TREASURY INSPECTOR GENERAL FOR TAX ADMINISTRATION

Affordable Care Act: Expanded Guidance Provided Assistance to the Exchanges, but Greater Assurance of the Protection of Federal Tax Information Is Needed

September 16, 2014

Reference Number: 2014-23-070

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

AFFORDABLE CARE ACT: EXPANDED GUIDANCE PROVIDED ASSISTANCE TO THE EXCHANGES, BUT GREATER ASSURANCE OF THE PROTECTION OF FEDERAL TAX INFORMATION IS NEEDED

Highlights

Final Report issued on September 16, 2014

Highlights of Reference Number: 2014-23-070 to the Internal Revenue Service Director, Privacy, Governmental Liaison, and Disclosure.

IMPACT ON TAXPAYERS

Affordable Care Act (ACA) legislation authorized States to create marketplaces, called "Exchanges," to simplify the search for health coverage by providing multiple options in one place. Eligible taxpayers who purchase health insurance through an Exchange may qualify for and request a refundable tax credit to assist with paying their health insurance premium. The ACA authorized the IRS to disclose limited tax return information to the Exchanges when an applicant seeks financial assistance. To protect the confidentiality of the Federal Tax Information (FTI) disclosed to the Exchanges, the IRS has established safeguards the Exchanges must employ. If required safeguards are not established and maintained, FTI is at an increased risk of unauthorized disclosure and use.

WHY TIGTA DID THE AUDIT

This audit was initiated to determine whether the IRS Office of Safeguards has implemented sufficient policies and procedures to ensure that ACA Exchanges are adequately protecting FTI received from the IRS. The IRS is responsible for approving agencies to receive FTI and ensuring that these agencies have controls in place to adequately protect the confidentiality of FTI and prevent its unauthorized disclosure and use.

WHAT TIGTA FOUND

The IRS provided staff dedicated to facilitating the readiness of ACA Exchanges to receive FTI and meet the October 1, 2013, deadline for enrollment for health insurance to begin. Also, TIGTA observed the Office of Safeguards while it conducted on-site reviews of two Exchanges and found its on-site testing procedures to be generally adequate.

However, additional procedures are needed to provide greater assurance that FTI will be protected prior to approving its release. Specifically, IRS procedures did not require the Exchanges or other agencies to submit an initial independent security assessment report that could help to evaluate risk levels and the status of required security controls. The current documentation on which the Office of Safeguards bases its approval decision for release of FTI does not provide sufficient evidence that required controls have been implemented. TIGTA also found deficiencies in procedures related to obtaining signed system security authorizations and ensuring that on-site reviews of agencies that have deployed new systems occur in a timely manner.

WHAT TIGTA RECOMMENDED

TIGTA recommended that the Director, Privacy, Governmental Liaison, and Disclosure, ensure that IRS Office of Safeguards' policy and procedures are revised so that independent assessments of security controls and signed system security authorizations are received and reviewed by the Office of Safeguards before approving the release of FTI, and on-site reviews of agencies that have deployed new systems should be prioritized according to risk and scheduled in a timely manner.

IRS management agreed with our recommendations. The IRS plans to require agencies to submit an initial independent security assessment and signed system security authorization. The IRS also plans to develop procedures to use the independent security assessment to validate that controls are implemented as described by the agencies, evaluate risk prior to releasing FTI, and prioritize on-site reviews.

TREASURY INSPECTOR GENERAL
FOR TAX ADMINISTRATION

DEPARTMENT OF THE TREASURY

WASHINGTON, D.C. 20220

September 16, 2014

MEMORANDUM FOR DIRECTOR, PRIVACY, GOVERNMENTAL LIAISON, AND DISCLOSURE

FROM: Michael E. McKenney
Deputy Inspector General for Audit

SUBJECT: Final Audit Report – Affordable Care Act: Expanded Guidance Provided Assistance to the Exchanges, but Greater Assurance of the Protection of Federal Tax Information Is Needed (Audit # 201420302)

This report presents the results of our review of whether the Internal Revenue Service (IRS) Office of Safeguards has implemented sufficient policies and procedures to ensure that Affordable Care Act[1] Exchanges are adequately protecting Federal Tax Information received from the IRS. This audit was initiated as part of the Treasury Inspector General for Tax Administration's Fiscal Year 2014 Annual Audit Plan and addresses the major management challenge of Implementing the Affordable Care Act and Other Tax Law Changes.

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

[1] The Health Care and Education Reconciliation Act of 2010 and the Patient Protection and Affordable Care Act, 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.

Table of Contents

Abbreviations

ACA	Affordable Care Act
CMS	Centers for Medicare and Medicaid Services
FTI	Federal Tax Information
HHS	Department of Health and Human Services
IRM	Internal Revenue Manual
IRS	Internal Revenue Service
NIST	National Institute of Standards and Technology
POA&M	Plan of Action and Milestones
SAR	Security Assessment Report
SPR	Safeguards Procedure Report
TIGTA	Treasury Inspector General for Tax Administration

Background

In March 2010, Congress passed two pieces of legislation that the President later signed into law—the Health Care and Education Reconciliation Act of 2010 and the Patient Protection and Affordable Care Act (ACA).[2] Collectively, these legislations are referred to as the ACA. ACA legislation seeks to provide more Americans with access to affordable health care. The ACA created a new structured marketplace, commonly called "Exchanges," for the sale and purchase of health insurance. The Exchanges are intended to provide a place for Americans to shop for health insurance in a competitive environment. The Exchanges should simplify the search for health coverage by providing multiple options in one place and comparing plans based on price, benefits, quality, and other important features that help consumers make a choice. The Department of Health and Human Services (HHS) and its Centers for Medicare and Medicaid Services (CMS) Division have primary responsibility for implementing the ACA, including many elements related to the Exchanges.

The ACA authorized States to establish and operate an Exchange themselves (referred to as a State-based Exchange) or may cede this authority to the HHS/CMS that was tasked with the creation of the Federal Exchange.[3] Developing the Exchanges has been a complex undertaking, involving the coordinated actions of multiple Federal,[4] State, and private stakeholders, and the creation of an information system, known as the Hub, to support connectivity and near real-time data sharing between multiple Federal and State agencies.

