TREASURY INSPECTOR GENERAL FOR TAX ADMINISTRATION

Improvements Are Needed to Ensure That External Interconnections Are Identified, Authorized, and Secured

September 14, 2015

Reference Number: 2015-20-087

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.

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

IMPROVEMENTS ARE NEEDED TO ENSURE THAT EXTERNAL INTERCONNECTIONS ARE IDENTIFIED, AUTHORIZED, AND SECURED

Highlights

Final Report issued on September 14, 2015

Highlights of Report Number: 2015-20-087 to the Internal Revenue Service Chief Technology Officer.

IMPACT ON TAXPAYERS

The IRS shares Federal tax information and other IRS records with many Federal, State, and local agencies as well as private agencies and contractors through system interconnections. The IRS must ensure that these system interconnections are authorized by written agreements that specify the technical and security requirements for the interconnection before information is shared. Both of the interconnected systems must meet IRS protection requirements in order to ensure that taxpayer and other sensitive data are secure.

WHY TIGTA DID THE AUDIT

This audit was initiated to determine whether controls are in place and operating effectively to protect IRS networks related to connections to external systems. If interconnections are not properly designed, security failures could compromise the connected systems and the sensitive data that they store, process, or transmit.

WHAT TIGTA FOUND

Many interconnections in use at the IRS do not have proper authorization or security agreements. Although the IRS has established an office to provide oversight and guidance for the development of security agreements, that office is not responsible for managing or monitoring agreements for all external interconnections in use in the IRS environment. TIGTA believes the lack of a centralized inventory and an enterprise-level approach to ensure that all external interconnections are monitored has contributed to interconnections that are currently active but lack proper approvals and assurances that the interconnections meet current security requirements. TIGTA also identified that improvements are needed to ensure that existing agreements contain all required elements and are renewed timely.

WHAT TIGTA RECOMMENDED

TIGTA recommended that the Chief Technology Officer: 1) identify all external interconnections and ensure that they are documented appropriately and maintained in a centralized inventory; 2) establish a repeatable process for conducting annual searches for external interconnections and for updating the centralized inventory accordingly; 3) ensure that policies and procedures are developed and implemented for monitoring the IRS's entire inventory of external interconnections and ensuring that all appropriate agreements are in place; and 4) establish an escalation process to resolve agreement renewal issues when contact efforts with the external partner have been exhausted with no resolution. TIGTA also recommended that the Associate Chief Information Officer, Cybersecurity: 5) ensure that agreements meet policies and are renewed timely and 6) reevaluate agreement processes and procedures to streamline and eliminate ineffective practices.

The IRS agreed with TIGTA's recommendations and planned appropriate corrective actions. The IRS agreed to: 1) identify and document external interconnections; 2) establish a repeatable process for identifying external interconnections; 3) ensure that policies and procedures are developed and implemented for updating the interconnections inventory; 4) establish an escalation process to resolve agreement renewal issues; 5) ensure that interconnection agreements meet policies and are renewed timely; and 6) streamline and eliminate ineffective practices related to interconnection agreements.

TREASURY INSPECTOR GENERAL
FOR TAX ADMINISTRATION

DEPARTMENT OF THE TREASURY

WASHINGTON, D.C. 20220

September 14, 2015

MEMORANDUM FOR CHIEF TECHNOLOGY OFFICER

FROM: Michael E. McKenney
Deputy Inspector General for Audit

SUBJECT: Final Audit Report – Improvements Are Needed to Ensure That External Interconnections Are Identified, Authorized, and Secured (Audit # 201520015)

Attached for your review and comments is the subject final audit report. The overall objective of this review was to determine whether controls are in place and operating effectively to protect Internal Revenue Service networks related to connections to external systems. This audit is included in our Fiscal Year 2015 Annual Audit Plan and addresses the major management challenge of Security for Taxpayer Data and Employees.

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

Copies of this report are also being sent to the Internal Revenue Service managers affected by the report recommendations. Please contact me at (202) 622-6510 or Danny Verneuille, Acting Assistant Inspector General for Audit (Security and Information Technology Services), at (901) 546-3111 if you have any questions.

Table of Contents

Abbreviations

FTI	Federal Taxpayer Information
IRS	Internal Revenue Service
ISA	Interconnection Security Agreement
MOU	Memorandum of Understanding
NIST	National Institute of Standards and Technology
NMC	Network Management Center
PII	Personally Identifiable Information
SAS	Security Assessment Services
SBU	Sensitive But Unclassified
SFT	Secure File Transfer

Background

Interconnecting information technology systems can expose the participating organizations to risk. Therefore, Federal regulations require agencies to establish agreements and obtain written management authorization beforehand.

The National Institute of Standards and Technology (NIST) defines a system interconnection as the direct connection of two or more information technology systems for the purpose of sharing data and other information resources.[1] The NIST states that significant benefits can be realized through a system interconnection, including reduced operating costs, greater functionality, improved efficiency, and centralized access to data. Interconnecting information technology systems may also strengthen ties among participating organizations by promoting communication and cooperation.

However, despite the advantages of an interconnection, interconnecting information technology systems can expose the participating organizations to risk. If the interconnection is not properly designed, security failures could compromise the connected systems as well as the data that they store, process, or transmit. Similarly, if one of the connected systems is compromised, the interconnection could be used as a conduit to compromise the other system and its data. The potential for compromise is underscored by the fact that, in most cases, the participating organizations have little or no control over the operation and management of the other party's system.

