TREASURY INSPECTOR GENERAL FOR TAX ADMINISTRATION

Affordable Care Act Verification Service: Security and Testing Risks

September 28, 2015

Reference Number: 2015-23-081

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 VERIFICATION SERVICE: SECURITY AND TESTING RISKS

Highlights

Final Report issued on September 28, 2015

Highlights of Reference Number: 2015-23-081 to the Internal Revenue Service Chief Technology Officer and Director, Services and Enforcement Affordable Care Act Office.

IMPACT ON TAXPAYERS

Starting with Tax Year 2014 individual income tax returns, the Affordable Care Act (ACA) requires taxpayers to file new forms (*e.g.*, Form 8962, *Premium Tax Credit*, and Form 8965, *Health Coverage Exemptions*) to report that they have qualifying health care coverage, are eligible for a health coverage exemption, or make a shared responsibility payment. To process the new forms, the IRS developed the ACA Verification Service (AVS).

WHY TIGTA DID THE AUDIT

The overall objective was to determine if the IRS adequately developed and tested the AVS.

WHAT TIGTA FOUND

The ACA authorizing official signed the ACA security authorization and the AVS was placed into production on January 20, 2015, prior to the completion of the security assessment. The authorizing official made this decision based on the results of security testing that had been completed, the Cybersecurity organization's memorandum concurring with the authorizing official's granting of an update to the current security authorization, and the urgent need to deploy ACA Release 5.0 at the start of the 2015 Filing Season. The Cybersecurity organization completed the security assessment in May 2015. AVS testing delays prevented the completion of security testing and the completion of documents needed for the security authorization package prior to deploying the AVS into production.

In addition, delays in testing extended the test period. Testing delays were caused by late code deliveries, changes in the test environment, and time needed to correct defects. Testing delays also caused numerous ACA builds, including the AVS, to be submitted for the Final Integration Test program approximately one week before the start of the 2015 Filing Season, increasing the risk that defects would not be corrected prior to production.

Finally, test results from designated sources did not match the test results reported in the project-level and release-level draft End-of-Test Completion Reports. Discrepancies identified were due to clerical errors and the use of the Implementation and Testing organization's internal tracking system instead of only using the mandated tools.

WHAT TIGTA RECOMMENDED

TIGTA recommended the Chief Technology Officer ensure that: 1) AVS security vulnerabilities are corrected prior to the next filing season; 2) security testing and security authorization packages are completed prior to authorizing and placing systems into production; 3) ACA developers are notified in advance when changes to the development, test, and production environments are made; and 4) testing organizations use only the information from the designated tools for documenting requirements, test results, and defects to prepare the End-of-Test Completion Report.

In their response to the report, IRS officials agreed with two of the four recommendations and partially agreed with the remaining two. For vulnerabilities that cannot be corrected prior to the next filing season, the IRS plans to continue following established procedures for addressing the vulnerabilities. When security testing and security authorization packages cannot be completed prior to system deployment, the IRS plans to exercise risk-based decisionmaking with appropriate governance approvals and documentation. IRS officials also stated that they have taken or plan to take appropriate corrective actions.

TREASURY INSPECTOR GENERAL
FOR TAX ADMINISTRATION

DEPARTMENT OF THE TREASURY
WASHINGTON, D.C. 20220

September 28, 2015

MEMORANDUM FOR CHIEF TECHNOLOGY OFFICER
DIRECTOR, SERVICES AND ENFORCEMENT AFFORDABLE CARE ACT OFFICE

FROM: Michael E. McKenney
Deputy Inspector General for Audit

SUBJECT: Final Audit Report – Affordable Care Act Verification Service: Security and Testing Risks (Audit # 201520324)

This report presents the results of our review to determine if the Internal Revenue Service adequately developed and tested the Affordable Care Act[1] Verification Service. This review is included in the Treasury Inspector General for Tax Administration's Fiscal Year 2015 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 Internal Revenue Service managers affected by the report recommendations. If you have any questions, please me or Danny Verneuille, Acting Assistant Inspector General for Audit (Security and Information Technology Services).

[1] Collectively, the Patient Protection and Affordable Care Act (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) and the Health Care and Education Reconciliation Act of 2010 (Pub. L. No. 111-152, 124 Stat. 1029 (see Affordable Care Act, *infra*)).

Table of Contents

Abbreviations

ACA	Affordable Care Act
AVS	Affordable Care Act Verification Service
EOTCR	End-of-Test Completion Report
EPD	Exchange Periodic Data
FIT	Final Integration Testing
IRS	Internal Revenue Service
I&T	Implementation and Testing
KISAM	Knowledge Incident/Problem Service Asset Manager
PTC	Premium Tax Credit
RTVM	Requirements Traceability Verification Matrix

Background

The Affordable Care Act[1] (ACA) was enacted in March 2010 to provide more Americans with access to affordable health care. The ACA created the Health Insurance Marketplace, also known as the Exchange. An Exchange is where individuals find information about health insurance options, purchase health plans, and, if eligible, obtain help paying premiums. Individuals began using the Exchanges on October 1, 2013, to purchase health insurance for Calendar Year 2014. The Department of Health and Human Services reported in March 2015 that the individual Exchange consisted of 14 States (including the District of Columbia) that operated their own Exchanges and 37 States that used the Federal Exchange during the 2015 Open Enrollment Period that ran from November 15, 2014, through February 15, 2015. Two significant ACA provisions that took effect starting with 2014 individual income tax returns are the individual shared responsibility provision and the Premium Tax Credit (PTC).

