TREASURY INSPECTOR GENERAL FOR TAX ADMINISTRATION

The Office of Safeguards Should Improve Management Oversight and Internal Controls to Ensure the Effective Protection of Federal Tax Information

September 15, 2014

Reference Number: 2014-20-059

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

THE OFFICE OF SAFEGUARDS SHOULD IMPROVE MANAGEMENT OVERSIGHT AND INTERNAL CONTROLS TO ENSURE THE EFFECTIVE PROTECTION OF FEDERAL TAX INFORMATION

Highlights

Final Report issued on September 15, 2014

Highlights of Reference Number: 2014-20-059 to the Internal Revenue Service Deputy Commissioner for Operations Support.

IMPACT ON TAXPAYERS

Internal Revenue Code Section 6103 authorizes the IRS to disclose Federal Tax Information (FTI) to various Federal agencies, State and local entities, and U.S. territories. It also requires recipients of FTI to establish effective safeguards for ensuring that taxpayer information is protected from unauthorized use and disclosure. If required safeguards for FTI are not established and maintained, the FTI is at an increased risk of unauthorized use and disclosure.

WHY TIGTA DID THE AUDIT

This audit was initiated to determine if the Office of Safeguards provides adequate oversight of the agencies that receive FTI. Federal regulations govern the confidentiality of FTI provided to agencies, and agencies must follow those requirements to receive it.

WHAT TIGTA FOUND

While the Office of Safeguards conducts on-site agency reviews to ensure that adequate safeguards are maintained, the reviews are conducted after FTI is released to agencies. This occurs in part because the IRS's Internal Revenue Manual does not require the performance of on-site validation of an agency's ability to protect FTI prior to its release to the agency.

In addition, the Office of Safeguards 1) does not set specific background investigation requirements for employees and contractors at agencies receiving FTI and 2) does not conduct on-site review tests on each agency's background investigation policies and procedures.

Effective controls have not been established to ensure that the IRS's annual report on the safeguards of agencies that receive FTI is timely submitted to the required U.S. congressional committees. In addition, policies and procedures do not require that information technology security test plans be designed with subtests weighted according to risk.

WHAT TIGTA RECOMMENDED

TIGTA recommended that the Deputy Commissioner for Operations Support ensure that on-site agency reviews are conducted prior to the release of FTI for any new systems or agencies receiving FTI for the first time unless an independent security assessment or IRS risk-based assessment is performed that includes the IRS requirements for the security of FTI and the assessment is reviewed and approved/prepared by the Office of Safeguards; establish and ensure that background investigation requirements for all agency employees and contractors with access to FTI are consistent with the IRS's background investigation requirements; ensure that background investigation validation tests are conducted during on-site agency reviews; improve congressional reporting timeliness; and improve on-site information technology security testing processes.

In their response to the report, IRS management partially agreed with the first recommendation and agreed with the other seven. The IRS plans to conduct an initial risk-based assessment before authorizing the release of FTI to an agency for the first time and develop a comprehensive policy to detail requirements; develop specific background investigation requirements for external agency employees and the agency's contractors authorized to access FTI; conduct background investigation validation tests; and timely submit reports to Congress. The IRS also deployed a new management information system to provide enhanced tracking capabilities for the list of active agencies, reports, and related documents.

TREASURY INSPECTOR GENERAL
FOR TAX ADMINISTRATION

DEPARTMENT OF THE TREASURY

WASHINGTON, D.C. 20220

September 15, 2014

MEMORANDUM FOR DEPUTY COMMISSIONER FOR OPERATIONS SUPPORT

FROM: Michael E. McKenney
Deputy Inspector General for Audit

SUBJECT: Final Audit Report – The Office of Safeguards Should Improve Management Oversight and Internal Controls to Ensure the Effective Protection of Federal Tax Information (Audit # 201320029)

This report presents the results of our review to determine whether the Internal Revenue Service (IRS) Office of Safeguards effectively provides oversight of agencies that receive Federal Tax Information. This review is included in the Treasury Inspector General for Tax Administration Fiscal Year 2014 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 IRS managers affected by the report recommendations. If you have any questions, please contact me or Danny Verneuille, Acting Assistant Inspector General for Audit (Security and Information Technology Services).

Table of Contents

Background ..... Page 1

Results of Review ..... Page 4

The Office of Safeguards Does Not Conduct On-Site Reviews of Agencies Prior to Release of Federal Tax Information ..... Page 4

Recommendation 1: ..... Page 5

The Office of Safeguards Does Not Require and Ensure That Agencies Conduct Proper Background Investigations ..... Page 6

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

The Office of Safeguards Needs to Strengthen Its Congressional Reporting and On-Site Information Technology Security Testing Processes ..... Page 8

Recommendation 4: ..... Page 9

Recommendation 5: ..... Page 10

The Office of Safeguards' Program Controls Need Improvement ..... Page 10

Recommendations 6 through 8: ..... Page 16

Appendices

Appendix I – Detailed Objective, Scope, and Methodology ..... Page 17

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

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

Appendix IV – Glossary of Terms ..... Page 21

Appendix V – Management's Response to the Draft Report ..... Page 23

Abbreviations

ACA	Affordable Care Act
CAP	Corrective Action Plan
FTI	Federal Tax Information
GLDS	Governmental Liaison, Disclosure, and Safeguards
I.R.C.	Internal Revenue Code
IRM	Internal Revenue Manual
IRS	Internal Revenue Service
SAR	Safeguards Activity Report
SPR	Safeguard Procedures Report
SRR	Safeguard Review Report

Background

The Internal Revenue Service (IRS) provides Federal Tax Information (FTI)[1] to approximately 280 Federal agencies, State and local entities, and U.S. territories (hereafter referred to as agencies). It is authorized under Internal Revenue Code (I.R.C.) Section (§) 6103 to disclose FTI to agencies. The agencies use FTI for various reasons such as to locate delinquent taxpayers, assist in determining whether a taxpayer can pay on a defaulted debt, and determine whether discrepancies exist in the reporting of income.

I.R.C. § 6103(p)(4), Internal Revenue Manual Section (IRM) 11.3.36,[2] and IRS Publication 1075, *Tax Information Security Guidelines For Federal, State, and Local Agencies*,[3] require recipients of FTI to establish procedures to ensure the adequate protection of FTI received. I.R.C. § 6103(p)(4) and (7) authorizes the IRS to remove FTI if misuse and/or inadequate safeguards are in place to protect it from unauthorized use and disclosure. The Office of Safeguards (hereafter referred to as the Office) is in the Governmental Liaison, Disclosure, and Safeguards (GLDS) function of the Privacy, Governmental Liaison, and Disclosure business unit within the IRS Operations Support organization and has oversight responsibility of agencies that receive FTI subject to I.R.C. § 6103(p)(4) to ensure that adequate safeguards are maintained. The IRS is responsible for producing and revising Publication 1075, which provides guidance to agencies regarding the required safeguard procedures necessary to protect FTI.

