Affordable Care Act: Improvements Are Needed to Strengthen Security and Testing Controls for the Affordable Care Act Information Returns Project

September 29, 2014

Reference Number: 2014-23-072

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

Redaction Legend:
2 = Risk Circumvention of Agency Regulation or Statute

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

AFFORDABLE CARE ACT: IMPROVEMENTS ARE NEEDED TO STRENGTHEN SECURITY AND TESTING CONTROLS FOR THE AFFORDABLE CARE ACT INFORMATION RETURNS PROJECT

Highlights

Final Report issued on September 29, 2014

Highlights of Reference Number: 2014-23-072 to the Internal Revenue Service Chief Technology Officer.

IMPACT ON TAXPAYERS

In March 2010, the President signed into law the Patient Protection and Affordable Care Act (ACA) to provide more Americans with access to affordable health care. The ACA Information Returns (AIR) Release 1 Project is an information technology project managed under the IRS's ACA Program. The ACA legislation requires the IRS to calculate and collect annual fees based on form reports provided by health insurance providers and pharmaceutical manufacturers and importers. The form reports include information that the IRS requires to calculate the fees that are due annually by September 30 of each year.

WHY TIGTA DID THE AUDIT

The overall objective of this review was to determine if the IRS is adequately mitigating systems development risks for the AIR Release 1 Project. TIGTA evaluated the IRS's key management controls and processes for risk management, requirements and change management, testing, security, and fraud detection for the AIR Release 1 Project, which is being developed by following the IRS's Enterprise Life Cycle Commercial Off-the-Shelf Path.

WHAT TIGTA FOUND

The IRS conducted security activities to identify vulnerability weaknesses. The IRS also conducted testing activities to validate whether the AIR Release 1 system would function as designed before it was placed into production. However, improvements are needed to ensure the long-term success of the AIR system by adherence to systems development controls for security and testing activities in accordance with applicable guidance. *****2**********:

- **********2**********2**********2**********2**********2**********2**********2**********2**********2**********.
- **********2**********2**********2**********2**********2**********2**********2**********2**********2********.

These security control weaknesses could impact the AIR system's ability to reliably process the electronic form reports and to accurately determine the applicable fees.

WHAT TIGTA RECOMMENDED

TIGTA recommended that the Chief Technology Officer ensure that: (1) procedures are developed to provide direction on how to mitigate vulnerability *****2********** ********2*********; (2) vulnerability weaknesses identified are promptly corrected and resolved; (3) the ACA Plan of Action and Milestones adequately addresses the vulnerability weaknesses within the required time frames; (4) **********2********** *******2******; (5) *****2********** **********2**********; (6)**********2********** **********2**********; and (7) the Information Technology Implementation and Testing organization effectively manages the testing processes executed by the external contractors.

In management's response to the report, the IRS agreed with the majority of TIGTA's recommendations and plans to implement corrective actions. However, the IRS partially agreed with one recommendation and disagreed with two recommendations. TIGTA notes its concern about the IRS response to these recommendations in the report.

TREASURY INSPECTOR GENERAL
FOR TAX ADMINISTRATION

DEPARTMENT OF THE TREASURY
WASHINGTON, D.C. 20220

September 29, 2014

MEMORANDUM FOR CHIEF TECHNOLOGY OFFICER

FROM: Michael E. McKenney
Deputy Inspector General for Audit

SUBJECT: Final Audit Report – Affordable Care Act: Improvements Are Needed to Strengthen Security and Testing Controls for the Affordable Care Act Information Returns Project (Audit #201420315)

This report presents the results of our review of how the Affordable Care Act (ACA) Information Returns (AIR) Project managed controls over systems development. The overall objective of this review was to determine if the Internal Revenue Service (IRS) is adequately mitigating systems development risks under the Affordable Care Act Program to achieve business and information technology goals for the AIR Release 1 Project as a core system for the program. This audit is included in our Fiscal Year 2014 Annual Audit Plan and addresses the major management challenges of *Implementing the Affordable Care Act and Other Tax Law Changes* and *Security for Taxpayer Data and Employees*.

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

Copies of this report are also being sent to the IRS managers affected by the report recommendations. Please contact me or Danny Verneuille, Acting Assistant Inspector General for Audit (Security and Information Technology Services), if you have questions.

Table of Contents

Background ..... Page 1

Results of Review ..... Page 6

Identified Security Weaknesses Should Be Fully Mitigated ..... Page 6

Recommendations 1 and 2: ..... Page 10

Recommendations 3 and 4: ..... Page 11

Recommendation 5: ..... Page 14

Recommendation 6: ..... Page 15

Testing Performed for Affordable Care Act Information Returns Release 1 ..... Page 15

Test Management Controls Need Improvement to Ensure Long-Term Success of the Affordable Care Act Information Returns Project ..... Page 17

Recommendation 7: ..... Page 19

Appendices

Appendix I – Detailed Objective, Scope, and Methodology ..... Page 20

Appendix II – Major Contributors to This Report ..... Page 22

Appendix III – Report Distribution List ..... Page 23

Appendix IV –**********2********** **********2********** **********2********** ..... Page 24

Appendix V – Glossary of Terms ..... Page 31

Appendix VI – Management's Response to the Draft Report ..... Page 35

Abbreviations

ACA	Affordable Care Act
AIR	Affordable Care Act Information Returns
BPD	Branded Prescription Drug
COTS	Commercial Off-the-Shelf
EOps	Enterprise Operations
IPF	Insurance Provider Fee
IRM	Internal Revenue Manual
IRS	Internal Revenue Service
IT	Information Technology
NIST	National Institute of Standards and Technology
PMO	Program Management Office
POA&M	Plan of Action and Milestone
SQL	Structured Query Language
TIGTA	Treasury Inspector General for Tax Administration
XML	Extensible Markup Language

Background

In March 2010, Congress passed two pieces of legislation that the President later signed into law—the Patient Protection and Affordable Care Act and the Health Care and Education Reconciliation Act of 2010 (collectively referred to as the Affordable Care Act (ACA).[1] The ACA legislation seeks to provide more Americans with access to affordable health care by creating a new Health Insurance Marketplace, enforcing patient/consumer protections, and providing Government subsidies for people who cannot afford insurance. The Marketplace simplifies an applicant's 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 Health Insurance Marketplace is commonly referred to as the "Insurance Exchange." These State-based Exchanges are intended to provide a place for Americans to shop for health insurance in a competitive and transparent environment.