It is critical, therefore, that both parties learn as much as possible about the risks associated with the planned or current interconnection and the security controls that they can implement to mitigate those risks. It is also critical that they establish an agreement between themselves regarding the management, operation, and use of the interconnection and that they formally document this agreement. The agreement should be reviewed and approved by appropriate senior staff from each organization.

Office of Management and Budget Circular A-130, Appendix III,[2] states the requirement for Federal agencies to obtain written management authorization before connecting their information technology systems to other systems based on an acceptable level of risk. It also requires that, where a connection is authorized, controls must be established which are consistent with the rules of the system and in accordance with guidance from the NIST.

---

[1] NIST, Special Publication 800-47, *Security Guide for Interconnecting Information Technology System* (Aug. 2002).

[2] Office of Management and Budget, OMB Circular No. A-130 (Revised), *Management of Federal Information Resources*, Appendix III, *Security of Federal Automated Information Resources* (Nov. 2000).

The NIST prescribes that two documents may be developed to govern the interconnection: a Memorandum of Understanding (MOU) or Agreement (or an equivalent document) and an Interconnection Security Agreement (ISA) based on the relevant technical, security, and administrative issues. The MOU documents the terms and conditions for sharing data and information resources in a secure manner. Specifically, the MOU defines the purpose of the interconnection; identifies relevant authorities; specifies the responsibilities of both parties in establishing, operating, and securing the interconnection; and defines the terms of agreement, including apportionment of costs and the timeline for terminating or reauthorizing the interconnection. The MOU should not include technical details on how the interconnection is established or maintained; that is the function of the ISA.

The ISA is a security document that specifies the technical and security requirements for establishing, operating, and maintaining the interconnection. Specifically, the ISA documents the requirements for connecting the information technology systems, describes the security controls that will be used to protect the systems and data, contains a topological drawing of the interconnection, and provides a signature line. The ISA supports the MOU between the organizations.

Rather than develop an MOU and ISA, NIST standards include that organizations may choose to incorporate this information into a formal contract, especially if the interconnection is to be established between a Federal agency and a commercial organization.

The Internal Revenue Service (IRS) shares Federal taxpayer information (FTI)[3] and other IRS records with many Federal, State, and local agencies as well as private agencies and contractors through system interconnections. The exchange of information may facilitate joint tax administration relationships, enable tax collection processes with financial institutions, or provide information needed for a variety of tax administration purposes. The IRS must ensure that these interconnections are authorized by written agreements that specify the technical and security requirements for the interconnection before information is shared. Both of the interconnected systems must meet IRS protection requirements in order to ensure that taxpayer and other sensitive data are secure.

This review was performed at the New Carrollton Federal Building in Lanham, Maryland, in the IRS Information Technology Office of Cybersecurity, and with information obtained from the Offices of Cybersecurity and User and Network Services, during the period October 2014 through June 2015. 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 objectives. Detailed

[3] FTI includes such information as the taxpayer's name, address, Social Security Number, telephone number, spousal information, and financial information.

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

IRS policy[4] requires interconnections between IRS information technology systems and external information technology systems to be documented in security agreements in accordance with NIST Special Publication 800-47, *Security Guide for Interconnecting Information Technology Systems* (August 2002). The IRS has developed templates for MOUs and ISAs that meet NIST standards. According to IRS policy, the MOU establishes the management agreement between the IRS and the external partner regarding the development, management, operation, and security of the interconnection, and the ISA documents the technical and security requirements for the interconnection. IRS policy requires the extent of the MOU and ISA information to be sufficient such that system owners and other management officials can make a prudent decision about approving the interconnection. IRS policy also requires that the non-IRS information technology systems approved for interconnecting with the IRS must meet or exceed the protection requirements of the IRS information technology system.

The IRS Information Technology Office of Cybersecurity is responsible for managing the IRS's Information Technology Security Program and ensuring the IRS's compliance with Federal statutory, legislative, and regulatory requirements. Within the Office of Cybersecurity, the Security Assessment Services (SAS) office provides oversight and guidance for the documentation of IRS interconnections in MOUs and ISAs. The SAS office has prepared ISA Standard Operating Procedures to help guide and assist IRS system owners in establishing an interconnection with an external partner and developing MOUs and ISAs. When contacted by a system owner that is establishing an external interconnection, the SAS office provides the approved MOU and ISA templates and other guidance needed to help ensure that the interconnection is properly secured and documented.

The SAS office also developed an ISA Process Flow Diagram that illustrates the 15-step process to properly complete an interconnection and identifies the parties responsible for each step.[5] In addition to the SAS office, the following parties are included in the MOU and ISA process.

- **The IRS system owner** is the agency official responsible for the overall procurement, development, integration, modification, operation, and maintenance of the information system. The system owner is responsible for facilitating and managing the overall ISA process to assure timely activation of the interconnection.
- **The external system owner** is the external partner who works with the IRS system owner to provide technical guidance and expertise to establish the interconnection. The external system owner of the non-IRS system is an integral part of the approval process

[4] Internal Review Manual 10.8.1, *Information Technology Security, Policy and Guidance.*
[5] See Appendix IV.

and formally assumes responsibility, on behalf of the external organization, for operating the system at an acceptable level of risk.