Before agencies can receive FTI, they must submit a formal report called a Safeguard Procedures Report (SPR) that describes how the agency will protect and safeguard FTI in accordance with I.R.C. § 6103(p)(4), IRM 11.3.36, and Publication 1075. Agencies are then required to submit an SPR every six years or when significant changes in their safeguard procedures occur. In addition to the SPRs, agencies must submit annually a Safeguards Activity Report (SAR) to describe any changes to their safeguard procedures, advise of future actions that will affect such procedures, and certify they are protecting FTI in accordance with I.R.C. § 6103(p)(4), IRM 11.3.36, and Publication 1075. The SPRs must be reviewed by the Office within 60 calendar days of receipt, and the SARs must be reviewed within 45 calendar days of receipt.

Agency reviews

On-site reviews of agencies receiving FTI are required to be conducted by the Office a minimum of once every three years. The reviews are designed to ensure compliance with I.R.C. § 6103(p)(4), IRM 11.3.36, and Publication 1075 regarding recordkeeping, secure storage, restricting access, other safeguards related to employee awareness and internal inspections,

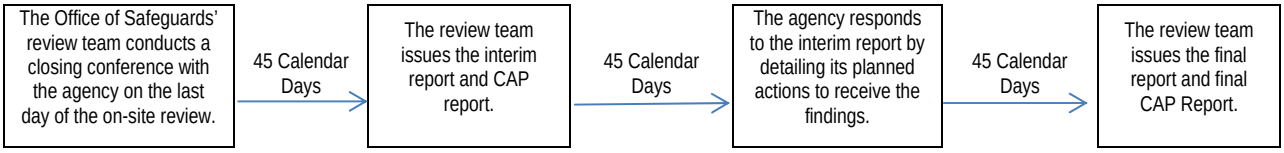
[1] See Appendix IV for a glossary of terms.
[2] Dated Aug. 2008.
[3] Dated Aug. 2010.

reporting requirements, and disposal. The on-site agency reviews are generally conducted over a three-day period.

The Office's review teams are made up of disclosure enforcement specialists and information technology specialists. Disclosure enforcement specialists lead the reviews and are responsible for reviewing the agencies' physical security, privacy, and disclosure policies and procedures. Most of the information technology specialists are contract employees and perform information technology security reviews under the direction of the review team's lead disclosure enforcement specialists. The review teams use test plans to assist in validating the adequacy of the agencies' safeguard controls and are generally designed in accordance with I.R.C. § 6103(p)(4) and the National Institute of Standards and Technology's Special Publication 800-53, *Recommended Security Controls for Federal Information Systems and Organizations*, Revision 3, controls.[4]

Once an on-site review has been completed, the review team provides the agency an interim report and a draft findings document called an interim Corrective Action Plan (CAP) report that lists any deficiencies found during the review. The agency is then required to respond through written statements and/or supporting documentation of the corrective actions that have been or will be taken to address the identified deficiencies. The interim report and interim CAP report are required to be issued within 45 calendar days of the on-site review closing conference that is held on the last day of the on-site review. The agency has 45 calendar days to respond to the interim report, after which the review team has 45 calendar days to issue a final report and a final CAP report. Figure 1 illustrates the 45 calendar day requirement.

Figure 1: Timeline of Requirements for the Office's Report Issuance and for Agencies' Response to Reports



Source: The Office's preliminary report documents provided to agencies and discussed with management.

In addition, responsibilities of the Safeguard Program were recently expanded. The Patient Protection and Affordable Care Act of 2010[5] and the Health Care and Education Reconciliation Act of 2010[6] (hereafter collectively referred to as the Affordable Care Act (ACA)) were both signed into law in March 2010. The ACA seeks to provide more Americans with access to affordable health care by creating a new Health Insurance Exchange, enforcing patient/consumer protections, and providing Government subsidies for people who cannot afford insurance. The exchange provisions of the ACA are centered on implementing tax provisions associated with

[4] Dated Aug. 2009.
[5] 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.
[6] Pub. L. No. 111-152, 124 Stat. 1029. (See Affordable Care Act, *infra*).

Federal and State health insurance exchanges. Under these provisions, the IRS is required to support eligibility and enrollment in health insurance exchanges by providing income and family size information that is classified as FTI. The IRS must provide this FTI disclosure to the U.S. Department of Health and Human Services, which will disclose FTI to the health care exchanges for use in the determination of health care qualifications and subsidies. The Office is responsible for oversight of this disclosure and ensuring that the exchanges have required safeguards in place. We are currently conducting an information technology security audit focused specifically on the processes used by the IRS to review and approve ACA-related requests for FTI based on the SPRs submitted by ACA agencies.

This review was performed at the Office of Safeguards in Dallas, Texas, the Texas Office of Attorney General Child Support in Austin, Texas, and the Montana Department of Revenue offices in Helena, Montana, during the period May 2013 through May 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 Office of Safeguards Does Not Conduct On-Site Reviews of Agencies Prior to Release of Federal Tax Information

I.R.C. § 6103(p)(4), IRM 11.3.36, and Publication 1075 require agencies that request or receive FTI provide to the IRS a report that describes safeguards established and used by the agency for ensuring that FTI is protected. Therefore, the agencies and their contractors must file an SPR with the IRS and obtain approval prior to the receipt of FTI. The SPR must describe how the agency and its contractors will protect and safeguard FTI in accordance with I.R.C. § 6103(p)(4), IRM 11.3.36, and Publication 1075. The SPR must contain written descriptions and supporting documentation that provide sufficient evidence that FTI is protected at all points where it is received, processed, stored, and/or maintained.

After the SPR has been submitted, the Office reviews the document to determine if there is sufficient documented evidence that the safeguards established adequately secure FTI. If the SPR is approved by the Office, the IRS releases the requested FTI without on-site verification that the controls, processes, and procedures are actually established. The Office does not perform independent validation of the information provided on the SPR until an on-site agency review is conducted by the Office review team. On-site agency reviews are scheduled by the Office a minimum of one to three years after an agency has begun receiving FTI.