The ACA required that enrollment for health insurance at the Exchanges begin on October 1, 2013, for coverage that would be effective January 1, 2014. Eligible taxpayers who purchase health insurance through an Exchange may qualify for and request a refundable tax credit[5] to assist with paying their health insurance premium. This credit is called the Premium Tax Credit and is claimed on the taxpayer's Federal tax return at the end of each coverage year. This credit can also be paid in advance to a taxpayer's health insurance provider to help cover the cost of premiums. These payments are referred to as the advance payments of the Premium Tax Credit.

---

[2] 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.

[3] The ACA requires States to establish Exchanges by January 1, 2014, Pub. L. No. 111-148, § 1311(b), 124 Stat. 173. The Secretary of the HHS must establish and operate an Exchange in States that do not elect to operate an Exchange or in States where the Secretary determines, by January 1, 2013, that a State has failed to take actions necessary to establish an exchange, Pub. L. No. 111-148, § 1321(c), 124 Stat. 186.

[4] Federal agencies involved in ACA collaboration include, *e.g.*, the HHS, the Social Security Administration, the Department of Homeland Security, and the Internal Revenue Service.

[5] Any tax credit that is refundable can be used to reduce a taxpayer's tax liability to zero. Any excess of the credit beyond the tax liability can be refunded to the taxpayer.

The Internal Revenue Service's (IRS) role with respect to the ACA is to implement and administer ACA provisions that have an impact on tax administration. The IRS's role includes providing information that will support the HHS/CMS and the Exchanges in three main areas: 1) eligibility and enrollment, 2) calculating maximum Advance Premium Tax Credits, and 3) reconciling advance payments of the Premium Tax Credit with reported taxable income.[6] As part of the eligibility determination related to the Premium Tax Credit, the ACA authorized the IRS to disclose limited tax return information[7] to the Exchanges when an applicant seeks financial assistance to obtain affordable coverage under ACA provisions. Because the tax credit may be claimed in advance, the Exchange needs to determine an individual's eligibility for the tax credit at the time the individual applies for coverage through the Exchange.

The IRS's role with respect to the ACA is to implement and administer ACA provisions that have an impact on tax administration.

As of October 1, 2013, the IRS had approved 16 Exchanges (14 State-based Exchanges, the District of Columbia, and the Federal Exchange) to receive Federal Tax Information (FTI) for income verification purposes related to eligibility and enrollment under provisions of the ACA. After the IRS approves an Exchange to receive FTI, the Exchange is required to validate income-related information reported by consumers with select FTI to determine eligibility for the tax credit.

The Exchanges obtain FTI by initiating an electronic request to the IRS through the Hub. Also via the Hub, the IRS returns the authorized items of tax return information with respect to each relevant taxpayer or a response code indicating why no information is provided. The Hub is a routing tool operated by the HHS to rapidly verify the information submitted by consumers seeking a determination of what coverage options and financial assistance are available to them. The Hub does not retain FTI; it routes the information from Exchange requests and IRS responses.

[6] The IRS has developed four system components to support the Exchange effort: the Coverage Data Repository, the Income and Family Size Verification project, the Information Sharing and Reporting project, and the Premium Tax Credit project. These components work together to store taxpayer data, provide responses to Exchange stakeholders, facilitate data exchange, and calculate amounts related to the Advance Premium Tax Credit, respectively.

[7] The ACA specified information that the IRS may disclose which includes the following data elements from individual tax returns for making eligibility determinations: household income, family size, filing status, adjusted gross income, and taxable Social Security benefits.

Premium Tax Credits and cost-sharing subsidies were authorized by the ACA to help certain individuals and families with incomes between 100 percent and 400 percent of the Federal poverty level pay for Exchange coverage. To qualify for these income-based financial subsidies, individuals must also meet the criteria for eligibility for enrollment and not be eligible for other health insurance coverage that meets certain standards. Without FTI data used to support applicant-provided information about projected household income, tax credits and subsidies could be incorrectly awarded. Paying back incorrect credits all at once could be a burden on taxpayers and could lead to the need for collection actions.

Without FTI data used to support applicant-provided information, tax credits and subsidies could be incorrectly awarded.

IRS Safeguards Program

The IRS's Office of Safeguards within the Privacy, Governmental Liaison, and Disclosure Division is responsible for managing and providing oversight to agencies that receive FTI and ensuring that these agencies have controls in place to adequately protect the confidentiality of FTI and prevent unauthorized disclosure and use. The Office of Safeguards oversees FTI sharing with about 300 agencies.[8] IRS Publication 1075, *Tax Information Security Guidelines for Federal, State and Local Agencies*,[9] provides guidance to ensure that the policies, practices, controls, and safeguards employed by Federal, State, and local recipient agencies, agents, or contractors adequately protect the confidentiality of FTI.

As part of its oversight responsibilities, the Office of Safeguards conducts periodic reviews of agencies that receive FTI. These reviews entail both documentary reviews of required reports and on-site visits to validate that controls reported by agencies are in place. The on-site visits include reviews of employee awareness programs, proper disposal and secure storage of FTI, and computer security. The Office of Safeguards' approach to fulfilling its responsibilities is to promote a cooperative effort with the recipient agencies and their contractors to ensure the confidentiality of FTI. Outreach and communication are key elements in this approach. The program must also maintain viable enforcement standards and capabilities.

The IRS has been tasked with both sharing FTI for authorized program activities, such as those related to the Exchanges, and with keeping FTI safe and confidential, even when the data are not in its direct control. There is high inherent risk in this situation.

The IRS Safeguards program has been tasked with both sharing FTI for authorized program activities, such as those related to the Exchanges, and with keeping FTI safe and confidential, even when the data are not in its direct control. The Treasury Inspector General for Tax

[8] According to the IRS, there were 299 agencies subject to Office of Safeguards' oversight as of April 8, 2014.
[9] The IRS updated Publication 1075 in January 2014 based on the National Institute of Standards and Technology Special Publication 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations.*

Administration (TIGTA) believes that sharing sensitive FTI data with agencies and their many different environments related to management, information systems, and internal controls presents a difficult challenge and high inherent risk.[10] The Safeguards program is designed to manage and mitigate these risks.