Individual Shared Responsibility Provision – Under the individual shared responsibility provision, individuals must have qualifying health care coverage for every month during the calendar year, qualify for a health coverage exemption, or make a shared responsibility payment with their tax return. Taxpayers who had qualifying coverage for every month check a box on their tax return. Form 8965, *Health Coverage Exemptions*, is used to report an exemption from coverage. Some coverage exemptions are available only from an Exchange, others are available only by claiming them on Form 8965, and others are available from either an Exchange or by claiming them on Form 8965. Taxpayers who have neither qualifying health care coverage nor a coverage exemption for any month during the calendar year are required to report a shared responsibility payment on their tax return.

Premium Tax Credit – The PTC is a refundable tax credit that assists eligible taxpayers with paying premiums of health insurance purchased from an Exchange. When enrolling in health insurance through an Exchange, individuals can choose to have some or all of the advance payment of the PTC paid to the insurance company on their behalf or can wait to claim the PTC as a credit on their tax return.[2] Because the Exchange's computation of the advance payment of the PTC is based on estimates of an individual's anticipated income and family size for the upcoming calendar year, the final amount of PTC taxpayers are entitled to receive is determined when they prepare their tax return.

[1] Collectively, the Patient Protection and Affordable Care Act (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) and the Health Care and Education Reconciliation Act of 2010 (Pub. L. No. 111-152, 124 Stat. 1029 (see Affordable Care Act, *infra*)).
Also, see Appendix IV for a glossary of terms.

[2] The Bureau of the Fiscal Service within the U.S. Department of the Treasury issues the monthly advance payment of the PTC to the insurers.

Taxpayers who purchased insurance through an Exchange are required to include Form 8962, *Premium Tax Credit*, with their tax return to claim the PTC. Taxpayers who received an advance payment of the PTC are required to file Form 8962 to reconcile the advance payment paid to the insurance company on their behalf against the amount of PTC to which they are entitled. Based on this reconciliation, taxpayers who are entitled to more PTC than was provided in advance receive the additional credit on their tax return. However, taxpayers who are entitled to less PTC than was provided in advance incur additional tax on their return subject to certain limitations.

Recognizing the critical role that information technology plays in executing the Internal Revenue Service's (IRS) responsibilities under the ACA, the IRS created the ACA Program Management Office within the Information Technology organization in January 2011 to ensure a dedicated focus on fulfilling ACA requirements. The ACA Program Management Office is developing numerous releases of ACA software to implement ACA provisions that take effect over several years. Under ACA Release 5.0, the ACA Program Management Office developed the ACA Verification Service (AVS) to process new Forms 8962 and 8965 filed by taxpayers during the 2015 Filing Season. The AVS will also identify taxpayers who received an advance payment of the PTC but did not file the required Form 8962 with their tax return. The AVS went into production at the start of the 2015 Filing Season on January 20, 2015.

AVS Checks of Form 8962 – At the time of filing Form 8962, the AVS performs:

- Math, completeness, and consistency checks of Form 8962.
- Compliance checks using data the IRS received from the Exchanges to confirm that taxpayers claiming the PTC on Form 8962 had enrolled in health care coverage from the Exchanges.
- Compliance checks of the PTC by matching the amount of certain figures reported on Form 8962 to figures reported to the IRS by the Exchanges.

Math, completeness, and consistency checks of Form 8962 are performed by the AVS using data reported on the form to ensure that the form was prepared correctly and in accordance with instructions. Compliance checks of Form 8962 ensure that taxpayers claiming the PTC had enrolled in health coverage from the Exchanges and that they correctly reported on Form 8962 certain figures essential to the accuracy of the amount of the PTC. These compliance checks are performed by matching the amount of these figures against data submitted to the IRS by the Exchanges.

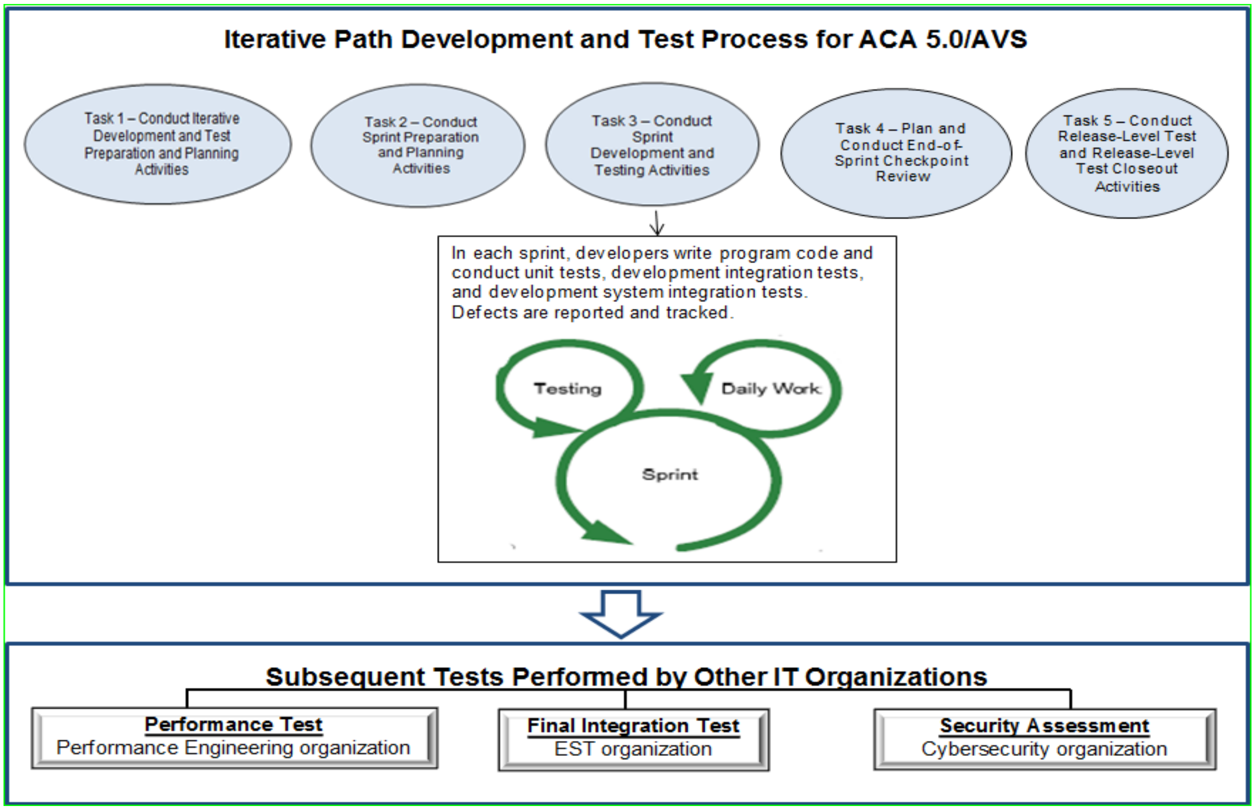
The ACA requires Exchanges to provide the IRS with information on individuals who are enrolled by the Exchanges on a monthly basis. These monthly reports are referred to as Exchange Periodic Data (EPD). The AVS performs at-filing compliance checks of Forms 8962 by matching the amounts of the Premium, Second Lowest Cost Silver Plan, and advance payment of the PTC reported by the taxpayer on Form 8962 to the amounts reported to the IRS in EPD. This compliance check is important because the amount of the Premium and Second Lowest Cost Silver Plan reported on the return must be accurate to correctly calculate the amount of the PTC, and the amount of the advance payment of the PTC reported on the return must be accurate to correctly perform the reconciliation necessary for determining if the taxpayer will receive additional credit or incur additional tax.