- **The IRS User and Network Services office** is responsible for managing the design and engineering of the IRS telecommunications environments, which includes the networks supporting interconnections.
- **The IRS Enterprise Operations Services office** is responsible for providing secure and reliable server and mainframe services for the IRS and taxpayers and for developing scripts to move files within the IRS infrastructure.
- **IRS Cybersecurity Computer Security Incident Response Center** provides proactive prevention, detection, and response to computer security incidents targeting IRS information technology assets. The Cybersecurity Computer Security Incident Response Center representative works with the external partner and the IRS to complete the Firewall Change Request form and configure and activate the IRS firewall that supports the interconnection.

At the time of our audit, the SAS office's inventory of interconnections consisted of 49 external partners. The SAS office monitors the security agreements for these external partners using a spreadsheet and notifies system owners when their agreements are about to expire. The ISA Standard Operating Procedures require ISAs to be reviewed, renewed, and updated at a minimum of every three years.

Despite the efforts from all participating individuals and offices on external interconnections, we found that many interconnections in use did not have proper authorization or security agreements and that the IRS does not have a method to identify and maintain an up-to-date inventory of its interconnections. Also, improvements are needed to ensure that existing agreements contain all required elements to comply with IRS policies.

External Interconnections Were Active Without Proper Authorizations or Security Agreements

Interconnecting information systems can expose the participating organizations to risk. As the NIST prescribes, IRS policy requires that two documents be developed to govern an interconnection: an MOU and an ISA. The MOU defines the purpose of the interconnection, identifies relevant authorities, specifies the responsibilities of both organizations, and defines the terms of the agreement. The ISA describes the security controls that will be used to protect the systems and data being shared. Both documents must be signed by authorizing officials of the IRS and non-IRS systems prior to allowing the connection to be implemented.

We found that the IRS did not have formal interconnection agreements in place to authorize all of its external system interconnections and to require information security controls commensurate with IRS standards.

Many interconnections did not have an MOU, ISA, and/or other agreement

During the audit, we requested information on all active external connections from the User and Network Services office's Network Management Center (NMC), which we then compared to the list of interconnections maintained by the SAS office. We identified 31 interconnections from the NMC list that did not have proper agreements in place. The SAS office was not aware of these external interconnections and, therefore, they were not in the SAS office's inventory.

Figure 1: Interconnections Not in the SAS Office's Inventory

	Name of Interconnections to the Martinsburg Computing Center		Name of Interconnections to the Memphis Computing Center
1	Automated Lien System Boston	16	Automated Data Processing
2	Automated Lien System Hartford	17	Commerce Clearing House
3	Commerce Clearing House	18	Drake
4	Embassy	19	Embassy
5	Federal Reserve Bank Dallas	20	Federal Reserve Bank Dallas
6	Federal Reserve Bank New Jersey	21	Federal Reserve Bank New Jersey
7	Federal Reserve Bank Richmond	22	Federal Reserve Bank Richmond
8	Integrated Submission and Remittance Processing	23	H&R Block
9	Intuit	24	Integrated Submission and Remittance Processing
10	Joint Committee on Taxation	25	Intuit
11	Joint International Tax Shelter Information Centre	26	Jackson-Hewitt
12	New Jersey State Tax	27	Joint Committee on Taxation
13	Taxworks	28	Paychex
14	United States Department of Justice	29	Taxwise
15	Volunteer Income Tax Assistance	30	Taxworks
		31	Volunteer Income Tax Assistance

Source: Treasury Inspector General for Tax Administration comparison of the NMC and the SAS office lists of interconnections. Interconnections with the same names are unique interconnections to different locations. However, the IRS may only need one ISA and related MOU to cover both locations.

We also conducted research using the following three sources of information pertaining to external interconnections to identify all possible interconnections with external partners.

- A list of security reviews completed by the Office of Cybersecurity in Fiscal Year 2014 of contractors that receive taxpayer data in systems external to the IRS.

- Lists from the As-Built-Architecture database maintained on the IRS intranet of "External Applications" and "External Trading Partners" that we obtained in November 2014.
- A list of potential external interconnections identified by the IRS's User and Network Services office in Fiscal Year 2013 during the Trusted Internet Connection implementation.

When we compared our resulting list of potential external interconnections to the SAS office list of existing ISAs, we identified three additional active interconnections that the SAS office was not aware of and that did not possess any MOUs or ISAs. These interconnections were also not included in the NMC list.

1. Tennessee Computing Center Electronic Management System – WeFile.
2. Department of Agriculture National Finance System.
3. Department of Labor in Puerto Rico.

Most of these 34 external partners appear to be legitimate organizations related to tax administration, but without signed MOUs and ISAs, we have no assurance that these interconnections are authorized for use and secured by IRS standards.

In addition to the 34 interconnections discussed, the IRS indicated that there were other interconnections on our compiled list that did not need ISAs because they used secure file transfer (SFT) protocol[6] when transmitting data. The SAS office's ISA Standard Operating Procedures state that an ISA is not required if using SFT; rather, an MOU or an SFT Participation Agreement is used in place of an ISA. However, the IRS could not provide any SFT Participation Agreements or any type of other agreements for the interconnections that it had indicated used SFT as its transmission method. The following are examples of the external partners for these interconnections:

- Alpine Access (supports IRS publishing).
- EG&G Technical Services (receives Personally Identifiable Information (PII)[7] from the IRS).
- California Franchise Tax Board (receives FTI from the IRS).
- New York State Tax Board (receives FTI from the IRS).

