailing their own PII to their personal e-mail addresses), and any necessary comments. No additional actions are taken with the false positives and nonincidents.

[8] The DLP Ops team is part of the SPIIDE Project team during systems development, but will be independent of the SPIIDE Project team after implementation.

However, if a potential incident is confirmed, the DLP Ops team will follow current established IRS processes and escalate the potential incident, based upon categorization, to the appropriate parties for further analysis and action as either 1) a criminal incident referral to TIGTA, 2) an IRS policy violation incident referral to the IRS Computer Security Incident Response Center (CSIRC), or 3) a broken business process to the business unit liaisons. In the event of a PII disclosure, the potential incident is sent to the PGLD office. If the appropriate party disagrees with the assessment, the potential incident is sent back to DLP Ops team for review until another party accepts the potential incident or the DLP Ops team closes the potential incident. IRS employees and managers respond to inquiries and requirements as mandated by IRS policy.

For the period June 2012 through December 2013, the SPIIDE Project team conducted a pilot and started preproduction testing of the DLP solution. This testing identified 1,903 events. To assess whether the IRS correctly assessed and forwarded potential disclosures of PII detected by the DLP solution, we reviewed a statistically valid stratified random sample of 105 of the 1,903 events.

Events were generally classified correctly during testing

Our analysis of the 105 sampled events showed that the DLP Ops team correctly classified 99 (94 percent) events as false positives, nonincidents, or potential incidents. However, for the remaining six (6 percent) events, the DLP Ops team classified these events incorrectly. These exceptions were discussed with the DLP Ops team, and they agreed with our results. The details for the six are below.

- **********1**********1**********. This event should have been referred to the IRS CSIRC for further review and action. The DLP Ops team stated that because this event did not contain an SSN, they ignored the event and wrote a policy to ignore similar events. However, they agreed that this event should have been forwarded to the IRS CSIRC or the business owner.
- Three e-mails were classified as nonincidents and were not referred to any event responders. Two of the e-mails contained files with passwords to various IRS databases and systems and should have been referred to the IRS CSIRC. The DLP Ops team explained that at the time when these events were reviewed, they were not referring events with system passwords to the IRS CSIRC, although they are referring them now. The remaining e-mail was sent from the IRS website to the TIGTA Office of Investigations and should have been referred to the IRS CSIRC.
- Two e-mails were classified as potential incidents that were closed as business processes and forwarded to the business unit liaisons for additional review. However, the number in one of the e-mails did not meet the pattern of a valid SSN. The remaining e-mail contained the PII of an IRS employee who disclosed the employee's information, which the IRS does not consider a disclosure. These two e-mails should have been classified as

false positive and nonincident, respectively. The DLP Ops team agreed that these two events were misclassified as business processes.

Established procedures did not always allow potential incidents to be forwarded to the PGLD office for reporting during testing

Our further analysis of the 105 sampled events showed that the DLP Ops team appropriately classified 30 events as potential incidents. For 13 (43 percent) of the 30 potential incidents, they were forwarded to the required responders. The remaining 17 (57 percent) potential incidents were forwarded to only one event responder based on established procedures, but should have also been forwarded to and/or accepted by the PGLD office. The details of the 17 potential incidents and the results of our discussions with the DLP Ops team are below.

- Seven potential incidents were reported to the business unit liaisons for further review and action. These involved IRS employees sending outgoing e-mails containing the names and SSNs of 104 taxpayers. The DLP Ops team stated that these seven potential incidents remain in the DLP inventory because the liaisons have not been trained and cannot work (review and resolve) the potential incidents until Union negotiations have been completed. The SPIIDE Project team anticipates training the business unit liaisons by August 2014.
- Four potential incidents were referred to a DLP Ops team lead analyst for further review and actions but have not been reviewed since September 11, 2013. When we asked why the potential incidents have not been reviewed, the DLP Ops team shared that they plan to forward them to the business unit liaisons, again, once they have been trained.
  - **********1**********. A quick search of the DLP solution system identified eight additional unencrypted e-mails from this same group e-mail account.
  - Three involved e-mails from IRS employees who sent unencrypted e-mails containing **********3**********.
- Three potential incidents were closed to the DLP Ops team as a business process and no further actions were taken. **********1**********.
- **********1**********.

- **********1**********
**********1**********
*1**. The SPIIDE Project team stated that they reconfigured the DLP solution to ignore the undeliverable e-mails from the IRS's postmaster server after discussing it with the IRS CSIRC. We believe that while reconfiguring the DLP solution to ignore the undelivered e-mails reduces the number of events for the DLP Ops team to review, it does not prevent the disclosure from occurring. When an unencrypted e-mail is not delivered, PII may still be disclosed when communication is made with the recipient's e-mail server. The recipient e-mail server could potentially have captured information from the body of the e-mail, despite it being undelivered to the intended recipient.

The seven potential incidents previously identified were referred to the PGLD office but were returned to the DLP Ops team because they did not meet PGLD criteria for a disclosure. The PGLD's disclosure definition provides that:

> *An unauthorized disclosure is a situation that occurs when an IRS employee discloses SBU information, including PII, to someone who is not authorized or does not have a legitimate business use for that information, and has the potential for identity theft. Examples of events to be sent to PGLD with the purpose of assessing the risk of ID theft or other harm as required by OMB 07-16:*
>
> - *Unencrypted, unblocked transmission, containing SBU/PII, sent to an unintended, unauthorized recipient, or one without a legitimate business use for that information.*
> - *Unencrypted, unblocked transmission, containing SBU/PII, and the DLP Ops team is unable to determine if the recipient is unintended or unauthorized after reasonable research.*