AVS Checks for Form 8962 Nonfilers – At the time of filing, the AVS performs a compliance check to identify Form 8962 nonfilers. The AVS matches taxpayers reported as receiving an advance payment of the PTC in EPD against every individual income tax return filed to identify taxpayers who received an advance payment but did not file the required Form 8962.

AVS Checks of Form 8965 – At the time of filing, the AVS performs completeness and consistency checks of Form 8965 to ensure that the form was prepared correctly and in accordance with instructions, using data reported on the form.

The ACA Program Management Office developed the AVS using the Iterative Path process whereby development and testing occurs through a series of repeated cycles (sprints). In each sprint, a small increment of the system is developed and tested until the system is completed. In addition to being tested in the Iterative Path process, the AVS is included in tests performed by other IRS Information Technology organizations. For example, the security assessment is performed by the Cybersecurity organization. Figure 1 shows the tasks within the Iterative Path process and the subsequent tests that included the AVS.

Figure 1: The Iterative Path Process and Subsequent Testing


Iterative Path Development and Test Process for ACA 5.0/AVS
Task 1 – Conduct Iterative Development and Test Preparation and Planning Activities
Task 2 – Conduct Sprint Preparation and Planning Activities
Task 3 – Conduct Sprint Development and Testing Activities
Task 4 – Plan and Conduct End-of-Sprint Checkpoint Review
Task 5 – Conduct Release-Level Test and Release-Level Test Closeout Activities
In each sprint, developers write program code and conduct unit tests, development integration tests, and development system integration tests. Defects are reported and tracked.
Testing
Daily Work
Sprint
Subsequent Tests Performed by Other IT Organizations
Performance Test
Performance Engineering organization
Final Integration Test
EST organization
Security Assessment
Cybersecurity organization

Source: *Iterative Development and Testing Process Description, Version 1, dated November 15, 2011, and the IRS Information Technology organization website.* EST = Enterprise Systems Testing; IT = Information Technology.

The Performance Engineering organization is responsible for conducting performance tests for ACA Release 5.0, which included the AVS. The Enterprise Systems Testing organization conducts the Systems Acceptability Test and the Final Integration Test (FIT) program, which is the integrated end-to-end testing of multiple systems that support the high-level business requirements of the IRS. The FIT is the final step of the application software testing effort designed to ensure that revisions to IRS computer applications interoperate correctly prior to the tax return filing season. The Cybersecurity organization is responsible for conducting the security assessment. For the 2015 Filing Season, these organizations tested the new ACA Release 5.0 systems, which included the AVS.

Within the ACA Program Management Office, AVS testing was performed at the project level and release level. Project-level testing was performed by two groups:

- AVS developers are responsible for developing code and conducting unit tests, development integration tests, and development system integration tests. AVS developers created and tested the AVS in seven sprints. An eighth sprint was conducted to support end-to-end testing, fix defects, and review and implement change requests.

- The ACA Implementation and Testing (I&T) organization independently performs functional and regression tests[3] to verify that all functionality within a system operates as expected prior to a release-level test. The I&T organization performed its project-level tests in eight sprints.

Figure 2 details planned AVS development dates.

Figure 2: Planned AVS Development Dates

Planned Dates	Activities
June 2014	Completion of AVS development and project-level testing.
July 2014	Start of release-level testing.
September 2014	Start of FIT.
January 2015	AVS to be placed into production.

Source: AVS Contingency Management Plan, Version 2.0, dated May 1, 2014, and ACA Program Management Office I&T Organization Consolidated Project-Level System Test Plan ACA 5.0 Version 1.1, dated April 1, 2014.

Figure 3 shows the planned and actual schedule for the I&T organization’s project-level testing for each sprint and the delays that occurred.

[3] Regression testing will be performed as needed when new builds are delivered to ensure that new functionality and defect correction are working as required and did not adversely impact affected components.