IRS efforts can at best provide reasonable, but not absolute, assurance that FTI is adequately safeguarded. Authoritative Federal guidance states that security is *never* perfect when a system is implemented. In addition, the behavior of system users and operators may intentionally or unintentionally bypass or subvert security controls designed to protect systems and data. Changes in the system or the environment can create new vulnerabilities. Strict adherence to procedures is rare over time, and procedures become outdated. Thus, Federal standards provide for a process that monitors the effectiveness of key security controls over time and tracks efforts to address known vulnerabilities as they are identified. The IRS follows a similar methodology to help secure FTI at external agencies.

This review was performed with information obtained from the Office of Safeguards in Washington, D.C.; and at the California Health Benefit Exchange office in Sacramento, California; and the Access Health CT office in Hartford, Connecticut, during the period December 2013 through July 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.

[10] Inherent risk is the likelihood that a loss of confidentiality, integrity, or availability could occur that would materially/significantly affect the audit objectives, assuming that there are no related internal controls.

Results of Review

Expanded Guidance Provided Assistance to the Exchanges

The IRS took several steps to facilitate the readiness of the Exchanges to receive FTI. Among these steps were assigning staff dedicated to the ACA Exchanges, providing for an extensive documentation review process, making on-site visits to provide guidance on required document preparation, and coordinating with other stakeholder organizations. The IRS also was responsive to issues raised during this audit.

The IRS used the Safeguards Procedure Report (SPR) as the primary tool to assess the readiness of Exchange agencies to receive FTI. The information in the SPR describes what the agencies are doing or plan to do to address the required FTI safeguarding controls described in Publication 1075. The SPR describes how FTI will be received and processed by the agency, and how FTI will be protected from unauthorized disclosure. The IRS also used additional security documents the Exchanges supplied to the HHS/CMS to supplement the information in the SPR when assessing readiness to receive FTI. In January 2014, the SPR was replaced by the Safeguard Security Report, which, in addition to serving as an initial report to the IRS on agency safeguarding procedures, is also used as an annual reporting vehicle.

Approximately two years prior to the October 1, 2013, enrollment commencement, the IRS began its work with the HHS/CMS and the Exchanges to facilitate timely completion of the SPRs and to assist the Exchanges in understanding safeguarding controls. The IRS provided staff to oversee Exchange SPR completions from September 2012 to March 2014. From December 2012 to September 2013, staffing ranged from eight to 14 individuals (employees and contractors) to work with the Exchanges, and to review and approve the SPRs. The IRS provided access to safeguarding requirements on its website and presented the requirements at a system-wide Exchange meeting in May 2012.

The IRS also collaborated with the HHS to ensure that Publication 1075 requirements were incorporated into HHS published guidance, security agreements with the Exchanges, and incident response plans. HHS guidance prohibits the display and disclosure of FTI during application processing (either electronically or in notices), which significantly reduces the risk of exposure of FTI. The IRS participated in HHS reviews with the Exchanges to ensure that Publication 1075 requirements were fully understood and incorporated into the systems' lifecycle development. The IRS also established standing biweekly office hours to answer technical questions posed by the Exchanges.

As a result of the early IRS efforts, the Exchanges submitted initial SPRs well before the October 1, 2013, enrollment commencement. The IRS subsequently worked through multiple SPR submissions with the Exchanges, providing iterative feedback, until IRS reviewers

concluded that all safeguard controls were adequately addressed in the SPRs. The IRS emphasized that some key controls should be fully implemented or have mitigating controls before agencies would be approved to receive FTI.

In addition to the document review, the IRS went beyond its standard procedures by visiting each of the Exchanges to review the SPRs and ensure that the Exchanges understood the importance of security controls prior to approving them to receive FTI. However, no testing of security controls occurred during these initial visits. Normally, the IRS would rely on document reviews with supplemental telephone or correspondence contacts as needed. The IRS made the on-site visits because the agencies were brand-new entities and not familiar with IRS procedures. IRS teams made an on-site visit to each Exchange in the July to August 2013 time frame to review draft SPR submissions, discuss IRS requirements with Exchange personnel, and ensure that any remaining concerns were properly understood and addressed.

The IRS systems supporting data exchange among the Exchanges and Federal agencies to enroll applicants functioned largely as expected. Figure 1 shows the IRS-reported number of FTI disclosures for ACA purposes (Income and Family Size Verification) since the Hub started operating on October 1, 2013. There is no direct correlation between these numbers and Exchange enrollments reported by the HHS/CMS or any State.

Figure 1: Volume of FTI Disclosures for ACA Purposes to Exchange Agencies

Exchange	October 2013	November 2013	December 2013	January 2014	February 2014	March 2014	**Total**
15 States With Exchanges	628,614	771,439	2,132,837	1,742,567	1,655,627	3,211,161	10,142,245
Federal Exchange	910,545	1,180,460	3,278,422	1,989,276	1,682,052	3,530,360	12,571,115
Total Disclosures	1,539,159	1,951,899	5,411,259	3,731,843	3,337,679	6,741,521	22,713,360

Source: IRS Office of Safeguards' internal report.

On-Site Testing Procedures Were Generally Adequate

A safeguard review is an on-site evaluation of the use of FTI and the measures employed by the receiving agency to protect the information. The Office of Safeguards generally conducts on-site reviews once every three years. IRS policy states that agencies receiving FTI for the first time may be reviewed within one year of initial receipt of FTI. Additionally, IRS guidance directs that risk factors identified outside the reporting process should be taken into consideration in determining the timing of on-site reviews. Examples of such considerations include, but are not

limited to, a history of problems, information reported by TIGTA, or news items affecting agencies and their contractors.

We observed the IRS conduct reviews of two State Exchanges. We found that the Office of Safeguards' testing procedures were generally adequate. The IRS conducted opening and closing meetings to inform agency staff about the review process and results. The testers were thorough in administering the security testing steps and asked additional questions when needed. The IRS provided the agencies with a Preliminary Findings Report at the end of the on-site visit that listed high-level findings related to the testing.

The Office of Safeguards is in the process of procuring the Nessus vulnerability scanner to help automate the test steps. We agree that automating test processes, where possible, will increase efficiencies in terms of time required for performing the tests and in regards to providing accurate and complete automated documentation of test results.