The ACA legislation requires the IRS to collect health care information reports from health insurance providers and pharmaceutical manufacturers.

In order to enroll in health insurance coverage offered through an Exchange, taxpayers must complete an application and meet certain eligibility requirements defined by the ACA. For example, they must be U.S. citizens or legal immigrants. Exchanges offer insurance plans by private companies, and taxpayers can access qualified health plan information online, via a call center, or in person. The Internal Revenue Service's (IRS) role with respect to the ACA is to implement and administer the ACA provisions that have an impact on tax administration. The U.S. Department of Health and Human Services is tasked with developing policy provisions for the ACA. These provisions require the IRS to build new computer applications, modify existing systems, revise or create business processes and fraud detection systems, and deploy and test new interagency communication portals to support ACA operations.[2]

[1] The Patient Protection and Affordable Care Act is 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.
Also, see Appendix V for a glossary of terms.

[2] This audit builds on prior work completed in the following Treasury Inspector General for Tax Administration (TIGTA) audit reports: (1) Ref. No. 2013-23-034, *Affordable Care Act – The Income and Family Size Project: Improvements Could Strengthen the Internal Revenue Service's New Systems Development Process* (Mar. 2013); (2) Ref. No. 2013-20-063, *Improvements Are Needed to Ensure Successful Development and System Integration for the Return Review Program* (Jul. 2013); and (3) Ref. No. 2013-23-119, *Affordable Care Act: Improvements Are Needed to Strengthen Systems Development Controls for the Premium Tax Credit Project* (Sept. 2013).

Recognizing the integral role that information technology (IT) plays in executing the IRS's portion of the ACA legislation, the IRS created the ACA IT Program Management Office (ACA PMO) in January 2011 in order to ensure a dedicated focus on fulfilling ACA requirements. The ACA PMO segmented implementation of ACA functionality into various releases. Current and upcoming ACA releases include:

- **ACA Release 4.0 (ACA 4.0)**

  ACA 4.0 includes the Coverage Data Repository Release 2 Project and the Information Sharing and Reporting Release 3 Project. ACA 4.0 is scheduled to be placed into production in September 2014.

- **ACA Release 4.1 (ACA 4.1)**

  ACA 4.1 includes the ACA Information Returns (AIR) Release 1 Project, the Insurance Provider Fee (IPF) Release 1 Project, and the Branded Prescription Drug (BPD) Release 3 Project. The IRS is implementing ACA 4.1 in phases by project. AIR Release 1 and IPF Release 1 were placed into production on March 11, 2014. The BPD system has been processing paper forms for three years as part of previous ACA releases. As part of ACA 4.1, the BPD system's required functionality is to process electronic forms and is scheduled to be placed into production on October 1, 2014.

- **ACA Release 5.0 (ACA 5.0)**

  ACA 5.0, which includes AIR Release 2, will receive and store issuer (ACA Provision Section (§) 6055), employer (ACA Provision § 6056), and State Exchange (1095x) submitted data, prioritize and separate receipt and acceptance queues, check the structural integrity of submissions, perform internal checks of input data and validation of data types, record data errors in a relational database, record status, and transform and transmit data after validation. The target implementation date for ACA 5.0 is January 2015.

The ACA PMO manages various ACA project offices that focus on specific areas of new systems development. The IRS has identified the following three ACA projects as core ACA systems.

- Coverage Data Repository.
- Information Sharing and Reporting.
- AIR.

The ACA legislation mandates that the IRS collect health care information reports from health insurance providers and pharmaceutical manufacturers. As part of ACA 4.1, the AIR Release 1 Project will support the processing of Non-Exchange ACA information returns electronically. ACA 4.1 is required to address the following functionality for meeting ACA provisions:

- **§ 9010 Imposition of an Annual Fee on Insurance Providers (Annual Electronic Report of Health Insurance Provider Information via Form 8963, *Report of Health Insurance Provider Information*)**

  The IPF provision imposes an annual fee on any health insurance provider that provides health insurance during the calendar year with net premiums written that exceed $25 million. Fully insured health plans and insurance companies will report this annual information to the IRS on Forms 8963. The AIR system will electronically process these annual reports and send the data to the IRS's IPF database.

- **§ 9008 Imposition of an Annual Fee on Branded Prescription Drugs (Annual Electronic Report of Branded Prescription Drug Information via Form 8947, *Report of Branded Prescription Drug Information*)**

  The BPD provision imposes an annual fee on pharmaceutical companies (manufacturer or importer of branded prescription drugs), who are required to provide sales data on branded prescription drugs, orphan drugs, and rebates to the IRS on Forms 8947. The AIR system will electronically process these annual reports and send the data to the IRS's BPD database.

The ACA legislation also requires the IRS to calculate and collect these fees annually based on the form reports provided by the health insurance provider and pharmaceutical manufacturer industries. The fees are due annually by September 30 of each year. The AIR system began playing a key role in this process as of March 2014. Specifically, the AIR system receives and processes the IPF and BPD electronic form reports as follows:[3]

- Health insurance providers file annual forms (Form 8963) with the IRS reporting their net premiums written for the preceding calendar year, and pharmaceutical manufacturers or importers of branded prescription drugs file annual forms (Form 8947) with the IRS reporting their sales data for drugs to certain government programs for the preceding calendar year.

  The AIR system's functionality includes validating, accepting/rejecting, and processing the electronic forms that will be submitted by the health insurance providers and pharmaceutical manufacturers and sending the data to the IRS's respective IPF and BPD systems, which calculate and collect the fees.

- The IRS will then compare the information provided on the forms to third-party data reports[4] to verify whether the information on the forms is correct.

[3] The AIR system began receiving and processing the IPF electronic form reports in March 2014 and is scheduled to start receiving and processing the BPD electronic form reports beginning on October 1, 2014.
[4] Third-party data reports are provided by the National Association of Insurance Commissioners, the Centers for Medicare and Medicaid Services, the Department of Defense, and the Department of Veterans Affairs.

- Once verified, the IRS will then calculate and inform the health insurance providers and pharmaceutical manufacturers of what their respective annual fees are.

The IRS is managing the AIR Release 1 Project under its development process within its Enterprise Life Cycle (ELC) Commercial Off-the-Shelf (COTS) Path. According to the ELC, this approach is intended to capitalize on the benefits of a preexisting commercially produced solution. The AIR Release 1 Project selected the COTS application**********2****** *****2*********. Specifically, the ******2******application provides a framework for the electronic processing of Forms 8963 and 8947 submitted to the IRS by the health insurance providers and pharmaceutical manufacturers respectively. The Enterprise Architecture organization explained that the ******2******application is on the IRS approved Enterprise Standards Profile.[5]

Figure 1 depicts **********2********** **********2**********.