[6] SFT uses the Axway Secure Transport product to provide a secure method for transferring files across the Internet as well as within a secured network.
[7] PII is any information about an individual maintained by an agency. This includes name, Social Security Number, date and place of birth, mother's maiden name, or biometric records.

- Fors Marsh Group (provides the IRS with customer satisfaction measurements; receives approximately 70,000 records from the IRS containing FTI, including personal contact points, e-mail addresses, taxpayer names, and adjusted income).
- Government, Retirement, and Benefits Inc. (developed the Employee Benefits Information System). The IRS receives payroll information from the National Finance Center and provides it to this external partner.

The IRS stated that many of its existing interconnections have been in place a long time, and former agreements could not be located. The IRS also stated that it did not establish external interconnections initially without signed authorizations and security agreements.

However, without proper and current agreements in place, external partners may not implement security controls required by IRS policies for interconnections. For example, during a contractor security review conducted in February 2014, the IRS Contractor Security Review team identified that the Government, Retirement, and Benefits Inc. external partner did not have a policy that required incidents to be reported to the IRS. If incidents are not reported timely, loss, destruction, or disclosure of IRS resources could occur. The IRS ISAs and MOUs include provisions that would have required the external partner to notify the IRS immediately in the event of an incident related to the interconnection. However, as noted, this external partner did not have an ISA, MOU, or SFT in place.

Interconnections were active even though either the MOU or ISA had expired

IRS policy requires the IRS to review, renew, and update its external interconnection agreements, at a minimum, every three years. The MOU states that it remains in effect up to three years after the last signature date or until a significant change occurs to the systems involved.

Our review of the 49 security agreements in the SAS office inventory revealed that three MOUs had expired although their ISAs were current. The SAS office was also working to renew an additional four ISAs and their related MOUs that had expired. The agreements relating to these seven interconnections have been expired from one to 19 years. The seven interconnections are active, despite the expired agreements. Six of the seven expired agreements indicate that sensitive data are transferred from the IRS to the external partner. Sensitive data may include FTI, PII, and/or Sensitive But Unclassified (SBU) data.[8] Figure 2 illustrates the details for the expired ISAs and MOUs.

[8] SBU is any information that requires protection due to the risk and magnitude of loss or harm to the IRS or the privacy to which individuals are entitled under 5 U.S.C. § 552a (the Privacy Act), which could result from inadvertent or deliberate disclosure, alteration, or destruction.

Figure 2: Expired MOUs and ISAs

External Partner	Type of Agreement	Date Expired	Data Transferred	FTI, PII, or SBU Data
1. Customs and Border Protection	MOU	June 3, 1996	Name, date of birth, passport number, and financial data.	PII; SBU
2. Defense Manpower Data Center	MOU	November 30, 2010	Records of delinquent taxpayers, including balances owed and Social Security Numbers.	FTI; PII; SBU
3. Financial Crimes Enforcement Network Bureau	MOU	September 24, 2013	Bank Secrecy Act[9] data from financial institutions and individuals.	FTI; PII; SBU
4. Federal Bureau of Investigations	ISA/MOU	May 31, 2010	Fingerprint images, demographic data, and search results for the applicant.	PII; SBU
5. Verizon	ISA/MOU	August 20, 2013	Telecommunications data.	SBU
6. Communication Service for the Deaf Inc.	ISA/MOU	September, 7, 2013	Non-sensitive American Sign Language communication.	None
7. Office of Personnel Management eDelivery	ISA/MOU[10]	September 16, 2013	Background investigation case files.	PII

Source: Treasury Inspector General for Tax Administration review of the IRS MOUs and ISAs and the SAS's ISA Status Log.

The SAS office relies on a cooperative relationship with external partners. Although the SAS office sends emails regarding pending renewals due on ISAs and MOUs, some external partners do not respond in a timely manner. Rather than terminate a connection when it expires, the SAS office just continues to work on getting it renewed. However, the SAS office has no formal escalation process in place to address ISA and MOU issues when external partners do not respond timely.

If ISAs and MOUs have expired, there is no longer an agreement for the management, operation, and use of the interconnection or accountability for the security controls required to protect it. In

[9] Pub. L. No. 91-508, 84 Stat. 1114 to 1124 (1970) (codified as amended in scattered sections of 12 U.S.C., 18 U.S.C., and 31 U.S.C.). Regulations for the Bank Secrecy Act and other related statutes are 31 C.F.R. §§ 103.11-103.77.

[10] On June 11, 2015, the IRS provided us a renewed ISA and MOU for its interconnection with the Office of Personnel Management eDelivery system. The renewed ISA was effective as of May 27, 2015.

addition, there is no written authorization for the systems to connect, as required by Office of Management and Budget Circular A-130, Appendix III. Without proper attention to the status of required security controls, security risks associated with the interconnection may exist without the IRS's knowledge. Consequently, the connected systems and data that are being transferred may not be adequately protected.