We believe that the PGLD office should have received and/or accepted the 17 potential incidents because sending unencrypted e-mails provides an opportunity for individuals other than the intended recipient to have access to the enclosed PII. A PGLD executive stated that it was not the PGLD office's current policy to treat unencrypted e-mails with PII sent to the intended recipient as a disclosure, and it might need to revise its policy. In a February 2011 TIGTA report,[9] the issue with sending unencrypted e-mails by employees, taxpayers, and taxpayer representatives was addressed. The report highlighted the IRS's internal procedures, guides, and training briefings in that they do not provide adequate guidance or instructions to employees to report violations of unencrypted e-mails with SBU data from employees or taxpayers. However, our research identified subsequent internal guidance effective July 8, 2011,[10] with a warning that employees should never consider e-mail secure, and they should not include taxpayer, SBU, or PII information in e-mail messages or attachments unless IRS-approved encryption technology is

[9] TIGTA, Ref. No.2011-20-012, *Additional Security Is Needed for the Taxpayer Secure E-mail Program* p. 12 (Feb. 2011).
[10] IRM 1.10.3.2.1(3) and (7), *Secure Messaging and Encryption*.

being used or an exception is approved by the Information Technology organization. We are not aware of any exceptions approved by the Information Technology organization for the SPIIDE Project, especially when the project's purpose is to protect SBU data.

Based on our findings on the 17 potential incidents, we believe that the PGLD office should have advised the affected parties of the disclosure and offered credit monitoring services in 11 of the 17 potential incidents. In the remaining six incidents, the PGLD office did not need to contact the individuals because they either disclosed their own PII or may have been the subject of a tax or criminal review. In addition, OMB procedures and the Treasury Incident Reporting and Guidelines Procedures[11] require the IRS to report PII disclosures to the Treasury CSIRC. We believe these 17 potential incidents should have also been reported.

Based upon projections from our sample, we estimate that 308 of the 1,903 potential incidents met the OMB PII disclosure reporting requirements and were not reported to the PGLD office and later to the Treasury CSIRC. In addition, we estimate that the individuals whose PII was disclosed in 199 of the 308 potential incidents were not contacted and offered credit monitoring services.[12]

Employees violated policies by providing and responding to tax information in e-mails during testing

While we understand that the SPIIDE Project and the DLP Ops teams are working through and refining the DLP solution process and procedures, we identified an additional condition that warrants the DLP Ops team's attention as they finalize their guidelines to comply with Federal guidelines. We identified 11 potential incidents that involved employees providing tax account information and replying to the original e-mail that contained unencrypted PII from tax preparers or other Government agencies. These 11 potential incidents remain in the DLP solution inventory and have not been referred to the business liaisons to be worked. Although the initiators of the e-mails may have been authorized to receive the information, the employees violated policy by sending unencrypted e-mails with PII outside the IRS. It appears that three of these 11 potential incidents were incoming e-mails sent directly to the employees from taxpayer representatives requesting tax account information.

Employees should not respond to requests for tax return information that are not received through official channels, such as taxpayer walk-in offices, telephone contact, or cases assigned by managers. We attempted to search the DLP solution for similar incidents. However, we could not easily identify any additional events, including those involving tax preparers, because

[11] Department of the Treasury Incident Reporting and Guidelines Procedures Version 4.0 June 15, 2011.
[12] 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 177 and 439 potential incidents that were not reported to the PGLD office and the Treasury CSIRC. In addition, we are 95 percent confident that the point estimate is between 90 and 308 that the PGLD office should have contacted the individuals affected by the unencrypted disclosures to offer them credit monitoring services.

the SPIIDE Project team did not add an attribute in the DLP solution to readily identify e-mails from tax preparers.

The OMB has issued specific guidance for Federal agencies to follow concerning disclosure and actions to be taken when suspected or confirmed breaches of PII occur. OMB M-06-19, *Reporting Incidents Involving Personally Identifiable Information and Incorporating the Cost for Security in Agency Information Technology Investments*,[13] requires agencies to report all suspected or confirmed incidents involving PII in electronic or physical form to the U.S. Computer Emergency Readiness Team within one hour of discovering the incident. The OMB also requires the reporting of PII incidents even when there is no risk of identity theft. Additionally, OMB M-07-16, *Safeguarding Against and Responding to the Breach of Personally Identifiable Information*,[14] provides a framework to reduce the risks related to data breaches of PII. Included in this framework is the use of encryption, strong authentication procedures, and other security controls to make information unusable by unauthorized individuals.

Taxpayers have the right to expect that any information they provide to the IRS will not be disclosed unless authorized by the taxpayer or by law, and to expect appropriate action will be taken against employees, return preparers, and others who wrongfully use or disclose taxpayer return information.

Furthermore, the IRS has specific internal requirements for providing information to the public. IRM 11.3.2.6, *Methods for Communication of Confidential Information*, allows employees to disclose tax information to a taxpayer, his or her legal representative, or a designated third party. However, disclosure is prohibited by e-mail even if the requester asked to submit the tax information via e-mail. Although the requester has a legal right to that information, e-mail is not an approved secure method. IRM 11.3.1.14.2, *Electronic Mail and Secure Messaging*, provides that employees may not use e-mail to transmit SBU data (including PII) to parties outside of the IRS, including other Government agencies, taxpayers, or their representatives, even if specifically authorized by the taxpayer, unless the employees use the IRS Secure Messaging system. In addition, IRM 10.5.5.3, *Covered Relationships and Official Channels*, states that employees are not allowed access to return information when the request is received through unofficial channels, such as requests from individuals at social functions and nonwork environments, and requests received from close friends, relatives, neighbors, or co-workers. Lastly, the IRS recently adopted the Taxpayer Bill of Rights. In these provisions, taxpayers have the right of confidentiality and can expect the IRS to only disclose information when authorized by the taxpayer and take

[13] Office of Management and Budget, OMB Memorandum M-06-19, *Reporting Incidents Involving Personally Identifiable Information and Incorporating the Cost for Security in Agency Information Technology Investments* (July 2006).
[14] Office of Management and Budget, OMB Memorandum M-07-16, *Safeguarding Against and Responding to the Breach of Personally Identifiable Information* (May 2007).

appropriate action against employees, tax return preparers, and others who wrongfully use or disclose taxpayer return information.