Figure 1: **********2******** **********2********** **********2**********

****
****
****
****
****
****
****
****
**********2**********
****
****
****
****
****
****
****
****
****
****
****
**********2**********.

[5] The IRS's Enterprise Standards Profile lists standards and approved products that will be incorporated into the target architecture.

The AIR Release 1 Project will support the following ACA business processes and functionality:

- Receive electronic BPD and IPF electronic filing reports from authorized submitters.
- Process those submissions.
- Validate data listed on the electronic IPF reports (Forms 8963).
- Validate data listed on the electronic BPD reports (Forms 8947).
- Deliver submissions to the IPF or BPD systems.
- Send status and acknowledgement to the submitter.

Our review focused on risk mitigation activities for the AIR Release 1 Project under ACA 4.1.

This review was performed at the ACA PMO in Lanham, Maryland, during the period November 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

Identified Security Weaknesses Should Be Fully Mitigated

The AIR system will validate, accept/reject, and process the BPD data and feed that data into the IRS's BPD database. The BPD system is currently in production and will begin accepting electronic forms through the AIR system on October 1, 2014.

The Cybersecurity organization is responsible for conducting security testing activities designed to ensure that systems security safeguards are in place and functioning as intended for IRS systems. In 2013, **********2********** **********2**********. It also conducted Developer Security Testing (SA-11) activities, including vulnerability detection scans, using the IBM Guardium vulnerability assessment tool in coordination with other IRS supporting organizations, including Enterprise Operations (EOps). These security testing activities were completed between August and November of 2013 to help ensure that the AIR, BPD, and IPF systems meet the established security requirements in accordance with IRS Internal Revenue Manual (IRM) guidelines and National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, *Recommended Security Controls for Federal Information Systems and Organizations*.[6]

**********2********** **********2********** **********2********** **********2**********.

- **********2**********.
  - **********2**********.
  - **********2**********.
- **********2**********.

[6] National Institute of Standards and Technology Special Publication 800-53 Rev. 4, *Security and Privacy Controls for Federal Information Systems and Organizations* (Apr. 2013).

**********2**********2**********

IRM 10.8.1, *Information Technology Security, Policy and Guidance*, states that vulnerabilities should be identified, analyzed, and mitigated. In May 2010, the Cybersecurity organization purchased the IBM Guardium vulnerability assessment tool to perform vulnerability detection scans on IRS databases. **********2**********
**********2**********
**********2**********
**********2**********
**********2**********. Figure 2 summarizes ******2****
**********2**********.

Figure 2: **********2********
**********2**********

2	Number of ***2*** Failures	Number of ***2*** Errors	Number of ***2*** Failures	Number of ***2*** Errors
2	***2***	***2***	***2***	***2***
2	***2***	***2***	***2***	***2***
2	***2***	***2***	***2***	***2***
2	***2***	***2***	***2***	***2***

Source: **********2**********.

**********2**********:

- ********2*********_**********2**********
  **********2**********
  **********2**********
  **********2**********
  **********2**********
  **********2**********.
- **********2**********_**********2**********
  **********2**********
  **********2**********
  **********2**********
  **********2**********.

- **********2**********–**********2**********
  **********2**********
  **********2**********
  **********2**********.
- **********2*********–**********2**********
  **********2**********
  **********2**********
  **********2**********
  **********2**********
  **********2**********.

**********2**********
**********2**********.

Vulnerability Weaknesses and Mitigating Controls

According to IRM 10.8.1, the IRS is responsible for reviewing and mitigating the vulnerability weaknesses identified in the vulnerability detection scan and creating a Plan of Action and Milestone (POA&M).[7] Also, the IRS's Standard Operating Procedures under the Federal Information Security Management Act[8] require that these plans are initiated within 60 days to correct vulnerability weaknesses or to create a risk-based decision.[9] This policy applies to IRS systems categorized as a moderate risk, including the AIR, BPD, and IPF systems.

**********2**********
**********2**********
**********2**********
**********2**********
**********2**********
**********2**********
**********2**********

[7] Also, according to the *Federal Information Security Management Act Plans of Actions and Milestones Standard Operating Procedures* dated April 4, 2014, and the NIST Federal Information Processing Standards Publication 199, *Standards for Security Categorization of Federal Information and Information Systems* (April 2014), vulnerabilities are assigned a priority level based on the severity of impact and are to be corrected within a specific time period and added to the POA&M so that the vulnerabilities can be managed.

[8] Federal Information Security Management Act of 2002 (FISMA), Pub. L. No. 107-347, Title III, 116 Stat. 2899, 2946-2961 (2002) (codified as amended in 44 U.S.C. §§ 3541-3549). Note: FISMA is located in Title III the E-Government Act of 2002, Pub. L. No. 107-374, 116 Stat. 2899.

[9] IRS policy (NIST SP 800-53 and IRM 10.8.1) allows designated approving authorities to tailor security control baselines for their systems using a cost-effective, risk-based approach. This type of risk-based decisionmaking gives designated approving authorities a process by which they can make exceptions or deviations to IRS IT security policies based on credible justification and a thorough assessment of the risks incurred as a result of the deviation.

**********2**********
**********2**********
**********[10]**********2**********
**********2**********.

**********2**********
**********2**********
**********2**********
Cybersecurity organization initiated a POA&M that was later provided to us on April 18, 2014. Our review of this POA&M considered the 25 ***2*** and ***2*** failures and errors identified by the Guardium tool. During audit fieldwork, we informed the IRS of the following concerns:

- The POA&M was developed 56 days after the 60-day requirement for a moderate system according to Federal Information Processing Standards 199.
- The POA&M only provided details on how to address 23 of the 25 critical and major failures and errors identified by the Guardium tool. The two weaknesses not addressed by the POA&M are:
  - **********2**********.
  - **********2**********.
- Although the POA&M provided details on how to address 23 of the 25 vulnerability weaknesses, several of the mitigation target dates are nine to 12 months after the BPD system is scheduled to start processing electronic forms on October 1, 2014. For example, there are 14 ***2*** and ***2*** failure weaknesses that have completion target dates in the fall of 2015. Our review found that some of these ***2*** and ***2*** failure weaknesses can be mitigated now. ********2********** **********2********** [11]**********.