In addition, we conducted preliminary work in August 2013 on the GLDS business unit's efforts to approve agencies that requested FTI due to the ACA. The GLDS business unit created a separate ACA review team to handle the ACA-related SPR review and approval process. The ACA review team was not a part of the Office and reported to the Director, Privacy, Governmental Liaison, and Disclosure. These ACA-related SPRs were tracked, controlled, and approved by this separate review team. The ACA review team stated that it conducted on-site agency reviews that entailed some validation prior to SPR approval. However, the on-site reviews were conducted before the agency systems and procedures were fully developed and implemented. Once the SPR was approved, the FTI was released and the Office was instructed to add these approved ACA-related agencies to its on-site review schedule. At the time of our review, agencies in 27 States had requested or planned to request FTI in support of fulfilling their responsibilities related to the ACA legislation. This separate review team was operating independent of the Office's normal SPR review process for receiving FTI and developed its own procedures for reviewing ACA-related SPR submissions and approvals.

While the IRM requires the Office to conduct on-site agency reviews once every three years, it does not require the Office to perform on-site validation of an agency's ability to protect FTI

prior to its release to the agency. IRM 11.3.36 states that on-site reviews may be conducted within 12 months of an agency initially receiving FTI.

The Office's management stated that the SPRs submitted by the agencies provide sufficient evidence for the Office to determine whether an agency can protect FTI at all points where it is received, processed, stored, and/or maintained. Management does not believe it is practical to conduct on-site reviews of agencies prior to their receipt of FTI because, in their view, the evaluation would not determine how agencies actually are performing the safeguards established. Additionally, management believes that review teams may only discover all agency locations of FTI during the on-site reviews after receipt of FTI, as agencies do not always accurately document processes on the submitted SPRs. Management also believes that if the Office conducts on-site reviews before FTI is received by an agency, the safeguards established for all FTI maintained could not be evaluated.

Agencies that request FTI must demonstrate the ability to safeguard FTI prior to its receipt. When the primary assessment by the Office of an agency's safeguarding processes, *i.e.*, on-site reviews, is performed one to three years after receipt of FTI, there is a significant risk that FTI provided may be subjected to unauthorized disclosure and use. Until a complete on-site review is conducted, FTI is vulnerable to unauthorized use and disclosure, and taxpayers cannot be assured that their FTI is properly safeguarded.

Management actions

After the completion of our fieldwork and in discussions with the Office's executive management, the IRS stated that the Office is not following the IRM and that the IRM is outdated. The IRS stated that the requirement for an on-site review to be conducted a minimum of one to three years after an agency has begun receiving FTI is no longer the requirement. The Office now performs a risk-based approach to conduct on-site reviews, which determines how often an on-site review is conducted. In addition, IRS management prefers that an agency receive FTI for a minimum of 30 calendar days prior to any on-site review.

Recommendation

The Deputy Commissioner for Operations Support should:

Recommendation 1: Establish policies and procedures to require that on-site agency reviews are conducted prior to the initial release of FTI for any new systems or agencies receiving FTI for the first time, unless an independent security assessment or IRS risk-based assessment is performed that includes the IRS requirements for the security of FTI, the assessment is reviewed and approved/prepared by the Office of Safeguards, and any significant security deficiencies identified are resolved.

> ***Management's Response:*** The IRS partially agreed with the recommendation. The IRS will conduct an initial risk-based assessment before authorizing the release of FTI to

an agency for the first time. The Office will develop a comprehensive policy to detail agency requirements to include an independent security assessment, IRS risk-based assessment, or a modified on-site review prior to initial release of FTI. The policy will detail risk-based criteria for release of data as well as actions taken to mitigate certain vulnerabilities before approval of the data exchange. The requirement will be published in the next revision of Publication 1075.

The Office of Safeguards Does Not Require and Ensure That Agencies Conduct Proper Background Investigations

Federal agencies are required to conduct a Minimal Background Investigation on all potential employees designated as moderate risk, including individuals hired to access or use FTI. The background investigation required for Federal employees with access to FTI includes 1) fingerprints as part of the preemployment background check; 2) a National Agency Check plus credit search and checks at local law enforcement agencies where the subject has lived, worked, and/or attended school within the last five years and, if applicable, of the appropriate agency for any identified arrests; 3) a personal subject interview; 4) written inquiries to employers, schools, and references for the past five years; and 5) a periodic reinvestigation once every 10 years.

The IRS's Human Resource Division requires the Federal Minimal Background Investigation for all positions within the IRS designated as moderate risk, including positions with access to FTI. Once completed and approved, the Minimal Background Investigation would provide an IRS employee with a National Security Non-Critical Sensitive clearance and authorization to access FTI if access is required to perform the employee's official duties.

The IRS does not set specific background investigation requirements for employees and contractors at agencies receiving FTI or for agency employees and contractors with access to FTI. The IRS allows each agency that receives FTI to set its own background investigation policies and requirements. Additionally, the Office does not conduct on-site review tests on each agency's background investigation policies and procedures or on agency employees to determine if background investigations have been performed by the agency receiving FTI.

We selected 15 agencies currently receiving FTI. We requested each agency's background investigation policies and compared them to the IRS's background investigation requirements. None of the 15 agencies reviewed had background investigation policies that require the same level of background investigation that is required for IRS personnel and contractors with access to FTI. Based on our review of background policies and procedures for the 15 agencies receiving FTI, we found:

- Four of the 15 agencies conduct fingerprint testing.
- Eleven of the 15 agencies conduct State-level background investigations.

- One of the 15 agencies conducts national-level background investigations.
- Seven of the 15 agencies may hire individuals convicted of crimes. The decision to hire such individuals is based on the nature of the crime committed, the time elapsed, and the duties of the position that would be filled.
- Two of the 15 agencies conduct additional background investigations on individuals hired to access data.
- One of the 15 agencies checks sex offender registries.
- Six of the 15 agencies conduct tax compliance checks.

IRS Publication 1075 does not provide explicit requirements for background investigations agencies conduct on employees and contractors authorized to access FTI. It only requires background investigations to be performed and suggests additional checks may be necessary when agency employees will have access to entire sets of FTI records, *e.g.*, database administrators. The publication also does not require agencies to adhere to the same background investigation requirements as IRS employees and contractors with access to FTI.

During a discussion with the Office's executive management at the end of our fieldwork, management stated that the IRS should set specific minimum standards that an agency must meet for both employees and contractors with access to FTI. While executive management does not believe these standards should be an exact replication of the Minimal Background Investigation referenced for IRS employees, the standards should be set at a high level in Publication 1075. The Office's executive management believes these standards should contain requirements such as fingerprints, national and local criminal checks, and an agency-written policy specific to FTI.