TIGTA also discussed the benefits of revising test steps on operating systems to begin with queries that determine what ports are open and what applications are running. These queries could reduce some unnecessary tests, depending on the results. In addition, IRS management stated that they have made some changes in response to feedback from TIGTA during the audit.

- Both recommendations from TIGTA's first on-site review visit regarding penetration testing and website analysis were added to the IRS's testing plan in response to TIGTA's feedback on the templates.
- The Office of Safeguards will now request and review the agency's security testing results, during its on-site reviews, and determine (through its own testing) whether the agency is taking action on the deficiencies.
- The Office of Safeguards has added, or will add, test steps for 17 Publication 1075 controls that TIGTA identified were not tested during on-site reviews. Five of the 17 controls had been newly added to the revised Publication 1075 that the Office of Safeguards issued in January 2014 based the National Institute of Standards and Technology (NIST) Special Publication 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*.

Independent Security Assessments and Authorizations Were Not Reviewed Prior to Approving the Release of Federal Tax Information

The steps that the IRS took to provide assistance to the Exchanges were helpful; however, additional procedures are needed to provide greater assurance that FTI is protected prior to its release. IRS procedures did not require the Exchanges or other agencies to submit an initial independent Security Assessment Report (SAR) that could help evaluate risk levels at the individual agencies and be used to prioritize on-site reviews. Moreover, although the IRS has a requirement that agencies complete signed security authorizations prior to receiving FTI, the IRS

does not require these authorizations be submitted to the IRS prior to approval, and on-site reviews revealed that authorizations were not always satisfactorily completed.

Independent SARs were not reviewed prior to approving agencies to receive FTI

A best practice as required for Federal agencies[11] is that an assessment of security controls must be conducted by an independent assessor prior to issuing the initial authority to operate for all newly implemented systems. The results of the assessment are summarized in the SAR, which identifies the security vulnerabilities that should be corrected or mitigated. The HHS/CMS initially required the Exchanges to conduct an independent assessment of the security controls in the newly implemented Exchange information systems prior to issuing the initial authority to connect to the Hub. Subsequently, the HHS/CMS altered its guidance to allow the Exchanges to complete independent testing and plan to submit the SAR by March 31, 2014, or within six months of granting authority to connect to the Hub. However, Publication 1075 does not require such an initial assessment prior to approval, but does require agencies to assess the security controls in the information system and its environment at a minimum on an annual basis.

The Office of Safeguards' current security procedures do not require agencies to submit an Independent SAR for the IRS's review prior to the release of FTI. To approve an agency as ready to receive and properly safeguard FTI, the IRS initially relies on a description of the controls in the SPR. In conjunction with the documentary review, the IRS works with the agencies to ensure that the SPR descriptions are comprehensive, and in the case of the Exchanges, also made visits to facilitate completing the SPR.

Testing for the SARs was generally completed within two months prior to Exchange implementation. Development of ACA systems continued to be ongoing during the time between testing and deployment. Consequently, the SARs would not necessarily have had current information as of the October 1 start date because the Exchanges would be working on correcting weaknesses that had been identified. However, had the Office of Safeguards obtained and reviewed the Exchanges' SARs, it would have had better information regarding the status of Publication 1075 controls on which to base its approval decisions and to prioritize on-site reviews to those Exchanges deemed most vulnerable to security breaches.

TIGTA reviewed the Exchange SARs and Plans of Action and Milestones (POA&M)[12] which the HHS/CMS provided to us. Figure 2 shows that our review of the POA&Ms for 11 Exchanges indicated at least one or more open weaknesses existed in the 17 key security controls as of October 1, 2013.

[11] NIST Special Publication 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, Apr. 2013.

[12] The POA&M is used to track security control weaknesses identified by the agency during the internal inspections process and any other internal or external security assessment. The POA&M must include the corrective actions identified during the internal inspections and will identify the actions the agency plans to take to resolve these weaknesses.

Figure 2: The Exchanges With Open Weaknesses in Key Controls As of October 1, 2013
(out of 11 Exchanges with POA&Ms suitable for evaluation)[13]

	Key Control NIST Designation	Control Name	The Exchanges With Open Weaknesses As of October 1, 2013
1	AC-3	Labeling	3
2	AC-6	Least Privilege	5
3	AC-20	Use of External Information System	4
4	AU-2	Auditable Events	6
5	IA-2	Identification and Authentication	8
6	IA-5	Identifier Management	7
7	IR-6	Incident Reporting	4
8	MP-3	Media Marking	5
9	MP-6	Media Sanitization	4
10	PE-3	Physical Access Control	3
11	SA-9	External Information System Services	3
12	SC-4	Information in Shared Resources	3
13	SC-7	Boundary Protection	5
14	SC-8	Transmission Integrity	3
15	SC-9	Transmission Confidentiality	5
16	SI-2	Flaw Remediation	6
17	SI-3	Malicious Code Protection	3

Source: TIGTA analysis of Exchange POA&Ms.

As shown in Figure 2, results of our review of the 11 Exchanges showed that as of October 1, 2013, multiple Exchanges had open weaknesses related to each of the 17 controls. These weaknesses were present even though the Office of Safeguards had reviewed the SPRs and related documents, and worked with the Exchanges to ensure that these particular controls were in place prior to October 1. IRS reviewers had based their approval decisions on the descriptions of the controls in the SPR, whether implemented or planned, rather than on the actual status of these controls, because they had neither the SARs nor IRS test results.

In addition, although not an IRS requirement, three Exchanges did not provide the SARs to the HHS/CMS prior to October 1, 2013, in accordance with the initial HHS/CMS requirement. Consequently, this HHS/CMS control was not fully in place for all of the Exchanges at the time the Office of Safeguards approved them to receive FTI. While the IRS was not responsible for

[13] We did not include five Exchanges in this analysis because two had no SARs, two had POA&Ms with incomplete data, and one had a draft POA&M. See Appendix IV for a more complete description of the controls as they apply to safeguarding FTI.

reviewing agency compliance with this requirement imposed by the HHS/CMS, it was not always evident in the SPRs whether or not the SARs were completed.