Security Patch Management Controls

IRM 10.8.50, *Information Technology (IT) Security, Servicewide Security Patch Management*, defines the security patch management process to ensure the timely implementation of security patches on all IRS computers, networks, COTS software, and IRS-developed applications and software. Also, this IRM requires that agencies test and install security patches on a timeline in accordance with the criticality of the patches. Based on the priority ranking, security patches are required to be installed within 30 to 150 days after the patches are released.

[10] TIGTA Ref. No. 2012-20-122, *Customer Account Data Engine 2 (CADE 2): System Requirements and Testing Processes Need Improvements* (Sept. 2012).
[11] This security test checks that **********2**********
**********2**********.

We also analyzed the 25 ****2**** and ***2*** failures and errors identified by the Guardium tool and concluded that the IRS had not installed two security patches on the BPD database as required:

- **********2**********2**********.
- **********2**********2**********2**********.

**********2**********2**********.

**********2**********2**********2**********.

*****2*******. This could affect the AIR system's ability to securely process the electronic reports from the insurance providers and the pharmaceutical manufacturers and calculate the fees that the insurance providers and pharmaceutical manufacturers owe, which are ACA legislative requirements. **********2**********2**********2**********.

Recommendations

The Chief Technology Officer should ensure that:

Recommendation 1: Processes and procedures are developed to provide direction on how to review and mitigate weaknesses *********2******vulnerability detection scans run on all databases.

> ***Management's Response:*** The IRS agreed with this recommendation. The IRS stated that the Cybersecurity organization has integrated ********2**** *******2*******, including creation of POA&M. The EOps and Cybersecurity organizations, working within the constraints of budget and resources, will revise the processes and procedures developed for the Security Assessment and Authorization process to provide direction on how to review and mitigate vulnerabilities **********2**********during continuous monitoring.

Recommendation 2: All vulnerability weaknesses **********2**********vulnerability detection scan are promptly corrected and resolved **********2**********.

> ***Management's Response:*** The IRS partially agreed with this recommendation. The IRS stated that the BPD database, **********2**********, is being

migrated to an upgraded version of the database software. In addition, to mitigate vulnerability weaknesses and manage risk, the IRS will create a risk-based decision regarding the processing of electronic form reports that will align the AIR system and BPD database to be consistent with its established risk management policies. Once the migration is complete, the IRS will, within the constraints of budget and resources, request another scan to verify compliance.

Office of Audit Comment: In its response to the draft report, the IRS takes partial exception with our conclusion that the IRS should ensure that all vulnerability weaknesses *********2**********vulnerability detection scan are promptly corrected and resolved **********2********** **********2********** **********2**********. However, the document did not state that the database will be migrated to an upgraded version of the database software. In its response, the IRS did not provide a completion date for when: (1) the BPD database will be migrated to an upgraded version of the database software, (2) the IRS will request another vulnerability detection scan once the migration is complete, and (3) the IRS will create a risk-based decision regarding the processing of electronic form reports to align the AIR system and BPD database to be consistent with its established risk management policies. TIGTA maintains that the IRS needs to ensure that vulnerability weaknesses, including all ***2*** and ***2*** failures, *****2******* ********2**********are promptly corrected and resolved **2*** **********2********** **********2********** **********2**********.

Recommendation 3: ACA POA&Ms, *******2**********, are developed for each vulnerability weakness identified and the mitigation actions adequately address the vulnerability weaknesses within the required time frames in accordance with IRS guidelines.

Management's Response: The IRS agreed with this recommendation. The IRS stated that the Cybersecurity organization has a process which ensures that vulnerabilities found during annual security assessments have actionable POA&Ms created timely. As a part of the continuous monitoring implementation of Guardium, the Cybersecurity organization will, within the constraints of budget and resources, ensure that ACA POA&Ms are developed within the required time frames.

Recommendation 4: **********2********** **********2**********within the required time frames in accordance with IRS guidelines.

Management's Response: The IRS agreed with this recommendation. The IRS stated that as part of its standard patch management process, the IRS is implementing ********2************and will, within the constraints of budget and resources, continue to ensure that ************2************************************ ************************************, are installed within the required time frames in accordance with IRS written guidelines.

2** **************2*********************

IRM 10.8.1, *Information Technology Security, Policy and Guidance*, requires the IRS to protect its information resources and allow the use, access, and disclosure of information in accordance with applicable laws, policies, Federal regulations, Office of Management and Budget circulars, and Treasury Directives. Also, all IRS IT resources are required to be protected at a level commensurate with the risk and magnitude of harm that could result from loss, misuse, or unauthorized access to that IT resource.

The ****2***** application provides a framework for the electronic processing of Forms 8963 and 8947 submitted to the IRS by the health insurance providers and pharmaceutical manufacturers respectively. ***********2************************************* *********************************2*** *********************************2*** *********************************2*** ******2******.

*******2******_******************2****************************** **************************2************************************** **************************2************************************** **************************2*******.

***********2********_************2****************** ******************************2************************************ ******************************2************************************ ******************************2************************************ ******************************2************************************ ******************************2************************************ *****************************2************************************* *****************************2************************************* *****************************2**********.

Figure 3 summarizes ********************2************************************* ******************************2********************************.

Figure 3: Summary of **********2********
**********2**********

Weakness Category	Number of ***2*** Weaknesses	Number of ***2*** Weaknesses	Number of ***2*** Weaknesses	Total
2[12]	***2***	***2***		***2***
2** **********2*********[13]	***2***	***2***		***2***
2 ******2****[14]	***2***			***2***
**********2********** **********2**********[15]		***2***		***2***
**********2*********[16]		***2***		***2***
**********2********** **********[17]		***2***		***2***
2**[18]		***2***		***2***
**********2********** **********2********** **********2**********[19]		***2***		***2***
*******2**********[20]			***2***	***2***
Total	***2***	***2***	***2***	***2***

Source: Fortify source code security scan report dated August 5, 2013.

[12]**********2********** **********2**********.
[13]**********2********** **********2**********.
[14]**********2**********.
[15] **********2********** **********2**********
[16]**********2********** **********2**********.
[17] **********2********** **********2**********
[18]**********2********** **********2**********.
[19]**********2**********.
[20]**********2********** ****2*****.

**********2**********
**********2**********
**********2**********
**********2**********
**********2**********
**********2**********
**********2**********.

**********2**********:

- **********2**********
  **********2**********.
- **********2**********
  **********2**********
  **********2**********.