An interconnection was activated before agreements were signed by approving officials

We also identified one interconnection that was activated prior to having proper interconnection agreements in place. An interconnection with the Pennsylvania Departments of Motor Vehicles was listed in the SAS office's tracking log as being under development but was also listed on the NMC list of current interconnections. As of April 2015, the SAS office confirmed that the development of agreements for this interconnection were still in progress and not yet signed by authorizing officials.

The IRS indicated that this connection has been in place for a very long time. In the fourth quarter of Fiscal Year 2013, the User and Network Services office stated that it notified the SAS office of a technical change to this connection and requested that interconnection agreements be updated. However, since former interconnection agreements could not be located, the SAS office began the process of overseeing the development of new ones.

Although the IRS intends for all changes to systems (including activation of new interconnections) to be monitored and controlled through a change management process, this control is being circumvented because external interconnections are activated without proper approval and coordination.

For the deficiencies discussed, the IRS has not developed sufficient controls to ensure that all external interconnections have proper security agreements in place prior to allowing connectivity. In addition, SAS officials stated that they were not responsible for managing or monitoring agreements for all external interconnections in use in the IRS environment. The NMC also stated that it did not monitor or maintain a list of all external interconnections. Both the SAS office and the NMC stated that they did not monitor interconnections that used SFT but indicated that the Enterprise Operations organization was the program owner of SFT. We believe that the lack of a centralized inventory and an enterprise-level approach to ensure that all external interconnections are monitored has contributed to interconnections that lacked proper authorizations and security agreements.

Interconnections are not actively identified or maintained in a centralized inventory

Title 44 of the United States Code Section 3505 (c) requires agencies to maintain an inventory of their information systems that includes an identification of the interfaces between such systems

and systems not operated by or under the control of the agency. Such inventory must be updated at least annually.

The IRS could not provide us with an accurate inventory of its external interconnections. As previously discussed, no one entity at the IRS had the responsibility for maintaining or monitoring all external interconnections in the IRS environment. The IRS did not have enterprise-level processes and procedures for maintaining a comprehensive inventory, for periodically identifying active external interconnections to keep the inventory current, and for ensuring that all active interconnections have proper security agreements.

Without a centralized inventory of external interconnections along with a process for regularly identifying existing connections to keep it updated, the IRS cannot ensure that all external interconnections are known and properly secured. Without proper agreements in place, the interconnections have not been authorized and external partners may not implement required security controls, increasing the risk that IRS data could be compromised.

Recommendations

The Chief Technology Officer should:

Recommendation 1: Identify all external interconnections and ensure that they are documented appropriately and maintained in a centralized inventory.

> ***Management's Response:*** The IRS agreed with this recommendation. The IRS has completed identifying all external interconnections and has updated the centralized inventory accordingly. The Office of Cybersecurity will work with the Information Technology organization and business stakeholders to ensure that ISAs and MOUs are fully documented.

Recommendation 2: Establish a repeatable process for conducting annual searches for external interconnections and for updating the centralized inventory accordingly.

> ***Management's Response:*** The IRS agreed with this recommendation. The Office of Cybersecurity will establish a repeatable process for conducting annual searches for external interconnections and for updating the centralized inventory accordingly.

Recommendation 3: Ensure that policies and procedures are developed and implemented for monitoring the IRS's entire inventory of external interconnections and ensuring that all appropriate ISAs and MOUs (or other approved agreements) are in place before interconnections are allowed to be established and activated.

> ***Management's Response:*** The IRS agreed with this recommendation. The Office of Cybersecurity will work with the Information Technology organization and business stakeholders to update policy and develop procedures for monitoring the IRS's inventory

of external connections and ensuring that all appropriate approved agreements are in place before interconnections are established.

Recommendation 4: Establish an escalation process to resolve ISA and MOU renewal issues at a higher level when the SAS office's contact efforts have been exhausted with no resolution. Consideration should be given to suspending the connection if system owners do not cooperate with the SAS office to resolve expired ISAs and MOUs.

> ***Management's Response:*** The IRS agreed with this recommendation. The Office of Cybersecurity will establish an escalation process to resolve ISA and MOU renewal issues.

Although Information Security Agreements Were Consistent, Memorandums of Understanding Did Not Always Meet Internal Revenue Service Policies

Both the IRS ISA and MOU templates comply with NIST standards and contain appropriate sections to cover required information. For example, these agreements collectively identify the requirements for the connection, the roles and responsibilities for each party, the security controls protecting the connection, the sensitivity of the data to be exchanged, the training requirements, cost considerations, and the time frame for the agreement to remain in effect.

We reviewed the agreements for the 49 external interconnections in the SAS office's inventory and found that the 49 ISAs were consistent and generally complied with Federal standards and IRS policies, including adequately documenting the security controls used to protect the systems and data. We noted that the two ISAs that did not fully meet standards consisted of one that did not include the signature and date of the IRS authorizing management official and another that had an expiration date beyond the IRS's established time frame for renewal of three years.

We found 23 MOUs[11] that did not meet IRS policies. Overall, we found the MOUs lacked consistency and uniformity. Specifically, we found the following policy deviations among the 23 MOUs.

- 11 MOUs had no disclosure clause, even though FTI, PII, and/or SBU were involved.