Breaches involving PII can receive considerable media attention, which can greatly harm the public's trust in the IRS. Failure to report all potential incidents involving PII disclosure to the appropriate IRS functions in a timely manner decreases the IRS's ability to respond quickly and effectively to report potential incidents to the Treasury CSIRC and to offer remedial services, such as credit monitoring, to affected individuals. Furthermore, noncompliance or delayed compliance can also result in substantial harm, embarrassment, and inconvenience to the affected individuals and could lead to identity theft, blackmail, or other fraudulent use of the information. Lastly, responding to requests for tax account information received from an unofficial channel can give the appearance of partiality and the perception of providing expedited or preferential treatment that is unavailable to the general public.

The DLP Ops team is not reporting tax preparers who violate disclosure rules during testing

The DLP Ops team is not reporting employee outbound reply e-mails originating from tax preparers who included taxpayer PII in inbound unencrypted e-mails as disclosure to the Office of Professional Responsibility (OPR). In our sample of 105 events, we identified three events in which employees replied to e-mails from tax preparers who sent taxpayer PII requesting tax account information. Although these e-mails did not originate from the IRS employees, the inbound e-mails still contained PII. As previously mentioned, we could not easily identify any additional events involving tax preparers because the SPIIDE Project team did not add an attribute in the DLP solution to readily identify e-mails from tax preparers.

The three events should have been classified as potential incidents and referred to the business unit liaisons and subsequently forwarded only the potential incidents involving a tax preparer who is also a licensed tax practitioner to the OPR. Tax preparers who are permitted to practice before the IRS are considered Circular 230 practitioners (hereafter referred to as licensed tax practitioners). The OPR can educate licensed tax practitioners of their responsibility to secure and protect their clients' tax return information and to correct their behavior of sending taxpayer PII by unencrypted e-mail. In addition, an executive from the OPR stated a referral to the OPR would be appropriate if the business unit liaison determines that a tax preparer who sent a prohibited e-mail is a licensed tax practitioner, such as an attorney, certified public accountant, or enrolled agent.

Unencrypted e-mails containing PII can lead to identity theft.

The OPR has the authority to ensure that all licensed tax practitioners adhere to professional standards and follow the law. Licensed tax practitioners have the responsibility to secure and protect taxpayer PII from disclosure. They must also abide by Internal Revenue Code Section 7216 by not recklessly, knowingly, or unknowingly disclosing taxpayer information. The National Institute for

Standards and Technology recommends that agencies implement automated tools to monitor transfers of PII and to monitor inbound and outbound communications.

We presented our concerns to the SPIIDE Project team, and they stated that they were not aware of the OPR's responsibilities and that tax preparers were violating their obligations to secure and protect taxpayer information. As a result, the SPIIDE Project team had not included the OPR as an event responder for handling these cases. The SPIIDE Project team stated that they will reconsider monitoring unencrypted inbound e-mail traffic after the DLP solution is initially deployed and operational. In the meantime, the DLP Ops team will incorporate identifying and routing such potential incidents to the appropriate event responders into current policy and procedures.

When faced with a security incident, an agency must be able to respond in a manner protecting both its own information and helping to protect the information of others who might be affected by the incident. The IRS may be exposing itself to lose trust with the American public and exposing taxpayers to potential identity theft and fraud. Additionally, the OPR loses an opportunity to correct the behavior of registered tax preparers, enrolled agents, and licensed tax practitioners who are not protecting their clients' tax return information as required.

Recommendations

To enhance the processes and procedures over the DLP solution, the Chief Technology Officer should:

Recommendation 6: Ensure that the SPIIDE Project team trains the DLP Ops team to forward potential incidents to the appropriate event responders and trains business unit liaisons to immediately start reviewing the potential incidents and then take appropriate action, when necessary (after Union negotiations are completed in regard to DLP solution implementation).

> ***Management's Response:*** The IRS agreed with this recommendation. The SPIIDE Project team trained the DLP Ops team to forward potential incidents to the appropriate event responders and business unit liaisons to immediately start reviewing the potential incidents and then take appropriate action, when necessary.

Recommendation 7: Change the forwarding procedures to refer all unencrypted e-mails containing PII to the PGLD office first and then to the business unit liaisons to ensure that all potential PII disclosure incidents are timely reported to the Treasury CSIRC.

> ***Management's Response:*** The IRS agreed with this recommendation. Events determined to be unencrypted PII exiting IRS network protection will be reviewed by the PGLD office's Incident Management team within the SPIIDE Project application and they plan to notify Treasury CSIRC when appropriate. In addition, the SPIIDE Project team plans to update the event management workflow.

Recommendation 8: Conduct an analysis to determine whether to remove the reconfiguration that ignores the undeliverable e-mails to allow the DLP solution to identify these events. The identification of similar e-mails will provide the IRS with an opportunity to notify the affected parties of the disclosure and report it to the Treasury CSIRC.

> ***Management's Response:*** The IRS agreed with this recommendation. The IRS plans to conduct an analysis to determine whether to remove the reconfiguration that ignores the undelivered e-mails in the DLP solution production system.