According to the Office of Safeguards, the SPR provided sufficient information to evaluate an agency's ability to protect FTI and for basing its approval decision to release FTI. The Office of Safeguards stated that it relies on agencies, as trusted governmental data exchange partners, to implement the security controls as described in the SPR prior to receipt of FTI. Agencies are expected to follow sound information security business practices, including testing as part of system development procedures, but are not required to provide evidence of compliance prior to SPR approval. The Office of Safeguards stated that the recipient agency assumes all responsibility for operation and maintenance of information systems, as well as legal liability for FTI received under Internal Revenue Code Section 6103. The IRS stated that agencies may establish additional processes to enhance data protection subsequent to receiving FTI.

Without sufficient and complete information regarding the status of required security controls, the IRS might approve the release of FTI to an environment that puts FTI at risk of unauthorized disclosure or misuse.

Signed security authorizations were not obtained prior to approving agencies to receive FTI

Publication 1075 requires that an authorizing official authorizes (through signature approval) the information system for processing before commencing operations. The purpose of the authorization is to ensure that management has reviewed the risks associated with operating the system and has accepted the risk based on the implementation of the security controls.

Although the IRS had communicated to the Exchanges that systems must be authorized, neither of the two Exchanges TIGTA visited during the audit had signed security authorizations in place. While Publication 1075 requires agencies to ensure that the authorizing official authorizes the information system before commencing operations, it does not require agencies to submit the signed security authorization to the Office of Safeguards prior to release of FTI.

Because the Office of Safeguards relied on agencies as trusted governmental data exchange partners to implement the security controls as described in the SPR prior to receipt of FTI, it did not consider it necessary to obtain signed authorization documents from the recipient agencies prior to conducting an on-site review. During on-site reviews, the authorization documents were checked. However, without obtaining security authorizations prior to the release of FTI, the IRS has insufficient assurance that a responsible agency official has assessed and accepted the risks of any controls not yet in place prior to making the system operational.

Recommendations

The Director, Privacy, Governmental Liaison, and Disclosure, should:

Recommendation 1: Revise Publication 1075 to state that agencies that are deploying new systems must conduct an independent assessment of the security controls in their information systems prior to issuing the initial authority to operate, and must provide the SAR and signed security authorizations of their systems to the Office of Safeguards before release of FTI will be granted.

> ***Management's Response:*** The IRS agreed with this recommendation. The IRS will revise Publication 1075 to require agencies to provide the signed Authority to Operate and the results of independent security testing for new systems that will process FTI when submitting the Safeguard Security Report specifying controls for the new system. The IRS currently requests this documentation from new agencies seeking IRS approval to receive FTI for the first time.

Recommendation 2: Revise Office of Safeguards' policies to include a review of the SAR for any significant security deficiencies before approving the release of FTI and to use SAR results as a factor in assessing risk and prioritizing agencies for on-site reviews

> ***Management's Response:*** The IRS agreed with this recommendation. The IRS partially implemented this recommendation by reviewing agency security testing results during on-site safeguard reviews. The IRS will establish requirements that include the SAR as evidence to validate that the controls described in the Safeguard Security Report are implemented before the IRS approves an initial release of FTI. The IRS will also develop policies and procedures to evaluate the agency's independent security assessment and conduct a 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 vulnerabilities before approval of the data exchange. The results will be used when developing the safeguards review schedule.

Agencies Deploying New Systems May Not Be Tested for Up to Three Years, Possibly Allowing Security Deficiencies to Persist

Publication 1075 requires that agencies that receive FTI must agree to Office of Safeguards' on-site testing of agency security controls. Additionally, the Internal Revenue Manual (IRM), although out of date, anticipates that agencies receiving FTI for the first time may be reviewed within one year of initial receipt of the information. The IRM states that factors, such as a past history of problems, news items, or major changes in a processing system, may indicate a need for the IRS to conduct a review sooner than it otherwise would.

The Office of Safeguards conducted on-site testing at three of the 16 Exchanges within the first six months of operation. By June 2014, the IRS stated it had conducted on-site testing of three

additional Exchanges, for a total of six Exchanges tested. We reviewed the overall testing results for the initial three sites the IRS had visited for 157 controls required in Publication 1075. The testing results revealed weaknesses in controls that the Exchanges had described as implemented in their documentation. The results of the on-site testing also showed that weaknesses persisted in most of the 17 key controls, which the Office of Safeguards had worked with the Exchanges to ensure were implemented prior to the release of FTI. Additionally, the on-site testing at one Exchange revealed a serious weakness related to remote access requiring prompt action that was not evident in the SPR. Figure 3 shows the number of controls with weaknesses identified by the Office of Safeguards' on-site testing for which Exchange documentation described as implemented.

Figure 3: Selected Results of Office of Safeguards' On-site Testing

Weakness Condition	Exchange		
	1	2	3
Publication 1075 controls (of 157 reviewed by TIGTA) with weaknesses that the Exchanges had described as implemented in documentation.	23	34	35
Key Controls (17 of the 157) with weaknesses that the Exchanges had described as implemented in documentation.	8	10	9

Source: TIGTA analysis of Office of Safeguards' testing results.

Because the Exchanges were undergoing system testing in the months just prior to system deployment and working to correct deficiencies that were identified in the testing process, it was not practical for the Office of Safeguards to perform on-site reviews at the Exchanges prior to system deployment. However, the current Office of Safeguards' process to schedule on-site reviews could significantly delay identifying weaknesses because agencies that have deployed new systems are reviewed on the same three-year testing cycle as other agencies in their States that are already receiving FTI. Consequently, although the IRS receives annual reports and maintains other contacts with them, agencies that have deployed new systems may not receive an on-site review for up to three years after they first receive FTI.

As we have illustrated, the current documentation on which the IRS bases its approval decision for release of FTI does not provide sufficient evidence that required controls have been implemented. The SARs provide better information regarding the status of required controls, which, as we previously recommended, the IRS should review to ensure that no serious weaknesses exist before releasing FTI. Therefore, if an agency does not submit a SAR that indicates the new system materially meets safeguard requirements for protection of FTI, the IRS

should schedule an on-site review prior to releasing FTI. Because another TIGTA report[14] related to the IRS Office of Safeguards' oversight procedures has already made this recommendation, we will not include it as a recommendation in this report. However, if the IRS approved the release of FTI based on its review of the SAR, we believe initial on-site testing should occur as soon as possible after the date FTI is first sent in order to obtain the best assurance that information is adequately protected.