Figure 3: Schedule and Delays in the I&T Organization's Testing for Each Project-Level Sprint

Key Testing Activity	I&T ***Estimated*** Timeline/Duration	I&T ***Actual*** Test Dates
Sprint 1	8/27/13 – 10/21/13	No I&T testing this period. Sprint 1 test cases were deferred to Sprint 2 for testing.
Sprint 2	10/22/13 – 11/18/13	No I&T testing this period. Sprints 1 and 2 test cases were deferred to Sprint 3 for testing.
Sprint 3	11/19/13 – 1/6/14	No I&T testing this period. Test cases from Sprints 1–3 were deferred to Sprint 4 for test execution.
Sprint 4	1/7/14 – 2/18/14	2/3/14 – 2/14/14. Executed 50 percent of test case inventory to support the Generalized Mainline Framework capability. The code to support Modernized e-File capability was not tested due to a defect found during an integration test. Test cases were deferred to Sprint 5 while the defect was being addressed.
Sprint 5	2/19/14 – 3/31/14	No testing was performed because the code delivered contained defects that would prevent successful verification of the capabilities. Test cases were deferred to Sprint 6 for testing.
Sprint 6	4/1/14 – 5/12/14	4/4/14 – 5/8/14. Test cases from the prior sprints were executed. Sprint 6 test cases were deferred to Sprint 7 for testing.
Sprint 7	5/13/14 – 6/23/14	5/12/14 – 6/23/14. Outstanding defects caused a significant block in test execution, so the remaining test cases were deferred to Sprint 8.
Sprint 8[4]	6/23/14 – 8/4/14	6/26/14 – 10/10/14.
End-of-Test Completion Report (EOTCR)	7/23/14	As of 6/4/15, the final report has not been approved and issued.

Source: ACA 5.0 Consolidated Project-Level System Test Plan Version 1.1, dated April 1, 2014, and various ACA 5.0 status reports.

I&T release-level testing is a functional integration test limited to the verification of ACA-developed systems interfacing with the current production environment systems.

[4] This was added after it was determined that additional time was needed to correct defects and complete testing.

Release-level testing was performed by the I&T organization and consisted of four phases. Phases I and II included preparatory activities, *e.g.*, validating connections between ACA systems, and then 1) validating connections between the current production environment and ACA systems to support the Enterprise Systems Testing organization's early integration testing and 2) testing the baseline functionality of the ACA Release 5.0 systems to confirm readiness of release-level testing. Phase III was the official start of release-level testing, and it focused on validating end-to-end tax return processing from input systems through the Enterprise Systems Testing organization's systemic processing of tax returns. Phase IV was the test execution for the Information Returns Processing and Reporting system and Change Management Support. The Change Management Support phase was an extension of the test execution phase. This phase provided test support for approved change requests, defect fixes, and regression testing.

Figure 4 shows the planned and actual schedule for the test execution phases for ACA Release 5.0 release-level testing and the delays that occurred.

Figure 4: Schedule and Delays in ACA Release 5.0 Release-Level Testing

Test Execution Phase	Planned Test Dates	Actual Test Dates
Phase III: Tax Return Processing	9/2/14 – 11/26/14	10/21/14 – 1/16/15
Phase IV: Information Returns Processing and Reporting	10/1/14 – 11/26/14	11/13/14 – 1/16/15
Phase IV: Change Management Support	11/28/14 – 12/17/14	11/28/14 – 1/16/15
EOTCR Development	1/2/15 – 4/7/15	A final signed report was issued on 7/16/15.

Source: IRS ACA Program Management Office I&T Organization Release-Level Test Plan ACA 5.0 v1.0, dated August 21, 2014; IRS Information Technology ACA Program Management Office Briefing to the Chief Technology Officer ACA 5.0 through 7.1, dated January 21, 2015; and I&T Executive Dashboards for the ACA 5.0 Release.

This review was performed at the IRS ACA Program Management Office in Lanham, Maryland, during the period January through August 2015. We conducted this performance audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objective. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objective. Detailed information on our audit objective, scope, and methodology is presented in Appendix I. Major contributors to the report are listed in Appendix II.

Results of Review

The Updated Security Authorization Was Signed and the Affordable Care Act Verification Service Was Placed Into Production Prior to the Completion of Security Testing

Internal Revenue Manual 10.8.1, *Information Technology Security, Policy and Guidance*, defines a security assessment as a comprehensive testing and assessment of the security controls in an information system to determine the extent to which controls are implemented correctly, operating as intended, and producing the desired security outcome. A security assessment is performed in support of a security authorization. A security authorization is the official management decision given by a senior agency official to authorize operation of an information system and to explicitly accept the risk to agency operations based on the implementation of security controls. Systems are assigned an authorizing official who assumes formal responsibility for operating an information system at an acceptable level of risk and who is accountable for the security risks associated with the information system. Internal Revenue Manual 10.8.1 also requires that the IRS use the security assessment and authorization process provided in National Institute of Standards and Technology Special Publication 800-37, *Guide for Applying the Risk Management Framework to Federal Information Systems* (February 2010).

The risk management framework in Special Publication 800-37 provides a disciplined and structured process that integrates information security and risk management activities into the systems development life cycle. The security assessment and security authorization are two of the six steps in that process. All tasks are completed prior to placing the information system into operation or continuing its operation.

Special Publication 800-37 requires that three key documents used by the authorizing official in making risk-based authorization decisions be included in the security authorization package. The security authorization package is provided to the authorizing official and includes comprehensive information on the security state of the information system.

- **System Security Plan –** This is a formal document that provides an overview of the security requirements for the information system and describes the security controls in place or planned for meeting those requirements. The System Security Plan is updated based on the findings of the security assessment and any remediation actions taken. The updated System Security Plan reflects the actual state of the security controls after the initial security assessment and any modifications in addressing recommendations for corrective actions. At the completion of the security assessment, the System Security Plan contains an accurate list and description of the security controls implemented and a list of residual vulnerabilities.