  The IRS's requirement for the disclosure clause is in addition to NIST standards for the MOUs. The clause requires the parties to agree to properly protect taxpayer and other sensitive data when they are involved. Specifically, it states: "All users covered by this agreement acknowledge that they will comply with disclosure and privacy statutes (including but not limited to section 6103 of the Internal Revenue Code, the Privacy Act,[12] the Bank Secrecy Act, and 18 United States Code) that are applicable to the

[11] Seven of the 23 MOUs had multiple issues and therefore were counted in more than one of the bulleted categories.
[12] Privacy Act of 1974, 5 U.S.C. § 552a.

information transmitted." The IRS MOU template specifies that this clause can be deleted if no taxpayer data are involved. However, because the clause covers all disclosure and privacy statutes, which include not only FTI but also PII and SBU information, it may be prudent to include the disclosure clause in the MOU if the interconnection is used to exchange or transfer any of these types of information.

The SAS office indicated that the disclosure clause was included in the IRS's MOU template per instructions from the IRS's Privacy, Governmental Liaison, and Disclosure office. However, if the disclosure clause is not being used consistently in interconnection agreements when sensitive data are being transmitted, the IRS should reevaluate its placement and use. For example, it might be more efficient to permanently include the requirement for protection of FTI, PII, and SBU information within the ISA Rules of Behavior section, which already includes other information protection requirements.

- 9 MOUs did not exist or did not specifically relate to the external interconnection specified in the ISA.
- 7 MOUs had no specific end date or had expiration dates that were set past the three year time frame allowed. The IRS MOU template specifies that the agreement will stay in effect for up to three years.
- 4 MOUs had no cost considerations. The cost consideration section is required to establish an agreement between the parties on how the responsibility for any costs related to the interconnection will be distributed.
- 1 MOU was not properly signed by the IRS system owner.

We also noted 11 instances in which the MOU date was not the same as the ISA date. This creates an increased burden for the SAS office in regards to monitoring both document expiration dates. The SAS office is aware that this had occurred and is taking steps to make MOU dates consistent with ISA dates during the renewal process.

The SAS office stated that its focus has been on the ISAs, and it has not given the MOUs as much priority. Rather, the SAS office defers responsibility for the MOUs to the IRS business owners of the interconnected systems.

When MOUs do not meet IRS policies, the IRS may be unable to hold the external partner fully accountable for maintaining secure interconnections. For example, if the MOU does not contain the disclosure clause when FTI, PII, or SBU is involved, the IRS cannot ensure that the external partner has agreed to protect it in accordance with section 6103 of the Internal Revenue Code and other relevant privacy statutes. In addition, if the MOU does not cover cost considerations, disputes could arise between the IRS and the external partner over the apportionment of costs (*e.g.*, if increases occur in the cost of maintaining the interconnection).

Recommendations

The Associate Chief Information Officer, Cybersecurity, should:

Recommendation 5: Ensure that the SAS office monitors ISA-related MOUs in a similar manner as ISAs to ensure that ISA-related MOUs meet IRS policies and are renewed timely.

> ***Management's Response:*** The IRS agreed with this recommendation. The Office of Cybersecurity will monitor ISA-related MOUs in a similar manner as ISAs to ensure that ISA-related MOUs meet IRS policy and are renewed timely.

Recommendation 6: Reevaluate MOU processes and procedures to streamline and eliminate ineffective practices.

> ***Management's Response:*** The IRS agreed with this recommendation. The Office of Cybersecurity will streamline the ISA-related MOU procedures to eliminate ineffective practices.

Appendix I

Detailed Objective, Scope, and Methodology

Our overall objective was to determine whether controls are in place and operating effectively to protect IRS networks related to connections to external systems. To accomplish our objective, we:

I. Determined if the IRS's ISA processes resulted in effective agreements for external system connections.

- A. Identified and interviewed key personnel within functions controlling ISAs.
- B. Obtained a current list of ISAs and MOUs.
- C. Determined if the IRS's ISA and MOU documents complied with Federal standards and if IRS ISA policies and processes were followed.

II. Determined if the IRS has adequate controls to identify all of its external connections.

- A. Identified and interviewed key personnel responsible for the identification of external connections.
- B. Determined if the IRS regularly maintains and regularly updates an inventory of external connections.
- C. Determined if the IRS conducts periodic reviews for unknown/uncontrolled external connections and if all functions are kept informed.
- D. Obtained a current list of external connections from known sources such as the IRS Information Technology Offices of User and Network Services and Cybersecurity contractor security reviews.
- E. Compared the list of ISAs obtained in Step I.B with the list of external connections obtained in Step II.D and identified discrepancies.
- F. Determined the reasons for discrepancies by interviewing pertinent personnel.

III. Determined if the IRS has adequate controls to ensure that security controls specified in ISAs for securing external connections are in place.

- A. Determined if security reviews were conducted annually or when significant changes to the system or environment occurred.
- B. Reviewed IRS security reports for external connections and determined if security weaknesses existed.

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: IRS policies and procedures for the identification and control of external interconnections and for ensuring that required security agreements are in place. We evaluated these controls by reviewing IRS, NIST, and Office of Management and Budget policies; interviewing IRS personnel; reviewing external interconnection security agreements; and evaluating IRS processes for identifying and documenting external interconnections.