**********2**********
**********2**********
**********2**********
**********2**********
**********2**********
**********2**********
**********2**********
**********2**********.

Recommendations

The Chief Technology Officer should ensure that:

Recommendation 5: **********2**********
**********2**********
**********2**********
**********2**********.

Management's Response: The IRS disagreed with this recommendation. The IRS stated that it executed its normal due diligence as required by the Federal Information Security Management Act to evaluate the entire system. Any residual identified risks will be mitigated through compensating controls or through the IRS's standard risk-based decision process.

Office of Audit Comment: In its response, the IRS did not provide an estimated date for when risks will be mitigated through compensating controls or through the IRS's standard risk-based decision process. In addition, during our review, the IRS informed us

that **********2**********
**********2**********
**********2**********
**********2**********
**********2**********
**********2**********
**********2**********
**********2**********
**********2*********.

Recommendation 6: **********2**********
**********2**********.

Management's Response: The IRS disagreed with this recommendation.
**********2**********
**********2**********
**********2**********
**********2**********
**********2**********
**********2**********
**********2**********.

Office of Audit Comment: Source code scans are critical to help assess and protect enterprise software and applications from security vulnerabilities. Without a source code scan, security vulnerabilities may go undetected and mitigating controls and/or strategies cannot be developed and implemented prior to application and software deployment into a production environment. **********2**********
**********2**********
**********2**********
**********2**********
**********2**********
********2**********.

Testing Performed for Affordable Care Act Information Returns Release 1

The IT Implementation and Testing organization verifies that the requirements and design for all ACA systems have been adequately tested to validate that the systems, including the AIR system, operate as intended. The AIR project personnel and the IT Implementation and Testing organization performed several types of testing to validate whether the AIR system would function as designed and meet the IRS's objectives for ACA 4.1 before it was placed into production in March 2014. Adequate testing is critical to ensure that costly retrofits are avoided

after a system is implemented. We considered the following types of testing and results for the AIR project:

- **Development System Integration Testing** – The AIR Release 1 Project personnel completed Development System Integration Testing to ensure that functional, nonfunctional, and business requirements were successfully tested prior to entering Systems Testing by the IT Implementation and Testing organization. According to the Development System Integration Testing Completion Report, the AIR Release 1 Project personnel verified and validated these requirements to ensure that the functionality and performance of the AIR system is able to process electronic Forms 8963 and 8947 and that testing should proceed to Systems Testing.
- **Systems Testing** – The IT Implementation and Testing organization completed Systems Testing of ACA 4.1, which included the AIR, IPF, and BPD systems, to verify functionality of the requirements for each of these systems. This testing did not consider the interoperability of ACA 4.1 as a whole. The Systems Testing End-of-Test Completion Report states that the test verified functionality of the ACA 4.1 business requirements. The capabilities that were validated during this test include the following:
  - The AIR System Test validated that the AIR system will receive, validate, and process the IPF and BPD electronic reports (Forms 8963 and 8947 respectively).
  - The IPF System Test validated that the IPF system will receive and process the electronic Forms 8963 from the AIR system.
  - The BPD System Test validated that the BPD system will receive and process the electronic Forms 8947 from the AIR system.
- **Release-Level Testing** – The IT Implementation and Testing organization completed Release-Level Testing of ACA 4.1. This test is a functional integration test responsible for verifying the interoperability of the ACA 4.1 systems, which includes the AIR, IPF, and BPD systems. The ACA 4.1 Release Level End-of-Test Completion Report states that the Release-Level Testing activities verified that the ACA 4.1 system satisfies the approved business requirements. The capabilities that were validated during this testing include:
  - § 9008 BPD – Validate the Taxpayer Identification Number for the filer, validate the data on the electronically filed forms, and validate the end-to-end processing of the BPD data.
  - § 9010 IPF – Validate the Taxpayer Identification Number for the filer, validate the data on the electronically filed forms, and validate the end-to-end processing of the IPF data.

- Reporting – Validate that the AIR submission reports are generated for the BPD and IPF systems.

Test Management Controls Need Improvement to Ensure Long-Term Success of the Affordable Care Act Information Returns Project

We observed a portion of ACA 4.1 Release-Level Testing and we also considered testing controls for some requirements for the AIR system. Testers who created, executed, and managed the ACA 4.1 test cases were external contractors that the IT Implementation and Testing organization personnel managed. Our review identified test management concerns that could affect the long-term success of the AIR system in the following specific areas.

Important test case development and test execution controls were not followed

Requirements are used to define specific business and technical functionalities that are needed from a system. IRM 2.127.2, *Software Testing Standards and Procedures, IT Software Testing Process and Procedures*, requires test cases to specify and document the conditions to be tested and to validate that the system functions correctly. Testers are required to determine the pass or fail status of test cases by comparing the actual results to the expected results and noting any deviations.

Test Case Development Controls

In December 2013, we observed a portion of ACA 4.1 Release-Level Testing that focused on six AIR system test cases out of a population of 188. Out of these six, we observed four instances in which the test cases did not adequately describe the expected results in the "Test Case Descriptions" field. We believe that increased contractor oversight by IT Implementation and Testing organization personnel during the development of the test cases would have helped identify this issue so that it could have been corrected prior to the start of testing. For example, the objective of three of the four test cases was to verify that the tested IPF Forms 8963[21] and supplemental attachments were successfully submitted and could be opened and that the contents of the attachments were unaltered. However, the respective Test Case Description field did not describe that the supplemental attachments should be successfully opened and that the contents should be unaltered. Also, the Test Case Description field for the remaining of the four test cases did not describe that the contents of the submitted Form 8947[22] should be unaltered.

[21] The IRS uses the information submitted on Forms 8963 to calculate and impose the annual IPF fees. Form 8963 will be used by the health insurance providers to report their net premiums written and other information.
[22] The IRS uses the information submitted on Forms 8947 and from Government programs to calculate and impose the annual BPD fee from BPD sales. Form 8947 will be used by manufacturers or importers of branded prescription drugs with gross receipts from branded prescription drug sales to Government programs, or pursuant to coverage under those programs, to report information necessary for the IRS to calculate the BPD fee. The information to be

Our concern is that the expected results should be accurate and complete in order for the testers to fully understand what they are testing and for the testers to be able to adequately compare the actual results to the expected results. Whenever actual results are not properly compared to expected results because the expected results are not effectively conveyed, the IRS may be unable to determine whether testing activities adequately validate system functionality and requirements and also ensure that the system operates as intended.