- **Security Assessment Report –** The results of security assessments, including recommendations for correcting any security weaknesses or deficiencies, are documented in the Security Assessment Report. The Security Assessment Report is an important factor in an authorizing official's decision to authorize operation of an information system.
- **Plan of Action and Milestones –** This describes the specific measures that are planned to correct weaknesses or deficiencies in security controls noted during the security assessment and to address known vulnerabilities in the information system. It details resources required to accomplish the elements of the plan, any milestones in meeting the tasks, and scheduled completion dates for the milestones. The plan of action and milestones is used by the authorizing official to monitor progress in correcting weaknesses or deficiencies noted during the security assessment. All security weaknesses and deficiencies identified during the security assessment are documented in the Security Assessment Report to maintain an effective audit trail. Organizations develop specific plans of action and milestones based on the results of the security assessment.

The security authorization decision document conveys the final security authorization decision by the authorizing official. The security authorization decision document contains the authorization decision, terms and conditions for the authorization, and the authorization termination date.

The Cybersecurity organization within the IRS Information Technology organization performs the security assessment. The authorizing official responsible for the security authorization is usually an IRS official who has budgetary oversight for an information system or is responsible for the business operations supported by the system. An official from the ACA Office under the Deputy Commissioner for Services and Enforcement is the authorizing official for ACA Release 5.0.

National Institute of Standards and Technology Special Publication 800-37 and Internal Revenue Manual 10.8.1 require a security authorization to be updated (reauthorized) when a significant change occurs to the information system. This type of reauthorization targets only the specific security controls affected by the changes. On January 2, 2015, an updated ACA security authorization was signed to include changes created by ACA Release 5.0. ACA Release 5.0 contained changes to three existing ACA systems plus the addition of two new systems, including the AVS.

The ACA authorizing official signed the authorization, and the AVS was placed into production on January 20, 2015, prior to the completion of the security assessment. The authorizing official made this decision based on the results of security testing that had been completed, the Cybersecurity organization's memorandum concurring with the authorizing official's granting of an update to the current security authorization, and the urgent need to deploy ACA Release 5.0 at the start of the 2015 Filing Season. The Cybersecurity organization completed the security assessment in May 2015.

At the time the updated ACA security authorization was signed, the security assessment included security scans of the ACA Release 5.0 server operating systems, database systems, program code, and network that were performed in the last week of December 2014. These scans are designed to identify vulnerabilities in the configurations and settings of the systems and to ensure that configurations and settings conform to IRS security policies. The program code and network scans applied to AVS servers, but the database system scans did not because the AVS does not have databases. AVS server operating systems were not part of the December 2014 security scanning. On December 31, 2014, the Cybersecurity organization provided the authorizing official with an executive summary of the scanning results that the authorizing official considered in issuing the updated ACA security authorization. The AVS server operating systems were scanned on January 6, 2015, four days after the signing of the updated ACA security authorization but before the start of the filing season. Because Cybersecurity staff stated that it needs to perform its scans in the production environment, the AVS servers were scanned on January 6, 2015, which is the date they were placed into the production environment. The operating system, program code, and network scans generally found the AVS systems to be properly configured, to be free of high-risk vulnerabilities, and to have only a small number of medium- and low-risk vulnerabilities.

Except for the scanning, security controls executed through operational and managerial processes had not yet been tested at the time the updated ACA security authorization was signed and the AVS was placed into production. Cybersecurity staff told us that even though these AVS controls were not tested prior to the AVS being placed into production, they had previous experience with the operation of these controls in versions prior to ACA Release 5.0 and the AVS. Because the security assessment had not yet been completed, the security authorization package provided to the authorizing official did not include a Security Assessment Report or System Security Plan.

In addition, an audit plan had not been approved and implemented and an information system contingency plan had not been finalized at the time the updated ACA security authorization was signed and the AVS was placed into production. An audit plan specifies the resources, content, and methods for performing audit trail reviews for detecting inappropriate user and system actions that could be security incidents. The information system contingency plan is maintained for emergency response, backup operations, and post-disaster recovery for an information system. It ensures the availability of critical resources and facilitates the continuity of operations in the event of an emergency, system failure, or disaster. Internal Revenue Manual 10.8.1 requires systems to have an audit plan and an information system contingency plan. The ACA audit plan and information system contingency plan was completed in May 2015.

Lastly, ACA Release 5.0, including the AVS, was using Java Runtime Environment versions 5, 6, and 7, which had dozens of unremediated vulnerabilities at the time the updated ACA security authorization was signed and the AVS was placed into production. These vulnerabilities could allow unauthorized connections, untrusted applications to gain privileges, and remote attackers to bypass intended access restrictions. Failure to correct such flaws increases the risk of successful data compromise, execution of arbitrary code, and attacks to disrupt computer operations.

Cybersecurity officials stated that security testing needs to be performed on a final version of software and that the development of the final version of ACA Release 5.0 was completed too late for the Cybersecurity organization to complete the security assessment in time for the signing of the updated ACA security authorization.

Due to the security assessment and security authorization package being incomplete, the updated ACA Release 5.0 security authorization was signed and the AVS was placed into production without complete information on the risks of placing the system into production. When security testing is not completed, security vulnerabilities might exist that could result in additional risks not taken into consideration when the updated ACA security authorization was signed.

Recommendations

Recommendation 1: The Chief Technology Officer should ensure that all identified AVS security vulnerabilities are corrected prior to the 2016 Filing Season.

> ***Management's Response:*** The IRS partially agreed with this recommendation. In situations for which identified AVS security vulnerabilities cannot be corrected prior to the 2016 Filing Season, the IRS will continue to follow established processes within the IRS Security Policy and Cybersecurity's Enterprise Federal Information Security Management Act Plan of Action and Milestones Standard Operating Procedures. This includes initiating a plan of action and milestones for vulnerabilities identified through the AVS security activities with appropriate remediation dates determined by the nature and criticality of the vulnerability.