Inconsistent agency polices and background investigations are being implemented/performed for agency employees and contractors with access to FTI. Agency employees and contractors with access to FTI do not have to obtain the same type of background investigation as IRS employees and contractors with access to FTI. When agency background investigation policies and procedures are not consistent with the IRS's background investigation policy and the Office does not conduct tests related to background investigations, agencies may hire individuals with backgrounds unsuited for access to FTI. The lack of specific background investigation requirements by the Office for agency personnel and contractors with access to FTI creates a significant risk that FTI provided may be subjected to unauthorized use and disclosure. In addition, the IRS cannot assure taxpayers that their FTI is properly safeguarded.

Recommendations

The Deputy Commissioner for Operations Support should:

Recommendation 2: Establish and ensure that background investigation requirements for all agency employees and contractors that have access to FTI are consistent with the IRS's background investigation requirements for access to FTI.

> ***Management's Response:*** The IRS agreed with this recommendation. The Office of Safeguards will evaluate the current IRS standards for background investigations and develop specific requirements for external agency employees and the agency's contractors authorized to access FTI that are subject to IRC § 6103(p)(4) oversight. These standards will be published in Publication 1075 and compliance will be evaluated as part of the on-site review process.

Recommendation 3: Include background investigation validation tests during the Office of Safeguards' on-site reviews for all agencies receiving FTI.

> ***Management's Response:*** The IRS agreed with this recommendation. Once the specific background investigation requirements for external agencies and contractors are established and published, the validation testing will become part of each on-site review. Specific tests will be developed and training delivered to staff to ensure that a random sampling of investigations is evaluated.

The Office of Safeguards Needs to Strengthen Its Congressional Reporting and On-Site Information Technology Security Testing Processes

Management oversight of congressional reporting requirement needs improvement

I.R.C. § 6103(p)(5) and IRM 11.3.36 require the Office to annually report to Congress on the procedures and safeguards of agencies that receive FTI. IRM Section 11.3.36.13(2) indicates the report will be submitted internally to the Director of the Office for approval on or before March 31 of each year. The report is then submitted through appropriate management levels for the IRS Commissioner's signature before it is issued to the U.S. Congress, U.S. House of Representatives Committee on Ways and Means, U.S. Senate Committee on Finance, and Joint Committee on Taxation.

The Office's annual report to Congress for Calendar Years 2010, 2011, and 2012 was not submitted to the Director of the Office timely, and the Calendar Year 2010 and 2011 reports were not issued to the required U.S. congressional committees timely. The Calendar Year 2010 annual report was submitted to the Office's Director in May 2011, the Calendar Year 2011 annual report was submitted in May 2012, and the Calendar Year 2012 annual report was

submitted in April 2013. During the fieldwork for this audit, the annual reports for Calendar Years 2010, 2011, and 2012 were all submitted to the required U.S. congressional committees in May 2013.

The Office's management does not have effective management controls established to ensure that the annual report on the procedures and safeguards of agencies that receive FTI is timely submitted to the required U.S. congressional committees. When the appropriate congressional committees are not provided with timely reports of the procedures and safeguards of agencies that receive FTI, the committees cannot provide timely oversight of the IRS's FTI-sharing activities and agencies' accountability for securing FTI.

Agency on-site reviews of information technology security requirements need improvement

I.R.C. § 6103(p)(4), IRM 11.3.36, and Publication 1075 require that access to FTI be restricted to only persons whose duties or responsibilities require access. It is the responsibility of the Office to review information technology infrastructures for agencies receiving FTI. The Office is also required to ensure that these agencies have built required security controls, according to I.R.C. § 6103(p)(4), IRM 11.3.36, and Publication 1075, into their information technology infrastructures.

The Office's information technology specialists use information technology security test plans designed to identify vulnerabilities in agencies' information technology environments. There are test plans designed for each type of environment and software/application in use by the agencies. These security test plans are comprised of multiple subtests that receive a "pass" or "fail" rating. An overall percentage score is calculated based on the total number of tests passed versus tests conducted. However, the test plans do not emphasize higher risk vulnerabilities as all tests are equally weighted. This provides an overall pass rate that is not representative of the risk to the FTI stored in these information technology environments.

The Office does not require information technology security test plans to be weighted according to risk because it does not have written policies and procedures that require the test plans be designed with subtests weighted according to the FTI risk to unauthorized disclosure and use. Using information technology security tests that are equally weighted does not adequately determine the actual risk to FTI stored in the agencies' information technology environment. As a result, the Office cannot attest to taxpayers that their FTI is safeguarded from unauthorized access and use.

Recommendations

The Deputy Commissioner for Operations Support should:

Recommendation 4: Establish roles and responsibilities for ensuring that the annual report to Congress on the procedures and safeguards of agencies that receive FTI is delivered timely.

Management's Response: The IRS independently took action on this issue prior to the recommendation. Procedures to compile the report were streamlined, and the annual report for Calendar Year 2013 was timely submitted to Congress.

Office of Audit Comment: During the fieldwork for this audit, the IRS had not submitted its annual report to Congress for Calendar Years 2010 and 2011. After the audit team requested the annual reports, the IRS took action on this issue by ensuring that the 2010, 2011, and 2012 annual reports were submitted to Congress in May 2013.

Recommendation 5: Ensure that the significance of each information technology security test is weighted according to the FTI risk to unauthorized disclosure and use.

Management's Response: The IRS agreed with this recommendation. The Office of Safeguards started the process of ranking each individual test case used to review systems based on severity. Once completed, the scoring will provide a more accurate risk-based ranking of devices that receive, process, store, and transmit FTI.

The Office of Safeguards' Program Controls Need Improvement

The Office's list of agencies receiving FTI and the agency on-site review schedule need improvement

I.R.C. § 6103(p)(4), IRM 11.3.36, and Publication 1075 require that the IRS maintain a permanent system of standardized records or accountings of all requests for inspection or disclosure of FTI and of FTI inspected or disclosed. The GLDS business unit is responsible for maintaining complete and current documentation of the agencies that receive FTI under I.R.C. § 6103(p)(4) and records of the data elements that are provided to the agency.

The Office is also responsible, once FTI has been provided to an agency, to ensure that on-site reviews of that agency are conducted at a minimum of once every three years. The Office develops annual review plans for all agencies on record as receiving FTI from the IRS to ensure that all agencies are reviewed once every three years. The Office maintains records of its on-site reviews in the Electronic Disclosure Information Management System.

We compared the list of all agencies authorized to receive FTI to the schedules for the Office's on-site reviews for Fiscal Years 2011, 2012, and 2013. We found:

- Seven agencies were not reviewed within the required three-year time frame.
- Five agencies are presently scheduled to be reviewed after the required three-year time frame.
- Two agencies scheduled to be reviewed in Fiscal Year 2013 were not included on the list.
- Fifteen agencies on the list are not currently receiving FTI and are not designated as such.