New untested systems carry a higher risk that controls are not properly implemented or working as intended. If not tested in a timely manner, security weaknesses may persist, unknown to the Office of Safeguards or the Exchanges, which may put FTI at risk.

Recommendation

Recommendation 3: The Director, Privacy, Governmental Liaison, and Disclosure, should prioritize according to risk and timely schedule on-site reviews of agencies that have deployed new systems and received FTI, particularly when those new systems relate to sensitive programs such as the ACA.

> ***Management's Response:*** The IRS agreed with this recommendation. The IRS will develop a comprehensive review scheduling process that documents risk-based deviations from the three-year review cycle for all agencies. The IRS will also establish procedures to incorporate new agencies receiving FTI into the review schedule when authorizing the initial release of FTI. The IRS will prioritize on-site reviews based on the evaluation of the agency's independent security assessment, IRS risk-based assessment, or a modified on-site review to increase assurance that FTI will be protected upon receipt.

Procedures to Suspend Transmission of Federal Tax Information Were Not Adequately Documented

Federal regulations provide for the IRS to take action to suspend or terminate FTI disclosures to a recipient agency that has failed to implement adequate safeguards to protect the confidentiality of FTI.[15] The IRS may also refuse to disclose FTI until it determines that Office of Safeguards' requirements have been or will be met.

The IRM provides procedures for the Office of Safeguards' on-site reviewers to follow when they identify serious deficiencies at recipient agencies. Deficiencies may be identified when the IRS reviews required reports or during on-site testing of security controls. The IRM states that when an on-site reviewer identifies a serious deficiency, the first action should be to attempt to obtain voluntary compliance through discussion and negotiation. When an impasse occurs, the

[14] TIGTA, Ref. No. 2014-20-059 , *The Office of Safeguards Should Improve Management Oversight and Internal Controls to Ensure the Effective Protection of Federal Tax Information* (Sept. 2014).
[15] Code of Federal Regulations, Title 26, §301.6103(p)(7)-1.

matter should be elevated to the appropriate IRS management level, and the reviewer should supply the relevant facts and a recommendation as to what action should be taken if the situation is not corrected.

The IRM further states that if IRS management is unable to break the impasse, it should initiate an administrative process to notify the recipient agency in writing of the IRS's intent to suspend or terminate FTI disclosures. Such notices allow the recipient agency 30 calendar days to appeal the IRS's preliminary determination. However, the IRM also states that a duly delegated IRS official may immediately suspend FTI disclosures where unauthorized accesses or disclosures would be made absent the suspension, and makes a reference to a delegation order.

However, the IRM does not clearly cite who has been delegated the authority to make the decision to immediately suspend FTI prior to initiating the administrative process. Consequently, the Office of Safeguards' reviewers may not know the full process to immediately suspend FTI when serious deficiencies exist. Also, the lack of clear procedures for immediate suspension of FTI could prolong the time needed to resolve potentially serious incidents.

The IRM also contains some out-of-date information, such as an incorrect business unit, that applied prior to reorganization. The IRM was last updated in August 2008 when the Office of Safeguards was in a different business unit. Consequently, the existing guidance is not reflective of the current organizational structure and should be updated.

As a practical matter, the IRS has not used its immediate authority or the administrative process to suspend or terminate FTI because it has been able to resolve matters with agencies through discussion and negotiation when serious deficiencies were discovered. However, clarifying the procedures to follow in the event that an impasse occurs and immediate suspension or termination is needed, including identifying the managers who have the authority to immediately suspend FTI, will help to facilitate IRS communication internally and with agencies about such issues.

Recommendation

Recommendation 4: The Director, Privacy, Governmental Liaison, and Disclosure, should update procedures in the IRM, including clarifying procedures for immediate suspension or termination of FTI, and identifying which managers have the authority to do so when deficiencies are serious enough to potentially allow unauthorized access or disclosure of FTI.

> ***Management's Response:*** The IRS agreed with this recommendation. The IRS is revising the IRM 11.3.36 to clarify the procedures to suspend or terminate disclosure when identifying an immediate risk to FTI. The Office of Safeguards' staff will be trained on the procedures and notified of the delegated IRS officials authorized to suspend disclosure of FTI.

Appendix I

Detailed Objective, Scope, and Methodology

Our overall objective was to determine whether the IRS Office of Safeguards has implemented sufficient policies and procedures to ensure that ACA Exchanges are adequately protecting FTI received from the IRS. To accomplish our objective, we:

I. Evaluated the IRS's processes and procedures related to the approval of ACA State and Federal Exchanges to receive FTI, and determined their adequacy in ensuring protection of FTI prior to its release.

A. Coordinated with TIGTA's other Security and Information Technology Services audit team on the overall Office of Safeguards' program[1] to ensure that we stayed informed about their findings and ensured consistency and continuity between the two audit reports.

B. Interviewed the ACA Office of Safeguards' staff to identify ACA-related processes and procedures.

C. Reviewed the Office of Safeguards' processes and procedures and other security control guidance as they relate to the State and Federal Exchanges and documented any control weaknesses identified related to the policies and procedures or guidance.

1. Publication 1075, *Tax Information Security Guidelines for Federal, State and Local Agencies*—incorporates NIST Special Publication 800-53 controls.
2. *Minimum Acceptable Risk Standards for Exchanges*.
3. The SPRs, System Security Plans, and System Security Plan Workbooks.
4. Authorization process prior to the release of FTI data.
5. SPR/System Security Plan validation visit prior to approval to receive FTI.

D. Determined whether Publication 1075 contains adequate security controls for protection of FTI when compared with NIST Special Publication 800-53, Rev. 4 *Security and Privacy Controls for Federal Information Systems and Organizations*.

1. Identified NIST Special Publication 800-53, Rev. 4, controls that, in TIGTA's opinion, should be added to Publication 1075 to ensure protection of FTI.
2. Determined whether the controls identified by the IRS as critical are sufficient or

[1] TIGTA, Ref. No. 2014-20-059 , *The Office of Safeguards Should Improve Management Oversight and Internal Controls to Ensure the Effective Protection of Federal Tax Information* (Sept. 2014).

should additional security controls be considered as critical and in place prior to release of FTI.