Recommendation 2: The Chief Technology Officer and authorizing officials should ensure that security testing and security authorization packages are completed prior to signing security authorizations and placing systems into production.

> ***Management's Response:*** The IRS partially agreed with this recommendation. The Cybersecurity organization will ensure that existing security policy is followed for system authorizations when possible. In those cases that they cannot be followed to the letter, the Cybersecurity organization will exercise risk-based decisionmaking, with appropriate governance approvals and documentation.

The Affordable Care Act Verification Service Testing Was Delayed and Inaccurate Test Data Were Included in the Draft End-of-Test Completion Reports

The System Test Plan is a requirement of Internal Revenue Manual 2.16.1, *Enterprise Life Cycle Guidance*. The System Test Plan defines the scope, approach, and required activities that will be used to effectively test and assess the quality of a system, including the criteria that must be met to begin and end a test. The *ACA 5.0 Consolidated Project Level System Test Plan, Version 1.1*, dated April 1, 2014, states that each sprint includes all previously tested code and new code. During each sprint, the AVS test team will execute test cases for the current build in parallel with regression test cases identified for the build. Before ending the project-level test, all defects must be resolved or appropriately dispositioned and all test cases must be dispositioned and documented. The ACA Program Management Office I&T organization's *ACA 5.0 Release Level Test Plan, Version 1.0*, dated August 21, 2014, specifically requires that prior to beginning Phase III of release-level testing, project-level testing must be completed and Severity 1 and 2 defects from project-level testing must be resolved. Any open defects must be disclosed and have a mitigation plan. Before ending the release-level test, all test cases must be completed or dispositioned, all Priority 1 (critical) defects must be closed, and open Priority 2 (high) and 3 (average) defects must be dispositioned, reviewed, and agreed to by the stakeholders. In addition, for the project-level and release-level tests, test results are required to be compiled and documented in the designated tool and in the EOTCR. The Government Accountability Office's *Standards for Internal Control in the Federal Government* states that activities should be completely and accurately recorded; for example, test results should be promptly and accurately recorded.[5]

The draft FIT Concept of Operations dated July 21, 2014, states that the FIT is a final preproduction test that occurs at the conclusion of either the IRS development and functional testing cycle or the modernization systems release integration testing and requires the FIT organization to conduct the FIT with versions or builds of production systems. Internal Revenue Manual 10.8.1 states that the security controls for all applications and systems must be tested prior to being placed into the production environment. The *IRS Event-Driven Security Controls Assessment Standard Operating Procedures Version 1.8*, dated February 14, 2013, states that the security assessment must be performed in a production-like environment.

Performance testing was completed before the start of the 2015 Filing Season

The *ACA 5.0 Consolidated Project Level System Test Plan, Version 1.1*, dated April 1, 2014, states that a performance test will be conducted by designated Information Technology organization delivery partners, which in this case is the Performance Engineering organization.

[5] Government Accountability Office, GAO-14-704G, *Standards for Internal Control in the Federal Government* (Sept. 2014).

The Performance Engineering organization completed the performance tests involving the AVS before January 20, 2015. The tests included end-to-end processing of simulated ACA peak workloads in the ACA performance test environment. The Performance Engineering organization determined that the test results demonstrated that the applications and infrastructure met the requirements for throughput and response times while the system was under the projected peak workload and that no performance issues were found during the execution of ACA Release 5.0 performance testing which would affect the release to production.

Delays in project-level testing delayed release-level testing

Project-level testing for the AVS was originally scheduled to be completed by June 23, 2014. The backlog of test cases and defects and the time needed to complete changes to the program code to correct the critical defects identified during project-level testing prolonged project-level testing and pushed project-level testing into release-level testing.

Delays in code delivery delayed testing. For example, by December 27, 2013, the I&T organization reallocated 76 test cases from Sprint 1, Sprint 2, and Sprint 3 to Sprint 4 for test execution because the design for the Coverage Data Repository to AVS interface was not finalized. The I&T organization expected a Sprint 7 build by midday June 16, 2014, to begin test execution. The development team experienced delays and the Sprint 7 build was delivered that night. By then, an upgrade to an application server had begun and was completed on June 17, 2014. As a result, the Sprint 7 build delivered on the night of June 16, 2014, was incompatible with the application server upgrade and the I&T organization could not use it for its tests. Subsequently, the development team revised and delivered a usable build by June 23, 2014. Had the build been available at midday on June 16, testing could have proceeded without being affected by the server upgrade. At the end of Sprint 7, testing was behind schedule due to the test backlog and late code delivery.

Defect corrections also delayed testing. A defect correction build scheduled for July 21, 2014, did not include all defects. Another build would be needed to address the remaining defects. In September 2014, the I&T organization reported that a significant number of defects identified inaccurate interim calculations that prevented the successful verification of subsequent calculations. This resulted in a significant number of test cases being blocked from execution and delays in test execution. Due to the number of outstanding defects and increased number of test cases that had not been executed, Sprint 8 was added to the schedule.

Late requirements and design delivery for a requirement related to complex exposure amount processing added over 50 test cases to the already outstanding inventory. There was an urgent need to quickly resolve the defects so that they could be retested. To assist in working through the outstanding test case inventory, the I&T organization realigned resources from the recently completed ACA Release 4.0 test effort, used additional contract personnel, and worked evenings and weekends.

To avoid further delays in starting the release-level test, management approved a request to end project-level testing on October 10, 2014, and to defer 35 test cases from the project-level test to the release-level test. The draft Project Level EOTCR stated that the results observed during the functional testing efforts for ACA Release 5.0 indicate that the system satisfies the approved business requirements except for those traced to the five unresolved defects identified in the EOTCR.