The Office does not have sufficient management oversight and written policies and procedures in place to ensure that all agencies are reviewed within the three-year requirement and to ensure that the agency list is accurately and timely updated to reflect current FTI receipt status. Without effective management oversight and written policies and procedures in place, the Office cannot fulfill its responsibility for oversight of the safeguard controls in place at agencies receiving FTI a minimum of every three years. The Office also cannot assure taxpayers that their FTI is protected.

Timeliness of document delivery/receipt and reviews and the completeness of agency files need improvement

IRM 11.3.36 and Publication 1075 require agencies to submit to the Office an SPR at a minimum of every six years or when significant changes in their safeguarding procedures occur, and agencies must submit an SAR annually. The SPR and SAR describe in detail the safeguard procedures agencies implement in accordance with I.R.C. § 6103(p)(4), IRM 11.3.36, and Publication 1075 for the safeguarding of FTI. The SPR must be reviewed after receipt by the Office within 60 calendar days, and the SAR must be reviewed by the Office within 45 calendar days. After the Office completes the review of the SPR or the SAR, it is submitted along with a delivery acceptance form (reflecting the delivery dates and due dates) for quality review. Once approved, an acceptance letter is submitted to the agency.

The Office review teams are required to conduct on-site reviews of agencies at a minimum of once every three years. The reviews are designed to ensure compliance with I.R.C. § 6103(p)(4), IRM 11.3.36, and Publication 1075 regarding recordkeeping, secure storage, restricting access, other safeguards related to employee awareness and internal inspections, reporting requirements, and disposal of FTI. After the Office review team completes an on-site review, it issues an interim Safeguard Review Report (SRR) and an interim CAP report within 45 calendar days of the on-site review closing conference. The agency has 45 calendar days to respond to the interim SRR, after which the review team has 45 calendar days to issue a final SRR and a final CAP report. Publication 1075 requires agencies to submit, to the Office, biannual CAP reports that address any unresolved deficiencies until all deficiencies have been resolved and the corrective actions taken have been approved by the Office. The Office's information technology specialists review and monitor incoming biannual CAP reports.

The Office requires agencies to correct deficiencies within the established time frame for each category. The Office categorizes deficiencies by risk, and the risk is based on the potential for loss, breach, or misuse of FTI. A category of catastrophic is the most serious, and agencies must correct this type of deficiency within three months of the on-site review closing conference. There are three other categories of deficiencies by risk: significant, which must be corrected within six months; moderate, which must be corrected within nine months; and limited, which must be corrected within 12 months.

The Office is required to keep workpaper documentation of its on-site reviews and mandatory reporting requirements for all agencies that are receiving FTI. The workpapers from the Office's

on-site reviews provide the evidence to support the conclusions and recommendations contained in the SRR. The workpapers serve as the connecting link between the on-site review and the SRR, provide the sole support that the Office is fulfilling its responsibilities for oversight, and should support the deficiencies identified and conclusions presented in the SRR.

We selected a statistically valid random sample[7] of 50 agencies from a population of 280 agencies that received FTI during Fiscal Year 2013. For the selected agencies, we analyzed the on-site review documents contained in the Office's SharePoint site. During our review, we identified agencies in our sample of 50 for which we were unable to perform a specific test. When this occurred, we determined the test could not be performed for the selected agency for three main reasons:

1. The report/document being tested, *e.g.*, SPR, SPR delivery acceptance form, SPR and SAR acceptance letters, closing conference reports, interim reports, responses to the interim reports, and final reports, was missing from the agency's file in the Office's database.
2. We were unable to determine the specific outcome of the report/document for that specific test. For example, an agency report may have been incomplete and missing the necessary information or the determination of the test outcome was contingent on another report/document that was missing.
3. The report/document was not applicable to the specific test for that agency. For example, if an agency does not receive FTI, no tests conducted would apply to that agency or the determination of the test outcome of a report/document was contingent on another report/document that was incomplete.

Therefore, for the three main reasons mentioned, the number of agencies tested for a specific report/document will not equal the sample size of 50 because all tests could not be performed for all agencies.

We identified several deficiencies for the sample of 50 agency files reviewed. Figure 2 provides a summary of our sample test results for timeliness of document delivery/receipt and review.

[7] The point estimate projections, shown in footnotes, are based on a two-sided 95 percent confidence interval.

Figure 2: Timeliness of Document Delivery/Receipt and Review

Description of Timeliness Deficiency	Number of Agencies	Percentage of Agencies	Range of Calendar Days Over the Timeliness Requirement
The SPR was not timely received.	3 of 41[8]	7.32%	286 to 814 days late
The SAR was not timely received.	19 of 34[9]	55.9%	1 to 151 days late
The contractor did not timely review the SPR.	32 of 37[10]	86.5%	3 to 1,276 days late
The contractor did not timely review the SAR.	26 of 43[11]	60.5%	1 to 229 days late
The responses to interim reports were not timely received.	28 of 35[12]	80.0%	2 to 324 days late
The biannual CAP reports were not timely received.	6 of 13[13]	46.2%	5 to 46 days late
Corrective actions for catastrophic deficiencies were not timely received.	9 of 13[14]	69.2%	162 to 927 days late
The interim report was not timely issued.	13 of 37[15]	35.1%	9 to 551 days late
The final report was not timely issued.	10 of 18[16]	55.6%	4 to 259 days late

Source: Treasury Inspector General for Tax Administration analysis of documents obtained from the Office's SharePoint site.

[8] We estimate that the Office did not receive SPRs timely from 19 of the 280 agencies. We are 95 percent confident that the true number of agencies in the population is between four and 51.
[9] We estimate that the Office did not receive SARs timely from 106 of the 280 agencies. We are 95 percent confident that the true number of agencies in the population is between 69 and 148.
[10] We estimate that the Office did not review SPRs timely for 219 of the 280 agencies. We are 95 percent confident that the true number of agencies in the population is between 175 and 250.
[11] We estimate that the Office did not review SARs timely for 155 of the 280 agencies. We are 95 percent confident that the true number of agencies in the population is between 112 and 196.
[12] We estimate that the Office did not receive responses to interim reports timely from 178 of the 280 agencies. We are 95 percent confident that the true number of agencies in the population is between 134 and 217.
[13] We estimate that the Office did not receive biannual CAP reports timely from 58 of the 280 agencies. We are 95 percent confident that the true number of agencies in the population is between 22 and 111.
[14] We estimate that the Office did not receive corrective action for catastrophic deficiencies timely from 54 of the 280 agencies. We are 95 percent confident that the true number of agencies in the population is between 26 and 93.
[15] We estimate that the Office did not issue interim reports timely to 83 of the 280 agencies. We are 95 percent confident that the true number of agencies in the population is between 47 and 127.
[16] We estimate that the Office did not issue final reports timely to 108 of the 280 agencies. We are 95 percent confident that the true number of agencies in the population is between 57 and 166.