Recommendation 9: Ensure that the SPIIDE Project team adds an additional attribute to identify tax preparers to the advance search criteria to allow for easy identification of events involving tax preparers in outbound unencrypted e-mails containing PII.

> ***Management's Response:*** The IRS agreed with this recommendation. The current DLP solution does not have the ability to correctly identify tax preparers via an automated search criterion. In lieu of this, a modification has been made to the DLP solution reason codes to allow for event responders to classify an event involving tax preparers.

Recommendation 10: Incorporate a process to forward outbound unencrypted e-mail traffic with PII from licensed tax preparers/taxpayer representatives to the OPR through the business unit liaisons into the current policy and procedures. After the DIM component of the DLP solution is deployed and operational, conduct a risk-based analysis to determine the feasibility on the monitoring and identifying of unencrypted inbound e-mail traffic with PII from these licensed tax practitioners to route to the OPR.

> ***Management's Response:*** The IRS partially agreed with this recommendation. The SPIIDE Project team plans to enhance the processes and procedures to forward outbound unencrypted e-mail traffic with PII from licensed tax preparers/taxpayer representatives to the OPR through the business unit liaison. The IRS disagreed with the part of the recommendation regarding inbound e-mail. The requirement to implement a DLP solution as defined in Treasury Directive 85-01 is to prevent the outbound transmission of unencrypted information from the Treasury. This expansion to review and monitor inbound e-mail traffic for unencrypted SSNs from licensed tax practitioners is not currently feasible or cost effective for the IRS. For example, no source of valid e-mail addresses for licensed tax practitioners currently exists.
>
> ***Office of Audit Comment:*** While the IRS's statement regarding the Treasury Directive's requirement is valid, we stated in the report that the National Institute for Standards and Technology recommends that agencies implement automated tools to monitor transfers of PII and to monitor inbound and outbound communications. However, we concur with IRS management's rationale for not implementing the inbound portion of the recommendation.

Recommendation 11: Coordinate with the business units to ensure that their employees follow the IRM procedures that require the use of the IRS Secure Messaging system when sending SBU/PII information to tax preparers, other Government agencies, and taxpayers.

> ***Management's Response:*** The IRS agreed with this recommendation. The IRS plans to redistribute an IRS-wide communication on authorized encryption procedures for SBU/PII to ensure that employees follow the IRM procedures.

We also recommend that the Director, Privacy, Governmental Liaison, and Disclosure, should:

Recommendation 12: Revise the disclosure acceptance criteria to ensure that all potential PII disclosure incidents are reported to the Treasury CSIRC within the required time period and that affected parties are timely notified.

> ***Management's Response:*** The IRS disagreed with this recommendation. The acceptance criteria used by the PGLD office's Incident Management team adheres to OMB and National Institute of Standards and Technology requirements for the reporting of inadvertent disclosures. The PGLD office's Incident Management team will review SPIIDE Project-identified events in conjunction with the business liaisons and the DLP Ops team and report appropriate items to the Treasury CSIRC. When applicable, a risk assessment will be performed and potentially affected individuals notified in accordance with existing direction.
>
> ***Office of Audit Comment:*** IRS management disagreed with our recommendation because they believe the PGLD office's acceptance criteria adhered to existing Federal Government guidance. We contend that the acceptance criteria did not address the exceptions identified during our audit. Specifically, we found employees responding with tax information in unencrypted e-mails. During the audit, the PGLD office stated that its office's current policy was not to treat unencrypted e-mails with PII sent to the intended recipient as a disclosure. However, as we reported, IRS policy, which has been in effect since March 7, 2008, prohibits communicating confidential information using e-mail other than through the Secure Messaging system. As such, the use of unencrypted e-mails outside of the IRS violates policy and should be included in the acceptance criteria so that the PGLD office can evaluate any possible actual disclosures due to the possible interception of unencrypted e-mails.

Appendix I

Detailed Objective, Scope, and Methodology

The overall objective of this review was to determine whether the SPIIDE Project is developing a data loss prevention and protection solution for implementation in accordance with applicable policies and procedures and within budget to safeguard sensitive data. To accomplish our objective, we:

I. Determined whether the development of the SPIIDE Project properly followed commercial off-the-shelf enterprise life cycle[1] procedures in accordance with Treasury, OMB, IRM, and other applicable guidelines.

   A. Determined whether the SPIIDE Project completed required key deliverables through the current milestone. In addition, we reviewed OMB and Treasury guidance to determine the requirements for the IRS to develop and implement a breach notification policy, to eliminate or reduce the unnecessary use of SSNs, and to implement additional controls in the cybersecurity environment.

   B. Determined whether system security controls have been considered and planned in the design of the SPIIDE Project.

      1. Determined whether security issues and risks were identified, tracked, and being addressed from project inception.

      2. Selected a statistically valid random sample of the SPIIDE Project's limited testing results[2] to determine if the IRS took appropriate actions to report the potential breaches. We used a 95 percent confidence level, an 8 percent expected error rate, and a ± 7 percent precision level. We took a statistically valid random sample because we wanted to project the number of events not reported properly over the population of all 1,903 events identified from June 2012 through December 2013.

      3. Used TIGTA's contracted statistician to review the sampling plan and to develop projections.

      4. Conducted independent testing of the DLP solution to determine whether the system is capable of identifying unencrypted e-mails containing PII.

   C. Determined the frequency of stakeholders' involvement in the SPIIDE Project.

[1] See Appendix V for a glossary of terms.
[2] We used the limited testing results and determined the accuracy of the DLP solution capabilities for identifying PII, which are included in this report.

II. Determined whether the SPIIDE Project is effectively and efficiently managing funds allocated for the implementation of the Symantec DLP solution by obtaining total cost, from inception to date, by category for the SPIIDE Project from the project manager or other responsible IRS officials.