Delays in release-level testing extended the test period

Release-level test Phase III execution was originally scheduled from September 2, 2014, to November 26, 2014. As a result of extending the end date of the project-level test, Phase III testing began on October 21, 2014, over one month later than scheduled. Subsequently, the I&T organization faced delays and challenges over the course of the ACA Release 5.0 test effort. Status reports provided details of the delays encountered during release-level testing that involved the AVS. For example, in December 2014, delays occurred when an automated scheduling application used to support EPD data loads failed. Delays also occurred due to a deployment configuration issue that affected Generalized Mainline Framework to AVS connectivity. To mitigate the impact of these delays and implement the approved change requests, testers worked extended hours including weekends and testing was extended to January 16, 2015.

Test results from designated sources did not match the test results reported in the project-level and release-level draft EOTCRs

For the project-level test and the release-level test, the Requirements Traceability Verification Matrix (RTVM) is the designated tool for documenting requirements and test case status. We found that all the requirements in the RTVMs for both tests were linked to test cases and the test cases either passed or were waived or deferred. The defect tracking log is the designated tool for documenting defects identified during project-level testing, and the Knowledge Incident/Problem Service Asset Manager (KISAM) is the designated tool for documenting defects identified during release-level testing. We compared AVS test case results and defects from the designated sources to the information in the project-level and release-level draft EOTCRs and found the following discrepancies.

- Two test cases were listed in the project-level test RTVM but missing from the project-level test draft EOTCR, and one test case was listed in the project-level test draft EOTCR but missing from the project-level test RTVM. The I&T organization agreed that these were discrepancies and stated that the information for the draft EOTCR was from the I&T organization’s internal tracking system, which had not been updated with the correct information.

- The defect tracking log listed 127 defects identified by the I&T organization, but the project-level test draft EOTCR reported 121 defects. The I&T organization did not explain this discrepancy.
- Five test cases in the release-level test RTVM were missing from the release-level test draft EOTCR, and 14 test cases in the release-level test draft EOTCR were not included in the release-level test RTVM. The I&T organization agreed that these were discrepancies and plans to correct its documentation.
- Twelve defects in the release-level test KISAM log dated March 12, 2015, were missing from the May 8, 2015, release-level test KISAM log that was used to summarize the defects in the release-level test draft EOTCR. Eleven defects in the May 8, 2015, KISAM log were not listed on the March 12, 2015, KISAM log. Because both logs were obtained from the KISAM system after the release-level test was completed, both should have the same information. The I&T organization agreed that these were discrepancies and plans to correct its documentation.

In addition to correcting documentation, the I&T organization stated that it met with relevant staff to reiterate the established processes for producing RTVMs, EOTCRs, and defect management.

Testing delays were caused by late code deliveries, changes in the test environment (*e.g.*, the changes to the automated scheduling application used to support the EPD data loads and a configuration issue that affected connectivity between the Modernized e-File system to the AVS), and time needed to correct defects. Discrepancies identified in the EOTCRs were due to clerical errors and the use of the I&T organization's internal tracking system instead of only using the mandated tools (RTVM, defect tracking log, and KISAM).

Delays in the project-level and release-level tests for the AVS affected the security assessment and FIT. Cybersecurity did not receive a production-like AVS system in time to complete its testing for the security assessment prior to releasing the AVS into production on January 20, 2015. After acknowledging that the security assessment would not be completed before ACA Release 5.0 was deployed into production, the authorizing official approved an update to the current ACA authorization to operate to include ACA Release 5.0 changes because the IRS had an urgent need to deploy the AVS. When testing is not completed, unknown security vulnerabilities might exist that could result in additional risks not taken into consideration when the updated authorization to operate was signed.

ACA applications, including the AVS, were not sufficiently tested before delivery to the FIT environment. A recent Treasury Inspector General for Tax Administration audit[6] reported that the FIT program was not provided with a production build of the ACA 5.0 systems prior to the

[6] Treasury Inspector General for Tax Administration, Ref. No. 2015-20-034, *Final Integration Test Planning and Preparation* pp. 7 and 8 (May 2015).

start of FIT execution on November 3, 2014. At that time, there were Coverage Data Repository performance concerns that had not been resolved, and the release-level testing completion date for the AVS was delayed to December 17, 2014. As a result, the start of ACA testing was deferred until a more advanced build of the systems was delivered to the FIT environment. On November 23, 2014, the FIT program deployed the next build of the ACA Release 5.0 systems and began testing. After this second ACA Release 5.0 systems build was deployed, the FIT began experiencing connectivity issues with AVS, causing major delays in the FIT's test cases. Each subsequent ACA Release 5.0 build contained errors until the seventh and eighth builds were both deployed on January 15, 2015, near the end of test execution and approximately one week before the start of the 2015 Filing Season.

By January 20, 2015, the FIT program opened 33 critical helpdesk tickets after receiving ACA and Modernized e-File systems into the FIT environment. Of the 33 critical helpdesk tickets, 10 (30 percent) are related to the AVS. In addition, during the FIT, Systems Acceptability Tests continued to identify and correct problems with the systems that should have been corrected before delivery to the FIT environment. Systems Acceptability Tests identified critical-level problems with the AVS after the system was delivered for FIT execution and continued to create critical- and high-level helpdesk problem tickets throughout the duration of the FIT execution process step.

Delays in the AVS release-level testing delayed the identification and correction of errors prior to being deployed to the FIT environment, contributing to the numerous builds submitted for the FIT test execution. It also increased the risk that defects would not be corrected prior to production. For example, due to programming errors, the AVS incorrectly performed the math check on Form 8962, line 8b, *Monthly Contribution for Health Care*, of certain returns and incorrectly performed a data matching compliance check of EPD to some Forms 8962.

Management needs quality information to evaluate a system's performance in achieving key objectives and addressing risks. Not using the information from the systems designated to document test case and defect information increases the risk that the EOTCR may not completely and accurately reflect the test results that management needs to evaluate the system being tested.