The Office maintains the on-site review records and mandatory reporting for agencies receiving FTI using a folder for each agency on a SharePoint site. We performed testing on our sample of 50 agencies and determined that required documentation was missing from the agency folders. Figure 3 provides a summary of the test results for missing required documentation.

Figure 3: Missing Required Documentation From Agency Folders

Missing Required Document	Number of Agencies	Percentage of Agencies
Current SPR	5 of 46[17]	10.9%
SPR delivery acceptance form	9 of 46[18]	19.6%
SPR acceptance letter	8 of 46[19]	17.4%
SAR acceptance letter	2 of 45[20]	4.4%
Closing conference report	4 of 45[21]	8.9%
Interim report	4 of 43[22]	9.3%
Response to interim report	3 of 39[23]	7.7%
Final report	23 of 42[24]	54.8%

Source: Treasury Inspector General for Tax Administration analysis of the Office's SharePoint site.

In addition to the results from the sample items presented in Figures 2 and 3, these on-site reviews contained deficiencies identified by the Office reviews, but in many instances these deficiencies were not corrected timely by the agencies. In our analysis of the review files for the 50 sampled agencies, we identified that 14 of the 50 agencies reviewed had catastrophic deficiencies. Specifically:

[17] We estimate that the Office did not have in its database current SPRs for 28 of the 280 agencies. We are 95 percent confident that the true number of agencies in the population is between nine and 61.
[18] We estimate that the Office did not have in its database SPR delivery acceptance forms for 50 of the 280 agencies. We are 95 percent confident that the true number of agencies in the population is between 24 and 88.
[19] We estimate that the Office did not have in its database SPR acceptance letters for 45 of the 280 agencies. We are 95percent confident that the true number of agencies in the population is between 20 and 82.
[20] We estimate that the Office did not have in its database SAR acceptance letters for 11 of the 280 agencies. We are 95 percent confident that the true number of agencies in the population is between one and 39.
[21] We estimate that the Office did not have in its database closing conference reports for 22 of the 280 agencies. We are 95 percent confident that the true number of agencies in the population is between six and 54.
[22] We estimate that the Office did not have in its database interim reports for 22 of the 280 agencies. We are 95 percent confident that the true number of agencies in the population is between six and 54.
[23] We estimate that the Office did not have in its database a response to the interim report for 17 of the 280 agencies. We are 95 percent confident that the true number of agencies in the population is between four and 46.
[24] We estimate that the Office did not have in its database final reports for 129 of the 280 agencies. We are 95 percent confident that the true number of agencies in the population is between 89 and 170.

- Nine of the 14 agencies had catastrophic deficiencies that were not corrected timely.
- Six of the 14 agencies had catastrophic deficiencies between 583 and 1,017 calendar days old and were not corrected at the completion of our review.
- One of the 14 agencies had 19 catastrophic deficiencies, or 70 percent of the total deficiencies identified.

The Office's management does not have documented policies and procedures, roles and responsibilities, performance metrics, and performance metrics reporting to ensure that requirements are met. Additionally, the Office only has legal enforcement authority in I.R.C. § 6103(p)(4) and (7) to withhold FTI if agencies do not timely correct deficiencies or establish required safeguards. The Office does not have legal authority to impose any penalties or other enforcement tactics to compel agency compliance.

Without the receipt and submission of complete and timely reporting by the Office and agencies receiving FTI, the Office cannot ensure that FTI received by agencies is properly safeguarded. When documentation is missing within agency review files, there is not sufficient evidence that the Office has performed its oversight responsibilities of agencies receiving FTI. Additionally, the Office does not restrict an agency's access to FTI data until deficiencies identified are corrected. Deficiencies not corrected could lead to internal or external breaches of FTI. Therefore, the Office cannot completely assure taxpayers that their FTI is protected.

Management actions

During this audit, the Office started to make efforts to add controls that will assist in its oversight of agencies that receive FTI. It recently migrated to a single database, called Entellitrak. According to the Office's management, this new system will be the single application through which all of the Office's review documentation, reporting, and on-site review schedules are tracked and maintained. Prior to the deployment of Entellitrak, three independent databases were used to track reports, deficiencies, and related work. Management believes combining the functionality of the three databases into one will assist in supporting and managing the Office as more agencies request FTI.

Additionally, as of April 2013, the Office conducted status meetings with its contractor information technology specialists to ensure that SPR and SAR reviews are conducted timely. Office management also has a procedure that should increase the oversight of agencies by contacting agencies when SARs and CAP reports are delinquent.

Recommendations

The Deputy Commissioner for Operations Support should:

Recommendation 6: Establish roles and responsibilities for ensuring that the master list of agencies receiving FTI subject to I.R.C. § 6103(p)(4) from the IRS is timely updated and maintained.

> ***Management's Response:*** The new Entellitrak management information system deployed in August 2013 provides enhanced and accurate tracking capabilities for the list of active agencies, reports, and related documents.

Recommendation 7: Establish roles and responsibilities for ensuring that the Office of Safeguards' review schedule is maintained and updated timely.

> ***Management's Response:*** The IRS agreed with this recommendation. The Office of Safeguards will develop a more comprehensive review schedule process that lists all agencies and documents all risk-based deviations from the three-year review cycle. There are multiple reasons to adjust the on-site review dates for certain agencies, and specific criteria will be implemented to ensure that proper evaluation has taken place for any review changes.

Recommendation 8: Establish a review process for the Office of Safeguards' database to ensure that all required agency documents are tracked, maintained, and accurately documented in each agency's file.

> ***Management's Response:*** The new Entellitrak management information system deployed in August 2013 provides enhanced and accurate tracking capabilities for the list of active agencies, reports, and related documents. Complete agency files are now monitored and audited as part of the quality review process to ensure proper inclusion of all required documents.

Appendix I

Detailed Objective, Scope, and Methodology

Our overall objective was to determine whether the Office of Safeguards effectively provides oversight of agencies that receive FTI. To determine the effectiveness of the oversight of agencies, we interviewed management, observed two on-site agency reviews, obtained the Office's annual reports to Congress, and reviewed policies on background investigations of agencies that receive FTI, information technology security test plans, and the Office's agency files of report documents.