III. Determined the U.S. Department of State and U.S. Postal Service's experience with the development and cost of implementing the Symantec DLP solution to identify best practices to share with the IRS's SPIIDE Project team.

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: Treasury Directives, and OMB, IRM, and National Institute for Standards and Technology guidelines for implementing an automatic tool to monitor transfers of PII and for developing a commercial off-the-shelf product. We evaluated these controls by interviewing Treasury, U.S. Department of State, and U.S. Postal Service officials; IRS procurement and budget personnel; the SPIIDE Project team; and an enterprise life cycle coach, and by reviewing enterprise life cycle commercial off-the-shelf artifacts and documents supporting the procurement, budget, and expenses for the DLP solution.

Appendix II

Major Contributors to This Report

Alan R. Duncan, Assistant Inspector General for Audit (Security and Information Technology Services)
Kent Sagara, Director
Deborah Smallwood, Audit Manager
Cindy Harris, Lead Auditor
Cari Fogle, Senior Auditor
Louis Lee, Senior Auditor

Appendix III

Report Distribution List

Commissioner C
Office of the Commissioner – Attn: Chief of Staff C
Deputy Commissioner for Operations Support OS
Deputy Commissioner for Services and Enforcement SE
Chief Financial Officer OS:CFO
Director, Office of Professional Responsibility SE:OPR
Director, Privacy, Governmental Liaison, and Disclosure OS:P
Director, Risk Management Division OS:CTO:SP:RM
Chief Counsel CC
National Taxpayer Advocate TA
Director, Office of Legislative Affairs CL:LA
Director, Office of Program Evaluations and Risk Analysis RAS:O
Office of Internal Control OS:CFO:CPIC:IC
Audit Liaisons:
- Chief Financial Officer OS:CFO
- Chief Technology Officer OS:CTO
- Director, Office of Professional Responsibility SE:OPR
- Director, Privacy, Governmental Liaison, and Disclosure OS:P

Appendix IV

Outcome Measure

This appendix presents detailed information on the measurable impact that our recommended corrective action 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; 308 potential incidents[1] of PII and tax account disclosures (see page 12).

Methodology Used to Measure the Reported Benefit:

We selected and reviewed a statistically valid random sample of 105 events identified by the DLP solution system. We selected the sample from the population of 1,903 events that were identified during the period of June 1, 2012, through December 31, 2013. We used a confidence level of 95 percent, a precision level of ± 7 percent, and an expected error rate of 8 percent to select the sample.

Our results showed that 17 (16.19 percent) of 105 events were not forwarded to all of the required responders. These 17 events, which are potential incidents, should have been forwarded to and/or accepted by the PGLD office as PII disclosures. In addition to reporting the potential incidents to the PGLD office, the 17 potential incidents should have been reported to the Treasury CSIRC as PII disclosures as required by OMB procedures. Furthermore, the PGLD office should have advised the affected parties of the disclosure and offered credit monitoring services in 11 of the 17 potential incidents.

We project[2] that an estimated 308 potential incidents that met the OMB PII disclosure reporting requirements were not reported to the PGLD office and later to the Treasury CSIRC. In addition, we project that the individuals whose PII was disclosed in 199 of the 308 potential incidents were not contacted and offered credit monitoring service.

[1] See Appendix V for a glossary of terms.
[2] The point estimate is based on a two-sided 95 percent confidence interval. We are 95 percent confident the point estimate is between 177 and 439 potential incidents that were not reported to the PGLD office and the Treasury CSIRC. In addition, the point estimate is between 90 and 308 potential incidents that the PGLD office should have contacted the individuals affected by the unencrypted disclosures and offered them credit monitoring services.

Appendix V

Glossary of Terms

Term	Definition
Baseline	A baseline consists of a specified set of documents, software, and other items defined as final (or point-in-time) products for a project. A baseline establishes a predefined point from which to evaluate project progress.
Business Unit	A title for major IRS organizations such as Appeals, Wage and Investment, the OPR, and Information Technology.
Circular 230 Practitioner	Any individual described as an attorney, certified public accountant, enrolled agent, enrolled actuary, enrolled retirement plan agent, and registered tax return preparer that is permitted to practice before the IRS. The IRS OPR is responsible for all matters related to practitioner conduct, discipline, and practice before the IRS under 31 Code of Federal Regulations part 10 (Circular 230).
Clear Text	Information that is not encrypted.
Compact Disk	A compact disk is a small, portable, round medium made of molded polymer for electronically recording, storing, and playing back audio, video, text, and other information in digital form.
Computer Security Incident Response Center	A group of individuals usually consisting of security analysts organized to develop, recommend, and coordinate immediate mitigation actions for containment, eradication, and recovery resulting from computer security incidents.
Customer Account Data Engine 2	The Customer Account Data Engine 2 leverages existing IRS systems and components to perform functions related to accessing and updating taxpayer account data, managing cases, and resolving account issues. It will implement a single system that uses a relational database to process accounts on a daily basis.
Data Center Warehouse	A collection of IRS databases containing various types of taxpayer account information that is maintained by TIGTA for the purpose of analyzing data for ongoing audits.