Test Execution Controls

We also observed three instances in which the testers had not verified whether the actual test case results met the expected results. After we alerted the testers about this, they then took needed steps to verify that the actual test case results met the expected results.

Improved contractor oversight by the IT Implementation and Testing organization during test execution is needed to manage risk in this area and ensure adequate testing for ACA systems. Actual test case results should meet the expected results in order to validate the functionality of the requirements being tested and to also ensure that the system operates as intended.

Management Action: The IT Implementation and Testing organization stated that based on the results of our observations, the ACA 4.1 Release-Level Test was restarted on December 19, 2013, to re-execute all test cases. This restart inserted quality checkpoints before, during, and after test case execution. The test staff ensured that for the re-execution: (1) before execution, the test case purpose and expected result associated with each verification point were clearly understood; (2) during execution, each verification point for which a discrepancy surfaced was reviewed for appropriate artifact collection; and (3) the test case results were validated.

Documentation for one test case was not available

It is important that the IRS creates test cases to document whether systems requirements and conditions are tested to validate that each system functions as intended. Documentation for each test case should include the requirements being tested to help ensure that each requirement is included in a test case and properly tested. It is also important to save and archive test cases, test case results, and related artifacts such as screen shots of the actual results as a control to help ensure that all test cases are successfully executed to validate the functionality of the system.

IRM 2.127.2, *Software Testing Standards and Procedures, IT Software Testing Process and Procedures*, requires that testing documentation (test cases, artifacts, *etc*.) be saved and archived. In addition, according to the ACA Program Configuration Management Plan, the purpose of configuration management controls is to establish and maintain the integrity of work products, including testing documentation, throughout their life cycle.

reported on Form 8947 includes (1) National Drug Codes, (2) controlled group information, (3) Medicaid State rebate information, (4) Section 45C Orphan Drug information, and (5) designated entity information.

We considered testing controls for 12 of the 347 requirements for the AIR system. The selected requirements address important functionality such as receiving and validating the data on the forms submitted to the IRS from the pharmaceutical manufacturers and health insurance providers. Important testing controls were not followed for one specific test case and its associated artifact that we considered to be important for the AIR system. ***2***** **********2********** **********2********** However, the executed test case and related artifact intended to validate this functionality was not documented or available for our review. The IRS explained that these documents were not archived as expected. However, the IRS provided a different test case to verify that the functionality of the requirement was successfully tested.

If contractor oversight, including documenting testing activities, is not adequate, the IRS may not have sufficient assurance that mission-critical system requirements are adequately tested and that the AIR system operates as intended. Consequently, the IRS may not be able to process the electronic reports from the insurance providers and pharmaceutical manufacturers and calculate the fees that they owe.

Management Action: The IT Implementation and Testing organization stated that training will continue to be provided to the staff to ensure understanding and compliance with the associated guidelines and that management will also continue to monitor staff performance and realign resources where needed to ensure that testing processes and procedures are followed.

Recommendation

Recommendation 7: The Chief Technology Officer should ensure that the IT Implementation and Testing organization effectively oversees and manages the key testing processes executed by the external contractors.

> ***Management's Response:*** The IRS agreed with this recommendation. The IRS stated that as a direct result of the testing audit findings, it ensures that a Federal tester resource is aligned to provide oversight on each test effort for which an external vendor is engaged. Since the findings of this audit, a Federal tester resource was engaged and remains in place for test case review during preparation (peer review process that validates the accuracy of the test case description, requirements cited, and verification points) and for post-test execution to validate test results and outcomes and to ensure proper artifact collection.

Appendix I

Detailed Objective, Scope, and Methodology

Our overall objective was to determine if the IRS is adequately mitigating systems development risks under the ACA Program to achieve business and information technology goals for the AIR Release 1 Project as a core system for the program. To accomplish our objective, we:

I. Analyzed systems testing activities for the AIR Release 1 Project, while following the ELC COTS Path, in accordance with the Treasury, Internal Revenue Manual, and other applicable guidelines.

   A. Interviewed the AIR project manager and IT Implementation and Testing organization personnel to discuss how risks are being mitigated regarding systems testing activities.

   B. Reviewed and analyze testing criteria, processes, and results.

   C. Analyzed the ACA Program and AIR Release 1 Project test plans (*e.g.*, ACA 4.1 Development Systems Integration Test Plan, ACA 4.1 Consolidated Project-Level Systems Test Plan, and ACA 4.1 Release-Level Integration Test Plan).

   D. Considered testing controls for some requirements for the AIR system.

   E. Conducted on-site observations of testing activities to determine if AIR Release 1 Project tests were completed in accordance with applicable guidelines.

II. Determined whether security controls were designed into the AIR Release 1 Project to protect taxpayer data in accordance with IRM and NIST guidelines.

   A. Reviewed security scan results and mitigation actions.

      1. **********2**********2********.

      2. Determined if issues identified as a result of the security scan results were properly mitigated.

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 the following internal controls were relevant to our audit objective: IRM and related IRS guidelines and the processes followed in the development of information technology projects using the COTS Path as they apply to the ACA Program's AIR Release 1 Project.

We evaluated these controls by conducting interviews with management and staff, making observations of systems development and testing activities, and reviewing relevant documentation. Documents reviewed include the AIR Project Management Plan, AIR testing and security plans, AIR security scan result reports, and other documents that provided evidence as to whether the IRS is adequately managing systems development risks for the AIR Release 1 Project.

Appendix II

Major Contributors to This Report

Alan Duncan, Assistant Inspector General for Audit (Security and Information Technology Services)
Danny Verneuille, Acting Assistant Inspector General for Audit (Security and Information Technology Services)
Gwendolyn McGowan, Director
Suzanne Westcott, Audit Manager
Kevin Liu, Audit Manager
David Allen, Lead Auditor
Allen Henry, Program Analyst
Nicholas Reyes, Information Technology Specialist
Mildred R. Woody, Senior Auditor

Appendix III

Report Distribution List

Commissioner C
Office of the Commissioner – Attn: Chief of Staff C
Deputy Commissioner for Operations Support OS
Deputy Commissioner for Services and Enforcement SE
Director, Affordable Care Act Office SE:ACA
Deputy Chief Information Officer for Operations OS:CTO
Director, Privacy, Governmental Liaison and Disclosure OS:P
Associate Chief Information Officer, Affordable Care Act (PMO) OS:CTO:ACA
Chief Counsel CC
National Taxpayer Advocate TA
Director, Office of Legislative Affairs CL:LA
Director, Office of Program Evaluation and Risk Analysis RAS:O
Office of Internal Control OS:CFO:CPIC:IC
Audit Liaisons:
    Deputy Commissioner for Services and Enforcement SE
    Director, Business Planning and Risk Management OS:CTO:SP:RM