To accomplish our objective, we:

I. Evaluated the Office's procedures and determined its adequacy in protecting FTI.

   A. Conducted walkthroughs of two agencies that receive FTI.

   B. Reviewed the guidance used by the Office and compared it to I.R.C. § 6103(p)(4) to determine whether it is consistent with the law.

   C. Reviewed Government criteria and compared it to Publication 1075, *Tax Information Security Guidelines for Federal, State, and Local Agencies*, and other additional guidance the Office uses to identify internal controls that would ensure adequate protection of FTI.

   D. Determined whether all agencies that receive FTI are reviewed at least once every three years in accordance with IRM 11.3.36 by comparing the Office's list of agencies that receive FTI to the most recent three-year on-site review schedule.

II. Determined whether the Office adequately monitored the agencies that receive FTI.

   A. Through discussions with management, determined how the Office tracks and controls the documents received from agencies.

   B. Conducted a statistical sample[1] of 50 agencies from a population of 280 agencies that received FTI in Fiscal Year 2013. We determined the Office's maintenance and timeliness of the agencies' report documents issued to and submitted by the agencies. We reviewed agencies that had an on-site review from the Office conducted in Fiscal Years 2011, 2012, or 2013 and did not identify any agencies that were reviewed more than once during the three-year cycle. We determined whether report documents the

[1] A contract statistician assisted with developing our sampling plans and projections. We selected a statistical sample because we wanted to estimate the total number of agencies for which report documents were missing and/or reviewed or received untimely.

Office receives from the agencies are kept up to date in its databases and obtained timely. We projected two-sided 95 percent confidence intervals for the population exception rate and the population number of exception agencies using a pass or fail methodology.

C. We reviewed the SPRs and the SARs for the random statistical sample of 50 agencies from Step II.B. to determine maintenance and timeliness of reviews and receipt of the reports.

D. Reviewed interim reports and final reports for the random statistical sample of 50 agencies from Step II.B. to determine maintenance and timeliness of issuance.

E. Reviewed CAP reports for the random statistical sample of 50 agencies from Step II.B. to determine maintenance and timeliness of reviews and receipt of the reports.

III. Conducted a random sample[2] of 15 agencies from a population of 62 agencies that received FTI in Fiscal Year 2013. We requested each agency's background investigation policies and procedures. We reviewed policies and procedures for the employee background investigations conducted by 15 agencies to determine consistency with the IRS's background policies and procedures for employees with access to FTI.

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: the IRS's policies, procedures, and practices for providing oversight to agencies that receive FTI in accordance with I.R.C. § 6103(p)(4). We evaluated these controls by interviewing management and reviewing agencies' policies on background investigations, information technology security test plans, and the Office's agency files and report documents.

[2] We used a random sample to ensure that each agency had an equal chance of being selected, which enabled us to obtain sufficient evidence to support our results.

Appendix II

Major Contributors to This Report

Alan R. Duncan, Assistant Inspector General for Audit (Security and Information Technology Services)
Danny Verneuille, Director
John Ledford, Audit Manager
Chanda Stratton, Lead Auditor
Ryan Perry, Senior Auditor
Anthony Morrison, Auditor
Mike Mohrman, Senior Information Technology Specialist

Appendix III

Report Distribution List

Commissioner C
Office of the Commissioner – Attn: Chief of Staff C
Director, Privacy, Governmental Liaison, and Disclosure OS:P
Director, Governmental Liaison, Disclosure, and Safeguards OS:P:GLDS
Director, Safeguards OS:P:S
Director, Office of Legislative Affairs CL:LA
Director, Office of Program Evaluation and Risk Analysis RAS:O
Chief Counsel CC
National Taxpayer Advocate TA
Office of Internal Control OS:CFO:CPIC:IC
Audit Liaisons:
    Director, Privacy, Governmental Liaison and Disclosure OS:P:PGLD
    Director, Governmental Liaison, Disclosure and Safeguards OS:P:GLDS

Appendix IV

Glossary of Terms

Term	Definition
Affordable Care Act Legislation	The Patient Protection and Affordable Care Act of 2010[1] and the Health Care and Education Reconciliation Act of 2010[2] are collectively referred to as the ACA. In March 2010, President Obama signed the ACA into law. The legislation seeks to provide more Americans with access to affordable health care, enforce patient/consumer protections, and provide Government subsidies for people who cannot afford insurance.
Catastrophic	The most serious deficiency identified during on-site reviews. Agencies must correct this type of deficiency within three months of the on-site review closing conference.
Electronic Disclosure Information Management System	Used by the Office of Safeguards prior to the implementation of the Entellitrak database system for tracking and controlling, work planning, and management reporting.
Entellitrak	Integrated system used to capture, track, and manage data related to agencies that receive FTI. The Office of Safeguards implemented Entellitrak in August 2013. It combines the functionality of the former multiple software applications the Office of Safeguards used into a single integrated solution which will more efficiently support and manage the increased business needs of the Office of Safeguards.
Federal Tax Information	Confidential tax information reported to the IRS and synonymous with tax returns and return information.
Fiscal Year	Any yearly accounting period, regardless of its relationship to a calendar year. The Federal Government's fiscal year begins on October 1 and ends on September 30.

[1] 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.
[2] Pub. L. No. 111-152, 124 Stat. 1029. (See Affordable Care Act, *infra*).

Term	Definition
Internal Revenue Code Section 6103(p)(4)	Section of the I.R.C. that provides safeguard regulations governing confidentiality of FTI for agencies that receive FTI.
Internal Revenue Manual Section 11.3.36[3]	Section of the IRS's IRM that is dedicated to the Office of Safeguards to provide procedural and operational supervision for its staff.
IRS Publication 1075, *Tax Information Security Guidelines for Federal, State, and Local Agencies*	Provides FTI security guidelines for Federal, State, and local agencies required to establish procedures to ensure the adequate protection of FTI received.
National Institute of Standards and Technology Special Publication 800-53, *Recommended Security Controls for Federal Information Systems and Organizations*[4]	Provides standards and guidelines for information security, including minimum requirements for Federal information technology systems.
SharePoint Site	Used by the Office of Safeguards prior to the implementation of the Entellitrak database system for maintaining report documents related to the Office's reviews of agencies that receive FTI.

[3] Dated Aug. 2008.
[4] Dated Aug. 2009.

Appendix V

Management's Response to the Draft Report

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

DEPUTY COMMISSIONER

August 28, 2014

MEMORANDUM FOR DEPUTY INSPECTOR GENERAL FOR AUDIT

FROM: Peggy Sherry
Deputy Commissioner for Operations Support

SUBJECT: Draft Audit Report – The Office of Safeguards Should Improve Management Oversight and Internal Controls to Ensure the Effective Protection of Federal Tax Information (Audit #201320029)

Thank you for the opportunity to respond to the above referenced audit report. The IRS takes data security very seriously and the Office of Safeguards has a key role to ensure that federal tax information shared with our agency partners under Internal Revenue Code (IRC) § 6103(p)(4) is properly protected at all times.