Term	Definition
Default Administrator Account	A default administrator account is a user account already created on the operating system (by default) that allows the administrator to make changes that will affect other users. Administrators can change security settings, install software and hardware, access all files on the computer, and make changes to other user accounts.
Development, Integration, and Test Environment	A controlled environment used to create, modify, integrate, and test configuration items, information technology services, applications, releases, processes, *etc*.
Disclosure	The making known to any person, in any manner, a return or return information.
Driver	A driver is a program that interacts with a particular device or special kind of software. The driver contains the special knowledge of the device or special software interface that programs using the driver do not.
Encryption	The process of converting plain text to cipher text by means of a cryptographic system.
Enterprise Life Cycle	The enterprise life cycle establishes a set of repeatable processes and a system of reviews, checkpoints, and milestones that reduce the risks of system development and ensure alignment with the overall business strategy.
False Positive	A false positive is a test result which incorrectly indicates that a particular condition or attribute is present. For example, a nine-digit ZIP code could be misconstrued as an SSN.
Filing Season	The period from January through mid-April when most individual income tax returns are filed.
Financial Management Service	An Office that supports IRS Information Technology by formulating and executing budgets, preparing clear financial policy, and providing financial services to the Associate Chief Information Officers. In addition, it serves as the link to the Chief Financial Officer and represents Information Technology's funding needs to Corporate IRS.

Term	Definition
Incident	An incident is an occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability of an information system or the information the system processes, stores, or transmits. Also, an incident could constitute a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies.
Integrated Financial System	An administrative accounting system used by the IRS.
Integrated Procurement System	A program that tracks all incoming commitment requests and captures the information necessary to process acquisition actions including purchase orders, delivery orders, task orders, contract awards, interagency agreements, and associated modifications.
Live Data Waiver	The IRS prohibits the use of live data without approval from the Office of Privacy, Information Protection, and Data Security. Live data shall be used only when other alternatives, such as sanitized live data or synthetic data, cannot be used to complete a business process or other assigned official duties, and live data waiver must be prepared for such use.
Milestone	Milestones provide for "go/no-go" decision points in a project and are sometimes associated with funding approval to proceed.
National Institute for Standards and Technology	Founded in 1901, the National Institute for Standards and Technology is a nonregulatory Federal agency within the U.S. Department of Commerce. Its mission is to promote U.S. innovation and industrial competitiveness by advancing measurement science, standards, and technology in ways that enhance economic security and improve our quality of life.
Permissions	A system administrator defines for the system which users are allowed access to the system and what privileges of use, such as access to which file directories, hours of access, and amount of allocated storage space.

Term	Definition
Plug and Play	Plug and play is a phrase used to describe devices that work with a computer system as soon as they are connected. The user does not have to manually install drivers for the device or even tell the computer that a new device has been added. Instead, the computer automatically recognizes the device, loads new drivers for the hardware (if needed), and begins to work with the newly connected device.
Privilege	A right granted to an individual, a program, or a process.
Sensitive But Unclassified	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 Section 552a (the Privacy Act), which could result from inadvertent or deliberate disclosure, alteration, or destruction.
Separation of Duties	Key duties and responsibilities need to be divided or segregated among different people to reduce the risk of error or fraud.
SharePoint Site	A platform from Microsoft that is used to create intranets (internal websites) for team collaboration, blogs, wikis, and company news. It is also commonly deployed to extend certain information to customers via password-protected websites.
Subject Matter Expert	A subject matter expert is an individual who understands a business process or area well enough to answer questions from people in other groups who are trying to help. It is most commonly used to describe the people who explain the current process to information technology and then answer their questions as they try to build a technology system to automate or streamline the process.
Taxpayer Bill of Rights	The Taxpayer Bill of Rights takes the multiple existing rights embedded in the tax code and groups them into 10 broad categories that include the Right to Be Informed and the Right to Privacy.
Thumb Drive	An external hard disk drive or optical disk drive that plugs into the universal serial bus port.

Term	Definition
Trusted Internet Connection	The primary goals of the TIC initiative are to consolidate and secure Federal agency external connections using a common set of security controls and to improve the Federal Government's incident response capability. To achieve these goals, the initiative has the objectives to 1) reduce and consolidate external connections, including connections to the Internet, across the Federal Government; 2) define and maintain baseline security capabilities at TIC access points; and 3) establish a compliance program to monitor agency adherence to TIC policy.
User Seat License	Licensed software on a server may only be accessed by those who have been granted a seat, also referred to as a seat license. Those with a seat license are identified in the system directory; only they can access the protected software. Thus, each user computer is considered a seat.

Appendix VI

Management's Response to the Draft Report

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

CHIEF TECHNOLOGY OFFICER

SEP 09 2014

MEMORANDUM FOR DEPUTY INSPECTOR GENERAL FOR AUDIT

FROM: Terence V. Milholland
Chief Technology Officer

SUBJECT: Draft Audit Report – While Data Loss Prevention (DLP) Solution Is Being Developed, Stronger Oversight and Process Enhancements Are Needed for Timely Implementation Within Budget (Audit # 201420024) (e-trak #2014-58500)

Thank you for the opportunity to review your draft audit report and meet with the audit team to discuss earlier report observations. We are pleased that your report acknowledged that the IRS's Safeguarding Personally Identifiable Information Data Extracts (SPIIDE) project team is progressing in its development and implementation of the Data Loss Prevention (DLP) solution. In addition, the report noted that the team completed key required enterprise life cycle deliverables and was identifying and addressing security weaknesses as they are detected.

The security and privacy of taxpayer information is of the utmost importance to us, and your report recommendations will further assist us in mitigating security risks. We totally agree with ten of the 12 report recommendations. We partially agree with recommendation #10, and we disagree with recommendation #12.

Specifically, for recommendation #10, we agree with the part that addresses outbound email; however, we disagree with the part regarding inbound email. The Treasury requirement to implement a DLP solution is to prevent the outbound transmission. The expansion to review and monitor inbound email traffic is not currently feasible or cost effective for the IRS.

For recommendation #12 regarding disclosure acceptance criteria, the IRS acceptance criteria adheres to both the Office of Management and Budget and the National Institute of Standards and Technology requirements for reporting inadvertent disclosures. The attachment to this memo details our planned corrective actions to implement audit report recommendations, and provides additional details about the recommendations we partially agree with, #10, and the one we disagree with, #12.