Appendix IV

**********2**********

**********2**********

**********2**********

**********2**********			
**********2**********			
**********2**********			
**********2**********			
**********2**********			
**********2**********			

**********2**********			
**********2**********			
**********2**********			
**********2**********			
**********2**********			
**********2**********			
**********2**********			
**********2**********			

**********2**********			
**********2**********			
**********2**********			
**********2**********			
**********2**********			
**********2**********			
**********2**********			

**********2**********			
**********2**********			
**********2**********			
**********2**********			
**********2**********			
**********2**********			
**********2**********			
**********2**********			
**********2**********			

**********2**********			
**********2**********			
**********2**********			
**********2**********			
**********2**********			
**********2**********			
**********2**********			
**********2**********			
**********2**********			

**********2**********			
**********2**********			
**********2**********			
**********2**********			
**********2**********			
**********2**********			
**********2**********			
**********2**********			
**********2**********			

**********2**********			
**********2**********			
**********2**********			
**********2**********			
**********2**********			
**********2**********			

**********2**********.

**********2**********
**********2**********
**********2**********
**********2**********.

Appendix V

Glossary of Terms

Term	Definition
Affordable Care Act (ACA)	In March 2010, the President signed into law the Patient Protection and Affordable Care Act to provide more Americans with access to affordable health care by January 1, 2014.
Authentication	The process by which a system verifies the identity of a user who wishes to access it.
Branded Prescription Drug (BPD)	Any prescription drug for which an application was submitted under section 505(b) of the Federal Food, Drug, and Cosmetic Act (21 U.S.C. 355(b)) or any biological product the license for which was submitted under section 351(a) of the Public Health Service Act (42 U.S.C. 262(a)).
****2****** *****2****	**********2********** **********2********** **********2**********
Commercial Off-the-Shelf (COTS) Path	One of the five paths of the ELC. The COTS Path specifies a development approach based on the purchase and use of prepackaged software.
Configuration	The way a computer system or program is prepared for a particular use.
Critical Code Weakness	According to the IRS, critical priority weaknesses have both a high potential impact and a high likelihood of occurring. They represent the highest security risks to an application and should be remediated immediately.
Enterprise Life Cycle (ELC)	The approach used by the IRS to manage and implement business change through information systems initiatives.
Enterprise Operations (EOps) Organization	Provides efficient, cost-effective, and highly reliable computing (server and mainframe) services for all IRS business entities and taxpayers.
Error	A Guardium Vulnerability scan error is an instance in which a tested condition could not be executed for certain reasons, such as insufficient administrator permissions.

Term	Definition
Exposure	A system configuration issue or a mistake in software that allows access to information or capabilities that can be used by a hacker as a stepping-stone into a system or network.
Failure	A Guardium Vulnerability scan failure is an instance in which the tested condition does not meet the expected outcome and is marked as failed.
False Positive	A suspected weakness found during software code analysis that is not really a weakness.
Fortify	Hewlett-Packard's Fortify tool scans software source code, identifies root causes of software security vulnerabilities, and correlates and prioritizes the results by providing a risk-ranked list of issues for closing gaps in the security of the software.
Guardium Tool	Scans database infrastructures on a scheduled basis to detect vulnerabilities to include in security patch updates and suggests remedial actions.
Hardening	Providing various means of protection in a computer system. Protection is provided in various layers and is often referred to as 'defense in depth.' Protecting in layers means to protect at the host level, the application level, the operating system level, the user level, the physical level, and all the sublevels in between. A hardened computer system is a more secure computer system.
Health and Human Services	The U.S. Government's principal agency for protecting the health of all Americans and providing essential human services.
High Code Weakness	According to the IRS, high-priority weaknesses have the potential for high impact but a low likelihood of occurring and should be remediated in the next scheduled patch release.
Low Code Weakness	According to the IRS, low priority weaknesses have low potential impact and a low likelihood of occurring and represent a minor security risk to an application.
Medium Code Weakness	According to the IRS, medium priority weaknesses have a low potential impact but a high likelihood of occurring. They represent a moderate risk to an application and are easy to detect and exploit.

Term	Definition
National Institute of Standards and Technology (NIST)	A nonregulatory Federal agency within the Department of Commerce responsible for developing standards and guidelines, including minimum requirements, for providing adequate information security for all Federal Government agency operations and assets.
Non-Exchange	The ACA provisions that affect the IRS can be broken down into two major categories: (1) Exchange-related provisions and (2) Non-Exchange provisions. The Non-Exchange provisions relate to traditional IRS processing capabilities, such as the collection of IPF and BPD fees.
Orphan Drug	A drug that is intended for the safe and effective treatment, diagnosis, or prevention of rare diseases/disorders that affect fewer than 200,000 people in the United States.
Patch	A small file that when executed will patch or fix specific problems in a target file or application.
Path Manipulation	Allowing user input to control paths used in file system operations that could enable an attacker to access or modify otherwise protected system resources. Path manipulation errors occur when the following two conditions are met: • An attacker specifies a path used in an operation on the file system. • By specifying the resource, the attacker gains a capability that would not otherwise be permitted. For example, the program may give the attacker the ability to overwrite the specified file or run with a configuration controlled by the attacker.
Port	A data connection in a computer to which a peripheral device or a transmission line from a remote terminal can be attached.
Requirement	A formalization of a need and the statement of a capability or condition that a system, subsystem, or system component must have or meet to satisfy a contract, standard, or specification.
Structured Query Language (SQL)	The standard language for relational database management systems. SQL statements are used to perform tasks such as update data on a database or retrieve data from a database.

Term	Definition
Test Case	Created to specify and document the conditions to be tested and to validate that a system functions as intended.
Vulnerability	A mistake in software that can be directly used by a hacker to gain access to a system or network.
XML Injection	Allowing unvalidated data into an XML document can allow an attacker to change the structure and contents of the XML. XML injection occurs when: • Data enters a program from an untrusted source. • The data are written to an XML document. Applications typically use XML to store data or send messages. When used to store data, XML documents can potentially contain sensitive information. XML messages are often used in Web services, can be used to transmit sensitive information, and can be used to send authentication credentials. XML documents and messages can be altered if an attacker has the ability to write raw XML.