E. Determined whether IRS processes are sufficient to ensure that ACA Exchanges have reported that standards are being met and controls are in place.

1. Based on ACA Exchange approval documents, identified the security controls that were not in place when the IRS approved the ACA Exchange to receive FTI. We noted if any of these were the security controls that the IRS deemed critical.

2. Reviewed and evaluated IRS processes to monitor and ensure that failed security controls are corrected before FTI is released. Based on available documentation, we determined if failed controls were corrected before FTI was released.

F. Evaluated IRS requirements for information security agreements between the IRS and the State and Federal Exchanges.

1. Determined what formal agreements are required prior to release of FTI.

2. Assessed whether the IRS has executed these agreements with the appropriate parties.

3. Determined whether the agreements adequately allow for the IRS's enforcement of protection of FTI.

II. Determined whether State and Federal Exchanges performed required independent security assessments prior to receiving FTI.

A. Determined requirements for State and Federal Exchanges with respect to independent security assessments.

B. Determined what the IRS obtains from State and Federal Exchanges related to the independent security assessment – a copy of the results, a copy of the POA&M, *etc*.

C. Determined how the IRS uses the information it obtains from the independent security assessments.

D. Reviewed State and Federal Exchanges' independent security assessment testing documentation for adequacy with respect to Publication 1075 for the State Exchanges, NIST standards for the Federal Exchange, and TIGTA's judgment. We coordinated with the HHS Office of Inspector General to obtain this documentation and on other matters during our review as needed.

1. Analyzed results and identified controls not in place and/or inadequately reported by the independent security assessments.

2. Determined whether the independent security assessments identified failed controls that the IRS's approval processes did not identify for input to Step I. and,

where available, that the IRS's on-site review test processes did not identify for input to Step II.

E. Evaluated the State and Federal Exchanges' processes to correct security control weaknesses reported by the independent security assessments.

1. Evaluated State Exchange POA&Ms.

2. Based on available documentation, determined whether failed controls are corrected in a timely manner.

III. Evaluated whether the Office of Safeguards' reviews are adequate to detect failed security controls and whether its processes adequately ensured that failed controls are corrected.

A. Evaluated test plans and templates that the IRS Office of Safeguards uses during reviews.

B. Evaluated test documents from completed on-site reviews to assess the adequacy of the IRS's review process.

C. Accompanied the IRS on reviews at the California and Connecticut Exchanges that took place during the audit period to determine if the Exchanges have implemented the security controls required by Publication 1075. We obtained and reviewed test plans for each site in advance.

D. Determined whether the IRS's reviews identified failed security controls that the IRS's approval process or the State and Federal independent security assessments did not identify.

E. Evaluated IRS processes to ensure that State and Federal Exchanges correct security control weaknesses reported by the IRS's reviews.

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 and procedures to administer the Safeguards program, other Federal guidance related to computer security controls, and guidance related to the Exchanges. We evaluated these controls by interviewing management and by reviewing the relevant IRS and Federal guidance, including the IRM, Publication 1075, NIST Special Publication 800-53, Revisions 3 and 4, and *Minimum Acceptable Risk Standards for Exchange*s.

Appendix II

Major Contributors to This Report

Alan Duncan, Assistant Inspector General for Audit (Security and Information Technology Services)
Kent Sagara, Director
Jody Kitazono, Audit Manager
Mary Jankowski, Lead Auditor
Louis Lee, Senior Auditor
Midori Ohno, Senior Auditor
Esther Wilson, Senior Auditor
Larry Reimer, Information Technology Specialist

Appendix III

Report Distribution List

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

Appendix IV

Description of Key Controls As They Apply to Safeguarding Federal Tax Information

	Key Control NIST Designation	Control Name	Description of Control As It Applies to Safeguarding FTI
1	AC-3	Labeling	Agencies must identify FTI data they have and consistently apply labels to that data in such a way that the data are easily identified, even when commingled. When data are commingled, the data must be identified at the most minor level. For example, if data are commingled at the table level, *i.e.*, a database which contains FTI and non-FTI data tables, the tables must be labeled in such a way so that it is readily apparent that those tables contain FTI. Additionally, if data are commingled within a table that includes FTI and non-FTI data, FTI data must be explicitly labeled and identified as such.
2	AC-6	Least Privilege	Access to FTI must be strictly on a need-to-know basis. FTI must never be indiscriminately disseminated, even within the recipient agency, body, or commission. No person should be given more FTI than is needed for performance of his or her duties.
3	AC-20	Use of External Information System	Only agency-owned computers, media, and software will be used to receive, process, access, and store FTI. The agency must retain ownership and control for the security configuration of all hardware, software, and end-point equipment connecting to public communication networks including encryption keys.
4	AU-2	Auditable Events	Auditing must be enabled to the extent necessary to capture access, modification, deletion, and movement of FTI by each unique user.
5	IA-2	Identification and Authentication	Two-factor authentication is required whenever FTI is being accessed from an alternative work location or if accessing FTI via an agency's web portal by an employee or contractor.

	Key Control NIST Designation	Control Name	Description of Control As It Applies to Safeguarding FTI
6	IA-5	Identifier Management	Passwords meet minimum Publication 1075, *Tax Information Security Guidelines for Federal, State and Local Agencies*, requirements. Enforce minimum password complexity consisting of at least eight (8) alphanumeric, *i.e.*, uppercase and lowercase letters, numbers, and/or special characters. Change/refresh authenticators every 90 days, at a minimum, for a standard user account, and every 60 days, at a minimum, for privileged users.
7	IR-6	Incident Reporting	Any data incident potentially involving FTI must immediately be reported to TIGTA and the IRS Office of Safeguards immediately, but no later than 24 hours after identification of a possible issue involving FTI.
8	MP-3	Media Marking	The agency must label information system media containing FTI to indicate the distribution limitations and handling caveats.
9	MP-6	Media Sanitization	If the media will be reused by the agency for the same purpose of storing FTI and will not be leaving the organization's control, then clearing is a sufficient method of sanitization. If the media will be reused and repurposed for a non-FTI function and/or will be leaving the organization's control, *i.e.*, media being exchanged for warranty, cost rebate, or other purposes, and where the specific media will not be returned to the agency, then purging should be selected as the sanitization method. If the media will not be reused at all, then destroying is the method for media sanitization.
10	PE-3	Physical Access Control	Minimum protection standards require two physical barriers between FTI and an individual not authorized to access FTI. This may be achieved through secured perimeter/locked container, locked perimeter/secured interior, or locked perimeter/security container. FTI must be containerized in areas where other than authorized employees or authorized contractors may have access after-hours.
11	SA-9	External Information System Services	FTI may not be accessed by agency employees, agents, representatives, or contractors located "off-shore" (outside of the United States or its territories). FTI may not be received, stored, processed, or disposed via information technology systems located off-shore.
12	SC-4	Information in Shared Resources	FTI that may reside in shared system resources, *e.g.*, memory, during application sessions is cleared before the memory is released back to the system when the session is terminated.