Draft Audit Report – While the Data Loss Prevention Solution Is Being Developed, Stronger Oversight and Process Enhancements Are Needed for Timely Implementation Within Budget (Audit # 201420024) (e-trak #2014-58500)

RECOMMENDATION #1: To ensure that the Safeguarding Personally Identifiable Information Data Extracts (SPIIDE) Project meets its new Data Loss Prevention (DLP) solution implementation date and meets its budget requirements, the Chief Technology Officer should associate fully implementing the DLP solution with meeting the recommended component requirement for the Administration's Trusted Internet Connection (TIC) initiative when competing for and securing additional funding and dedicated information technology resources.

CORRECTIVE ACTION #1: The IRS agrees with this recommendation. The IRS will implement the DLP Data-in-Motion (DIM) solution by August 2015 to the extent funding is provided.

IMPLEMENTATION DATE: August 25, 2015

RESPONSIBLE OFFICIALS: 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: To ensure that the SPIIDE Project meets its new DLP solution implementation date and meets its budget requirements, the Chief Technology Officer should ensure that the SPIIDE team conducts a risk-based analysis on volume and impact on the system by adding a new criterion to the DLP solution that includes the key word "Taxpayer Identification Number (TIN)." In addition, ensure that the DLP solution is upgraded to the most current version available to identify social security numbers (SSNs) in embedded comments in the Microsoft Office 2007 application files, especially in the Excel spreadsheets.

CORRECTIVE ACTION #2: The IRS agrees with this recommendation. A risk-based analysis for adding new criterion to the Data-in-Motion solution for TIN will be conducted in 2015. In addition, the DLP solution will be upgraded in 2016 to the extent funding is provided.

IMPLEMENTATION DATE: July 25, 2016

RESPONSIBLE OFFICIALS: 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.

Draft Audit Report – While the Data Loss Prevention Solution Is Being Developed, Stronger Oversight and Process Enhancements Are Needed for Timely Implementation Within Budget (Audit # 201420024) (e-trak #2014-58500)

RECOMMENDATION #3: To ensure that the SPIIDE Project meets its new DLP solution implementation date and meets its budget requirements, the Chief Technology Officer should ensure that the SPIIDE team, with the assistance of the contracting officer's representative, reconciles the DLP funding and expenses and resolves discrepancies identified during the audit.

CORRECTIVE ACTION #3: The IRS agrees with this recommendation. The SPIIDE team will work with the contracting officer's representative to reconcile discrepancies identified during the audit, to the extent resources are available.

IMPLEMENTATION DATE: June 25, 2015

RESPONSIBLE OFFICIALS: 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 #4: To ensure that the SPIIDE Project meets its new DLP solution implementation date and meets its budget requirements, the Chief Technology Officer should coordinate with the contracting officer's representative and Information Technology Financial Management Services to ensure processes are in place and accounting entries are accurate as it pertains to the SPIIDE Project. This will assist the SPIIDE Project with properly accounting for dollars spent and provide assurance that sufficient funding remains to implement the initial release of the DLP solution by December 2014.

CORRECTIVE ACTION #4: The IRS agrees with this recommendation. Information Technology Financial Management Services (IT FMS) has internal management processes in place to ensure that invoices are properly expensed and prevent overspending. IT FMS will ensure that those processes are re-communicated to all applicable internal stakeholders.

IMPLEMENTATION DATE: January 25, 2015

RESPONSIBLE OFFICIALS: Director, Financial Management Services

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.

Draft Audit Report – While the Data Loss Prevention Solution Is Being Developed, Stronger Oversight and Process Enhancements Are Needed for Timely Implementation Within Budget (Audit # 201420024) (e-trak #2014-58500)

RECOMMENDATION #5: To ensure that the SPIIDE Project meets its new DLP solution implementation date and meets its budget requirements, the Chief Technology Officer should ensure that the SPIIDE team clearly documents and maintains sufficient information of stakeholder involvement in the future as the SPIIDE team continues to implement the DIM and other DLP solution components.

CORRECTIVE ACTION #5: The IRS agrees with this recommendation. The SPIIDE team documented stakeholder involvement with the DLP Working Group and the information is stored on the SPIIDE SharePoint. This action was completed February 24, 2014.

IMPLEMENTATION DATE: February 24, 2014

RESPONSIBLE OFFICIALS: Associate Chief Information Officer, Cybersecurity

CORRECTIVE ACTION MONITORING PLAN: Not applicable (N/A)

RECOMMENDATION #6: To enhance the processes and procedures over the DLP solution, the Chief Technology Officer should ensure that the SPIIDE Project team trains the DLP Operations (Ops) team to forward potential incidents to the appropriate event responders and trains business unit liaisons to immediately start reviewing the potential incidents and then take appropriate action, when necessary (after Union negotiations are completed in regard to the DLP solution implementation.

CORRECTIVE ACTION #6: The IRS agrees with this recommendation. The SPIIDE team trained the DLP Operations team to forward potential incidents to the appropriate event responders and Business Unit Liaisons to immediately start reviewing the potential incidents and then take appropriate action, when necessary. This action was completed on August 15, 2014.

IMPLEMENTATION DATE: August 15, 2014

RESPONSIBLE OFFICIALS: Associate Chief Information Officer, Cybersecurity

CORRECTIVE ACTION MONITORING PLAN: N/A

Draft Audit Report – While the Data Loss Prevention Solution Is Being Developed, Stronger Oversight and Process Enhancements Are Needed for Timely Implementation Within Budget (Audit # 201420024) (e-trak #2014-58500)

RECOMMENDATION #7: To enhance the processes and procedures over the DLP solution, the Chief Technology Officer should change the forwarding procedures to refer all unencrypted email containing personally identifiable information (PII) to the Privacy Governmental Liaison and Disclosure (PGLD) office first and then to the business unit liaisons to ensure that all potential PII disclosure incidents are timely reported to the Treasury Computer Security Incident Response Center (CSIRC).