Appendix II

Major Contributors to This Report

Alan Duncan, Assistant Inspector General for Audit (Security and Information Technology Services)
Danny Verneuille, Acting Assistant Inspector General for Audit (Security and Information Technology Services)
Kent Sagara, Director
Jody Kitazono, Audit Manager
Bret Hunter, Lead Auditor
Mark Carder, Senior Auditor
Esther Wilson, Senior Auditor

Appendix III

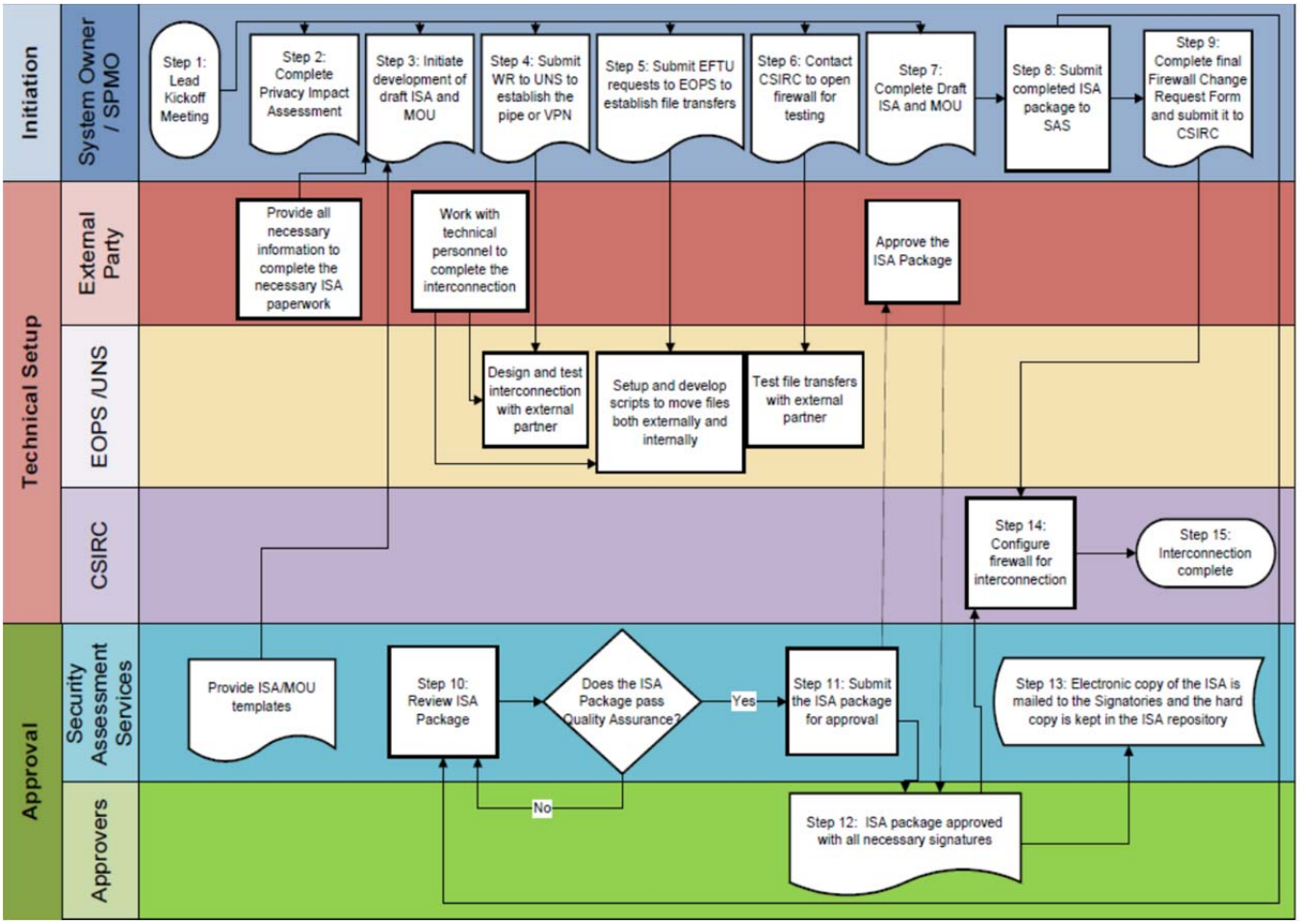
Report Distribution List

Commissioner C
Officer of the Commissioner – Attn: Chief of Staff C
Deputy Commissioner for Operations Support OS
Deputy Commissioner for Services and Enforcement SE
Associate Chief Information Officer, Cybersecurity OS:CTO:C
Associate Chief Information Officer, User and Network Services OS:CTO:UNS
Chief Counsel CC
National Taxpayer Advocate TA
Director, Office of Program Evaluation and Risk Analysis RAS:O
Director, Office of Audit Coordination OS:PPAC:AC
Office of Internal Control OS:CFO:CPIC:IC
Audit Liaison: Director, Risk Management Division OS:CTO:SP:RM

Appendix IV

Interconnection Security Agreement Process Flow Diagram

The following is a diagram showing the ISA process by IRS and external party responsibilities.



Source: The IRS Security Assessment Services ISA System Owner Standard Operating Procedure, April 24, 2014.
Note: CSIRC = Computer Security Incident Response Center. EFTU = Electronic File Transfer Utility. EOPS = Enterprise Operations. SPMO = Security Program Management Office. UNS = User and Network Services. VPN = Virtual Private Network. WR = Work Request.