Appendix VI

Management's Response to the Draft Report

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

CHIEF' TECHNOLOGY OFFICER

September 25, 2014

MEMORANDUM FOR DEPUTY INSPECTOR GENERAL FOR AUDIT

FROM: *for* Terence V. Milholland /s/ Stephen Manning
Chief Technology Officer

SUBJECT: Draft Audit Report - Affordable Care Act: Improvements Are Needed to Strengthen Security and Testing Controls for the Affordable Care Act Information Returns (AIR) Project - Audit# 201320315 (e-trak #2014-58568)

Thank you for the opportunity to review your draft audit report and meet with the audit team to discuss earlier report observations. The IRS is committed to ensuring the security of our information technology systems and maintaining appropriately configured databases. Your report acknowledges our security practices and makes several recommendations that upon implementation, will contribute to our shared objective of identifying and mitigating security vulnerabilities.

We are equally committed to ensuring that we deploy quality systems and have well-honed and robust software testing practices. In observing test execution for the release, your audit team identified an instance where increased contractor oversight by IRS testing personnel was needed to ensure we receive the best possible outcomes from test execution. Your team's feedback was very timely. Immediately upon receiving it, we inserted additional IRS oversight on this contractor-staffed team and completely re-executed a portion of our testing prior to system deployment.

The attachment to this memo details our planned corrective actions to implement those recommendations or portions of recommendations with which we concur. We do not concur with TIGTA's assertion that we should include **********2**********2**********2********.

The IRS values your continued support and the assistance your organization provides. If you have any questions, please contact me at (202) 622-6800 or Lisa Starr, Program Oversight Coordination Manager at (240) 613-4219.

Attachment

Attachment

RECOMMENDATION #1: The Chief Technology Officer should ensure processes and procedures are developed to provide direction on how to review and mitigate weaknesses *********2********** **********2**********.

CORRECTIVE ACTION #1: The IRS agrees with this recommendation. IT Cybersecurity has integrated Guardium in its Security Assessment and Authorization (SA&A) processes including creation of Plan of Action and Milestones (POA&Ms). IT Cybersecurity, working with EOps, within the constraints of budget and resources, will revise the processes and procedures developed for the SA&A process to provide direction on how to review and *********2********** during continuous monitoring.

IMPLEMENTATION DATE: October 25, 2015

RESPONSIBLE OFFICIAL: The Associate Chief Information Officer, Cybersecurity

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

RECOMMENDATION #2: The Chief Technology Officer should ensure all vulnerability weaknesses *****2********** are promptly corrected and resolved **********2********** **********2**********.

CORRECTIVE ACTION #2: The IRS partially agrees with this recommendation. The Branded Prescription Drug (BPD) Database, *****2**********, is being migrated to an upgraded version of the database software. In addition, to mitigate vulnerability weaknesses and manage risk, we will create a risk-based decision regarding the processing of electronic form reports that will align the AIR system and BPD database to be consistent with our established risk management policies. Once the migration is complete, we will, within the constraints of budget and resources, request another scan to verify compliance.

IMPLEMENTATION DATE: November 25, 2014

RESPONSIBLE OFFICIAL: The Associate Chief Information Officer, Enterprise Operations

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

Attachment

RECOMMENDATION #3: The Chief Technology Officer should ensure ACA POA&Ms, ******2********, are developed for each vulnerability weakness identified, and the mitigation actions adequately address the vulnerability weaknesses within the required time frames in accordance with IRS guidelines.

CORRECTIVE ACTION #3: The IRS agrees with this recommendation. As noted in recommendation 1, IT Cybersecurity has a process that ensures vulnerabilities found during annual security assessments have actionable POA&M's created timely. As a part of the continuous monitoring implementation of Guardium, IT Cybersecurity will, within the constraints of budget and resources, ensure ACA POA&Ms are developed within the required timeframes.

IMPLEMENTATION DATE: November 25, 2014

RESPONSIBLE OFFICIAL: The Associate Chief Information Officer, Cybersecurity

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

RECOMMENDATION #4: The Chief Technology Officer should ensure ********2********** **********2*********within the required time frames in accordance with IRS guidelines.

CORRECTIVE ACTION #4: The IRS agrees with this recommendation. As part of our standard patch management process, IRS is implementing **********2**********and will, within **********2******* **********2**********, are installed within the required time frames in accordance with IRS written guidelines.

IMPLEMENTATION DATE: October 25, 2015

RESPONSIBLE OFFICIAL: The Associate Chief Information Officer, Enterprise Operations

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

RECOMMENDATION #5: The Chief Technology Officer should **********2********* **********2********** **********2**********.

Attachment

CORRECTIVE ACTION #5: The IRS disagrees with this recommendation. The IRS has executed its normal due diligence as required by the FISMA to evaluate the entire system. Any residual identified risks will be mitigated through compensating controls or through the IRS's standard risk based decision process.

IMPLEMENTATION DATE: Not Applicable

RESPONSIBLE OFFICIAL: The Associate Chief Information Officer, Cybersecurity

CORRECTIVE ACTION MONITORING PLAN: Not Applicable

RECOMMENDATION #6: The Chief Technology Officer should ensure **********2********* **********2**********.

CORRECTIVE ACTION #6: The IRS disagrees with this recommendation. **********2********* **********2********** **********2********** **********2********** **********2**********.

IMPLEMENTATION DATE: Not Applicable

RESPONSIBLE OFFICIAL: The Associate Chief Information Officer, Cybersecurity

CORRECTIVE ACTION MONITORING PLAN: Not Applicable

RECOMMENDATION #7: The Chief Technology Officer should ensure that the IT Implementation and Testing organization effectively oversee and manage the key testing processes executed by the external contractors.

CORRECTIVE ACTION #7: The IRS agrees with this recommendation and as a direct result of the audit findings, I&T ensures that a Federal tester resource is aligned to provide oversight on each test effort, where an external vendor is engaged. Since the findings from this audit, a Federal tester resource was engaged and remains in place for test case review during preparation (peer review process - validates accuracy of description, requirements cited, and verification points); and, post-test execution to validate test results/outcomes and proper artifact collection.

IMPLEMENTATION DATE: Completed (December 29, 2013)

Attachment

RESPONSIBLE OFFICIAL: The Associate Chief Information Officer, Affordable Care Act PMO

CORRECTIVE ACTION MONITORING PLAN: Not Applicable