The Office of Safeguards has undergone significant change over the past two years. The IRS increased the Safeguards staffing to accommodate the recent legislative changes that allowed for data sharing with many new agencies including State Departments of Correction and Health Insurance Exchanges. This effort required extensive coordination, training and support to ensure the appropriate staff was available to manage the significant increase in workload.

As a part of the audit, Treasury Inspector General for Tax Administration (TIGTA) reviewed the legacy Safeguards inventory system that tracked and maintained safeguard reports, findings and correspondence. This system relied on SharePoint document repositories for reports and correspondence as well as another database that maintained the review findings. A new comprehensive inventory management system was deployed while the audit was in process that remediates multiple concerns identified in the audit report. This new system was not evaluated by TIGTA.

Attached are the IRS comments to your recommendations. If you have any questions, please contact me at (202) 317-3950, or a member of your staff may contact Mary Howard, Director, Privacy, Governmental Liaison and Disclosure at (202) 317-6449.

Attachment

Attachment

Recommendation 1: Establish policies and procedures to require that on-site agency reviews are conducted prior to the initial release of FTI for any new systems or agencies receiving FTI for the first time, unless an independent security assessment or IRS risk-based assessment is performed that includes the IRS requirements for the security of FTI, the assessment is reviewed and approved/prepared by the Office of Safeguards, and any significant security deficiencies identified are resolved.

Corrective Action: The IRS partially agrees with the recommendation. IRS will conduct an initial risk-based assessment before authorizing the release of Federal Tax Information (FTI) to an agency for the first time. The Office of Safeguards will develop a comprehensive policy to detail agency requirements to include an independent security assessment, IRS risk-based assessment or a modified on-site review prior to initial release of FTI. The policy will detail risk based criteria for release of data as well as actions taken to mitigate certain vulnerabilities before approval of the data exchange. This requirement will be published in the next revision of Publication 1075 *Tax Information Security Guidelines for Federal, State and Local Agencies.*

Implementation Date: December 31, 2014.

Responsible Official: Director, Privacy, Governmental Liaison and Disclosure.

Corrective Action Monitoring Plan: Establish a timeline of necessary actions that incorporates expected outcomes and dates to successfully accomplish stated tasks.

Recommendation 2: Establish and ensure that background investigation requirements for all agency employees and contractors that have access to FTI are consistent with the IRS's background investigation requirements for access to FTI.

Corrective Action: The IRS agrees with this recommendation. The Office of Safeguards will evaluate the current IRS standards for background investigations and develop specific requirements for external agency employees and the agency's contractors authorized to access FTI that are subject to IRC § 6103(p)(4) oversight. These standards will be published in the Publication 1075 and compliance will be evaluated as part of the on-site review process.

Implementation Date: January 1, 2015.

Responsible Official: Director, Privacy, Governmental Liaison and Disclosure.

Corrective Action Monitoring Plan: Establish a timeline of necessary actions that incorporates expected outcomes and dates to successfully accomplish stated tasks.

Attachment

2

Recommendation 3: Include background investigation validation tests during the Office of Safeguards on-site reviews for all agencies receiving FTI.

Corrective Action: The IRS agrees with this recommendation. Once the specific background investigation requirements for external agencies and contractors are established and published, the validation testing will become part of each on-site review. Specific tests will be developed and training delivered to staff to ensure that a random sampling of investigations is evaluated.

Implementation Date: January 1, 2015.

Responsible Official: Director, Privacy, Governmental Liaison and Disclosure.

Corrective Action Monitoring Plan: Establish a timeline of necessary actions that incorporates expected outcomes and dates to successfully accomplish stated tasks.

Recommendation 4: Establish roles and responsibilities for ensuring that the annual report to Congress on the procedures and safeguards of agencies that receive FTI is delivered timely.

Corrective Action: The IRS independently took action on this issue prior to the recommendation. Procedures to compile the report were streamlined and the annual report for calendar year 2013 was timely submitted to Congress.

Implementation Date: Implemented.

Responsible Official: N/A

Corrective Action Monitoring Plan: N/A

Recommendation 5: Ensure that the significance of each information technology security test is weighted according to the FTI risk to unauthorized disclosure and use.

Corrective Action: The IRS agrees with this recommendation. The Office of Safeguards started the process of ranking each individual test case used to review systems based on severity. Once completed, the scoring will provide a more accurate risk based ranking of devices that receive, process, store and transmit FTI.

Implementation Date: December 1, 2014.

Responsible Official: Director, Privacy, Governmental Liaison and Disclosure.

Attachment

3

Corrective Action Monitoring Plan: Establish a timeline of necessary actions that incorporates expected outcomes and dates to successfully accomplish stated tasks.

Recommendation 6: Establish roles and responsibilities for ensuring that the master list of agencies receiving FTI subject to I.R.C. § 6103(p)(4) from the IRS is timely updated and maintained.

Corrective Action: The new e-TRAK management information system deployed in August 2013 provides enhanced and accurate tracking capabilities for the list of active agencies, reports and related documents.

Implementation Date: Implemented.

Responsible Official: N/A

Corrective Action Monitoring Plan: N/A

Recommendation 7: Establish roles and responsibilities for ensuring that the Office of Safeguards' review schedule is maintained and updated timely.

Corrective Action: This IRS agrees with this recommendation and the Office of Safeguards will develop a more comprehensive review schedule process that lists all agencies and documents all risk based deviations from the three year review cycle. There are multiple reasons to adjust the on-site review dates for certain agencies and specific criteria will be implemented to ensure that proper evaluation has taken place for any review changes.

Implementation Date: March 1, 2015.

Responsible Official: Director, Privacy, Governmental Liaison and Disclosure.

Corrective Action Monitoring Plan: Establish a timeline of necessary actions that incorporates expected outcomes and dates to successfully accomplish stated tasks.

Recommendation 8: Establish a review process for the Office of Safeguards' database to ensure that all required agency documents are tracked, maintained, and accurately documented in each agency's file.

Corrective Action: The new e-TRAK management information system deployed in August 2013 provides enhanced and accurate tracking capabilities for the list of active agencies, reports and related documents. Complete agency files are now monitored and audited as part of the quality review process to ensure proper inclusion of all required documents.

Attachment

4

Implementation Date: Implemented

Responsible Official: N/A

Corrective Action Monitoring Plan: N/A