CORRECTIVE ACTION #7: The IRS agrees with this recommendation. Events determined to be unencrypted PII exiting IRS network protection will be reviewed by PGLD's Incident Management team within the SPIIDE application and they will notify Treasury CSIRC when appropriate. In addition, the SPIIDE Project team will update the event management workflow.

IMPLEMENTATION DATE: November 25, 2014

RESPONSIBLE OFFICIALS: 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 #8: To enhance the processes and procedures over the DLP solution, the Chief Technology Officer should conduct an analysis to determine whether to remove the reconfiguration that ignores the undeliverable e-mails to allow the DLP Solution to identify these events. The identification of similar e-mails will provide the IRS with an opportunity to notify the affected parties of the disclosure and report it to the Treasury CSIRC.

CORRECTIVE ACTION #8: The IRS agrees with this recommendation. An analysis will be conducted to determine whether to remove the reconfiguration that ignores the undeliverable e-mails in the DLP production system.

IMPLEMENTATION DATE: August 25, 2015

RESPONSIBLE OFFICIALS: Associate Chief Information Officer, Cybersecurity

Draft Audit Report – While the Data Loss Prevention Solution Is Being Developed, Stronger Oversight and Process Enhancements Are Needed for Timely Implementation Within Budget (Audit # 201420024) (e-trak #2014-58500)

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: To enhance the processes and procedures over the DLP solution, the Chief Technology Officer should ensure that the SPIIDE team adds an additional attribute to identify tax preparers to the advance search criteria to allow for easy identification of events involving tax preparers in outbound unencrypted e-mails containing PII.

CORRECTIVE ACTION #9: The IRS agrees with this recommendation. The current DLP solution does not have the ability to correctly identify tax preparers via an automated search criterion. In lieu of this, a modification has been made to the DLP reason codes to allow for event responders to classify an event involving tax preparers. This action was completed on July 1, 2014.

IMPLEMENTATION DATE: July 1, 2014

RESPONSIBLE OFFICIALS: Associate Chief Information Officer, Cybersecurity

CORRECTIVE ACTION MONITORING PLAN: N/A

RECOMMENDATION #10: To enhance the processes and procedures over the DLP solution, the Chief Technology Officer should incorporate a process to forward outbound unencrypted email traffic with PII from licensed tax preparers/taxpayer representatives to the OPR through the business unit liaisons into the current policy and procedures. After the DIM component of the DLP is deployed and operational, conduct a risk-based analysis to determine the feasibility on the monitoring and identifying of unencrypted inbound email traffic with PII from these licensed tax practitioners to route to the Office of Professional Responsibility (OPR).

CORRECTIVE ACTION #10: The IRS partially agrees with this recommendation. We agree with the part of the recommendation addressing outbound email. The SPIIDE team will enhance the processes and procedures to forward outbound unencrypted email traffic with PII from licensed tax preparers/taxpayer representatives to the OPR through the business unit liaisons.

We disagree with the part of the recommendation regarding inbound email. The requirement to implement a DLP solution as defined in Treasury Directive 85-01 is to prevent the outbound transmission of unencrypted information from the Department. This expansion to review and monitor inbound email traffic for unencrypted SSNs from licensed tax practitioners is not currently feasible or cost effective for the IRS. For example, there currently is no source of valid email addresses for licensed tax practitioners.

Draft Audit Report – While the Data Loss Prevention Solution Is Being Developed, Stronger Oversight and Process Enhancements Are Needed for Timely Implementation Within Budget (Audit # 201420024) (e-trak #2014-58500)

IMPLEMENTATION DATE: November 25, 2014

RESPONSIBLE OFFICIALS: 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 #11: To enhance the processes and procedures over the DLP solution, the Chief Technology Officer should coordinate with the business units to ensure that their employees follow the IRM procedures that require the use of the IRS Secure Messaging system when sending SBU/PII information to tax preparers, other Government agencies, and taxpayers.

CORRECTIVE ACTION #11: The IRS agrees with this recommendation. An IRS-wide communication on authorized encryption procedures for SBU/PII will be re-distributed to ensure employees follow the IRM procedures.

IMPLEMENTATION DATE: November 25, 2014

RESPONSIBLE OFFICIALS: 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 #12: We recommend that the Director, Privacy, Governmental Liaison, and Disclosure (PGLD) should revise its disclosure acceptance criteria to ensure that all potential PII disclosure incidents are reported to the Treasury CSIRC within the required time period and that affected parties are timely notified.

CORRECTIVE ACTION #12: The IRS disagrees with this recommendation. The acceptance criteria used by PGLD Incident Management adheres to OMB and NIST requirements for the reporting of inadvertent disclosures. The PGLD Incident Management Team will review SPIIDE identified events in conjunction with BSP Liaisons and the DLP OPS Team and report appropriate items to Treasury CSIRC. When applicable, a risk assessment will be performed and potentially affected individuals notified in accordance with existing direction.

IMPLEMENTATION DATE: N/A

RESPONSIBLE OFFICIALS: N/A

Draft Audit Report – While the Data Loss Prevention Solution Is Being Developed, Stronger Oversight and Process Enhancements Are Needed for Timely Implementation Within Budget (Audit # 201420024) (e-trak #2014-58500)

CORRECTIVE ACTION MONITORING PLAN: N/A