Appendix V

Management's Response to the Draft Report

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

CHIEF TECHNOLOGY OFFICER

AUG 19 2015

MEMORANDUM FOR DEPUTY INSPECTOR GENERAL FOR AUDIT

FROM: Terence V. Milholland
Chief Technology Officer

SUBJECT: Draft Audit Report – Improvements Are Needed to Ensure External Interconnections Are Identified, Authorized and Secured, (Audit # 201520015)
(e-trak #2015-71242)

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 the IRS has developed templates for Memorandums of Understanding (MOU) and the Interconnections Security Agreements (ISA), in accordance with NIST standards. The MOU establishes the management agreement between the IRS and the external partner on the security of the interconnections; and the ISA documents the technical and security requirements for the interconnections before information is shared. The interconnected systems must meet IRS protection requirements. Additionally, the connections described in the report are monitored by our incident response function.

The IRS understands and honors the trust given to it by American taxpayers to safeguard their personal and private information. As part of that trust, IRS is continuously improving the External Interconnections program, to ensure taxpayer and other sensitive data are protected and secure. The attachment to this memo details our planned corrective actions to implement the audit report's recommendations.

The IRS values your continued support and the assistance your organization provides. If you have any questions, please contact me at (240) 613-9373 or Carmelita White, Senior Manager of Program Oversight Coordination, at (240) 613-2191.

Attachment

IMPROVEMENTS ARE NEEDED TO ENSURE THAT EXTERNAL INTERCONNECTIONS ARE IDENTIFIED, AUTHORIZED, AND SECURED
(Audit # 201520015, e-trak #2015-71242

RECOMMENDATION #1 The Chief Technology Officer should identify all external interconnections and ensure that they are documented appropriately and maintained in a centralized inventory.

CORRECTIVE ACTION #1: The IRS agrees with this recommendation. IT has completed identifying all external interconnections and updated the centralized inventory accordingly. Cybersecurity will work with IT and business stakeholders to ensure ISAs and MOUs are fully documented.

IMPLEMENTATION DATE: September 15, 2016

RESPONSIBLE OFFICIAL: Associate Chief Information Officer, Cybersecurity

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

RECOMMENDATION #2: The Chief Technology Officer should establish a repeatable process for conducting annual searches for external interconnections and for updating the centralized inventory accordingly.

CORRECTIVE ACTION #2: The IRS agrees with this recommendation. Cybersecurity will establish a repeatable process for conducting annual searches for external interconnections and for updating the centralized inventory accordingly.

IMPLEMENTATION DATE: October 15, 2015

RESPONSIBLE OFFICIAL: Associate Chief Information Officer, Cybersecurity

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

RECOMMENDATION #3: The Chief Technology Officer should ensure that policies and procedures are developed and implemented for monitoring IRS's entire inventory of external interconnections, and ensure that all appropriate ISAs and MOUs (or other approved agreements) are in place before interconnections are allowed to be established and activated.

IMPROVEMENTS ARE NEEDED TO ENSURE THAT EXTERNAL INTERCONNECTIONS ARE IDENTIFIED, AUTHORIZED, AND SECURED
(Audit # 201520015, e-trak #2015-71242

CORRECTIVE ACTION #3: The IRS agrees with this recommendation. Cybersecurity will work with IT and business stakeholders to update policy and develop procedures for monitoring IRS's inventory of external interconnections and ensuring all appropriate approved agreements are in place before interconnections are established.

IMPLEMENTATION DATE: September 15, 2016

RESPONSIBLE OFFICIAL: Associate Chief Information Officer, Cybersecurity

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

RECOMMENDATION #4: The Chief Technology Officer establish an escalation process to resolve ISA and MOU renewal issues at a higher level, when the SAS office's contact efforts have been exhausted with no resolution. Consideration should be given to suspending the connection if system owners do not cooperate with the SAS office to resolve expired ISAs and MOUs.

CORRECTIVE ACTION #4: The IRS agrees with this recommendation. Cybersecurity will establish an escalation process to resolve ISA and MOU renewal issues.

IMPLEMENTATION DATE: November 15, 2015

RESPONSIBLE OFFICIAL: Associate Chief Information Officer, Cybersecurity

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

RECOMMENDATION #5: The Chief Technology Officer should ensure that the SAS office monitors ISA-related MOUs in a similar manner as ISAs to ensure that ISA-related MOUs meet IRS policies and are renewed timely.

CORRECTIVE ACTION #5: The IRS agrees with this recommendation. Cybersecurity will monitor ISA-related MOUs in a similar manner as ISAs to ensure ISA-related MOUs meet IRS policy and are renewed timely.

IMPROVEMENTS ARE NEEDED TO ENSURE THAT EXTERNAL INTERCONNECTIONS ARE IDENTIFIED, AUTHORIZED, AND SECURED
(Audit # 201520015, e-trak #2015-71242

IMPLEMENTATION DATE: November 15, 2015

RESPONSIBLE OFFICIAL: Associate Chief Information Officer, Cybersecurity

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

RECOMMENDATION #6: The Chief Technology Officer should reevaluate MOU processes and procedures to streamline and eliminate ineffective practices.

CORRECTIVE ACTION #6: The IRS agrees with this recommendation. Cybersecurity will streamline the ISA-related MOU procedures to eliminate ineffective practices.

IMPLEMENTATION DATE: March 15, 2016

RESPONSIBLE OFFICIAL: Associate Chief Information Officer, Cybersecurity

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