	Key Control NIST Designation	Control Name	Description of Control As It Applies to Safeguarding FTI
13	SC-7	Boundary Protection	FTI is not directly accessible from the Internet. Virtual Private Network (or similar technology providing similar protection, *e.g.*, end-to-end encryption) should be used when remotely accessing FTI.
14	SC-8	Transmission Integrity	The information system protects the integrity of transmitted information. All FTI in transit must be encrypted when moving across a Wide Area Network and within the agency's Local Area Network.
15	SC-9	Transmission Confidentiality	The information system protects the confidentiality of transmitted information.
16	SI-2	Flaw Remediation	Agencies must identify, report, and correct information system flaws.
17	SI-3	Malicious Code Protection	The organization employs malicious code protection mechanisms at information system entry and exit points and at workstations, servers, or mobile computing devices on the network to detect and eradicate malicious code.

Source: IRS internal document describing the key controls and NIST Special Publication 800-53, Rev. 3.

Appendix V

Management's Response to the Draft Report

PRIVACY, GOVERNMENTAL LIAISON AND DISCLOSURE

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

August 29, 2014

MEMORANDUM FOR DEPUTY INSPECTOR GENERAL FOR AUDIT

FROM: Mary Howard Mary J. Howard
Director, Privacy, Governmental Liaison and Disclosure

SUBJECT: Draft Audit Report – Affordable Care Act: Expanded Guidance Provided Assistance to the Exchanges, but Greater Assurance of the Protection of Federal Tax Information Is Needed (Audit #201420302)

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 (FTI) shared with our agency partners under Internal Revenue Code Section 6103 is properly protected at all times.

We appreciate TIGTA's acknowledgement of the extra measures taken by PGLD to ensure the protection of FTI provided to the Health Insurance Exchanges (Exchanges) during implementation of the data exchange provisions of the Affordable Care Act (ACA). This effort took extensive coordination with security staff at the Centers for Medicare and Medicaid Services (CMS), our federal data exchange partner leading ACA implementation. We ensured CMS incorporated IRS data protection standards in all privacy and security guidance issued to states. In addition, we provided technical assistance and educational outreach covering the statutory restrictions on access to FTI and the use of taxpayer information in eligibility determinations under the ACA directly to state Exchanges. As a result, we note that TIGTA did not find any specific or elevated risk to FTI maintained by the Exchanges during the audit.

Although TIGTA's recommendations in this report focus on initial approval to release FTI to the Exchanges, as the recommendations are implemented by the Office of Safeguards, the IRS will have increased assurance that all new data exchange partners have appropriate safeguards in place to protect sensitive taxpayer from loss, breach or misuse, upon initial receipt of FTI.

Attached are our comments to your recommendations. If you have any questions, please contact me at (202) 317-3950, or a member of your staff may contact Gregory Ricketts, Associate Director Office of Safeguards at (901) 546-3078.

Attachment

Attachment

Recommendation 1: Revise Publication 1075, *Tax Information Security Guidelines for Federal, State and Local Agencies*, to state that agencies that are deploying new systems must conduct an independent assessment of the security controls in their information systems prior to issuing the initial authority to operate, and must provide the Security Assessment Report (SAR) and signed security authorizations of their systems to the Office of Safeguards before release of Federal Tax Information (FTI) will be granted.

Corrective Action: The IRS will revise Publication 1075, to require agencies to provide the signed Authority to Operate and the results of independent security testing for new systems that will process FTI when submitting the Safeguard Security Report specifying controls for the new system. The IRS currently requests this documentation from new agencies seeking IRS approval to receive FTI for the first time.

Implementation Date: January 31, 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 2: Revise Office of Safeguards' policies to include a review of the SAR for any significant security deficiencies before approving the release of FTI and to use SAR results as a factor in assessing risk and prioritizing agencies for onsite reviews.

Corrective Action: The IRS partially implemented this recommendation by reviewing agency security testing results during on-site safeguard reviews. We will establish requirements that include the SAR as evidence to validate that the controls described in the Safeguard Security Report are implemented before the IRS approves an initial release of FTI. We will also develop policies and procedures to evaluate the agency's independent security assessment and conduct 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 vulnerabilities before approval of the data exchange. The results will be used when developing the safeguards review schedule.

Implementation Date: March 1, 2015.

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

Attachment

2

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

Recommendation 3: The Director, Privacy, Governmental Liaison, and Disclosure, should prioritize according to risk and timely schedule onsite reviews of agencies that have deployed new systems and received FTI, particularly when those new systems relate to sensitive programs such as the Affordable Care Act.

Corrective Action: The IRS will develop a comprehensive review scheduling process that documents risk based deviations from the three year review cycle for all agencies. We will also establish procedures to incorporate new agencies receiving FTI into the review schedule when authorizing the initial release of FTI. The IRS will prioritize on-site reviews based on the evaluation of the agency's independent security assessment, IRS risk-based assessment or a modified onsite review to increase assurance that FTI will be protected upon receipt.

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 4: The Director, Privacy, Governmental Liaison, and Disclosure, should update procedures in the IRM, including clarifying procedures for immediate suspension or termination of FTI, and identifying which managers have the authority to do so when deficiencies are serious enough to potentially allow unauthorized access or disclosure of FTI.

Corrective Action: We are revising IRM 11.3.36 to clarify the procedures to suspend or terminate disclosure when identifying an immediate risk to FTI. Safeguards staff will be trained on the procedures and notified of the delegated IRS officials authorized to suspend disclosure of FTI.

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.