Recommendations

Recommendation 3: The Chief Technology Officer should ensure that ACA developers are notified in advance when changes to the development, test, and production environments are made to ensure that the programs being developed are compatible with the updated environments.

> **Management's Response:** The IRS agreed with this recommendation. The IRS has instituted an ACA Environment Work Group that meets biweekly and communicates a variety of environment-related information, including when changes or updates are made.

Recommendation 4: The Chief Technology Officer should ensure that testing organizations use only the information from the designated tools for documenting requirements, test results, and defects to prepare the EOTCR.

> ***Management's Response:*** The IRS agreed with this recommendation. The testing organization will document this issue in lessons learned and will reiterate the processes/procedures for creating the EOTCRs with the analysts.

Appendix I

Detailed Objective, Scope, and Methodology

The overall objective of this review was to determine if the IRS adequately developed and tested the AVS. To accomplish our objective, we:

I. Reviewed ACA background, Tax Year 2014 Federal tax returns, and similar records to identify ACA provisions reported on Tax Year 2014 Federal tax returns.

II. Determined the risks to AVS availability for the 2015 Filing Season.

   A. Obtained and reviewed risk management Enterprise Life Cycle artifacts, risk reports, and similar records to identify the major risks (system development testing, security assessment, and system performance).

   B. Analyzed ACA/AVS Status Reports and related risk management documentation to determine the status of each of these risks.

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: ACA Program Management Office policies, procedures, and processes for developing and testing the AVS. We evaluated these controls by interviewing ACA Program Management Office, security, and testing management about AVS functions, risk management, development and testing activities, security testing, and defects management. We identified ACA tax provisions taking effect on Tax Year 2014 tax returns. We reviewed policies and procedures on system development, testing, security testing, and the IRS systems development life cycle.

Appendix II

Major Contributors to This Report

Alan R. Duncan, Assistant Inspector General for Audit (Security and Information Technology Services)
Danny Verneuille, Director
John Ledford, Audit Manager
Richard Borst, Lead Auditor
Chanda Stratton, Senior Auditor
Tina Wong, 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
Deputy Chief Information Officer for Operations OS:CTO
Director, Affordable Care Act Office SE:ACA
Associate Chief Information Officer, Applications Development OS:CTO:AD
Associate Chief Information Officer, Cybersecurity OS:CTO:C
Associate Chief Information Officer, Enterprise Program Management Office OS:CTO:EPMO
Associate Chief Information Officer, Enterprise Services OS:CTO:ES
Director, Core Application Systems ACA:OS:CTO:AD:CAS
Director, Security Risk Management OS:CTO:C:SRM
Director, Solution Engineering OS:CTO:ES:SE
Director, Office of Audit Coordination OS:PPAC:AC
Director, Office of Program Evaluation and Rick Analysis RAS:O
Chief Counsel CC
National Taxpayer Advocate TA
Office of Internal Control OS:CFO:CPOC:IC
Audit Liaison: Director, Risk Management Division OS:CTO:SP:RM

Appendix IV

Glossary of Terms

Term	Definition
Advance Payment of the Premium Tax Credit	The advance payment of the PTC paid to an insurance company on a monthly basis on the taxpayer's behalf.
Affordable Care Act	The comprehensive health care reform law enacted in March 2010 and subsequently amended. The law was enacted in two parts. The Patient Protection and Affordable Care Act[1] was signed into law on March 23, 2010, and was amended by the Health Care and Education Reconciliation Act on March 30, 2010. The ACA refers to the final amended version of the law.
Build	A version of a software program.
Coverage Data Repository	This database will support ACA provisions. It contains data imported from other IRS systems, other ACA systems, and the Department of Health and Human Services.
Cybersecurity Organization	The Cybersecurity organization, within the IRS Information Technology organization, is responsible for ensuring IRS compliance with Federal statutory, legislative, and regulatory requirements governing confidentiality, integrity, and availability of IRS electronic systems, services, and data.
Department of Health and Human Services	The U.S. Government's principal agency for protecting the health of all Americans and providing essential human services.
Disposition	A process to determine whether a test case or defect will be deferred or reassigned to a future test phase or waived because the associated requirement is removed or deleted.

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

Term	Definition
End-of-Test Completion Report	A required report that summarizes the complete test effort for the release.
End-to-End Testing	A methodology used to test whether the flow of an application is performing as designed from start to finish.
Enterprise Life Cycle	The Enterprise Life Cycle establishes a set of repeatable processes and a system of reviews, checkpoints, and milestones that reduces the risks of systems development and ensures alignment with the overall business strategy.
Exchange	A new, transparent, and competitive insurance exchange where individuals and small businesses can buy affordable and qualified health benefit plans. Exchanges will offer a choice of health plans that meet certain benefits and cost standards.
Exchange Periodic Data	The data the IRS receives each month from the Exchanges. The EPD flows are cumulative, meaning each submission will contain data for each month from January up to and including the current month being submitted.
Federal Exchange	An Exchange developed by the Federal Government to assist States that have chosen not to build their own individual State marketplace.
Filing Season	The period from January through mid-April when most individual income tax returns are filed.
Final Integration Test	A system test consisting of integrated end-to-end testing of mainline tax processing systems to verify that new releases of interrelated systems and hardware platforms can collectively support the IRS business functions allocated to them.
Generalized Mainline Framework	The Generalized Mainline Framework system validates and perfects data from a variety of input sources (*e.g.*, tax returns, remittances, information returns, and adjustments) and controls, validates, and corrects updated transactions. The AVS interacts with the Generalized Mainline Framework system to perform checks on paper tax returns.
Information Technology Organization	The IRS organization responsible for delivering information technology services and solutions that drives effective tax administration to ensure public confidence.

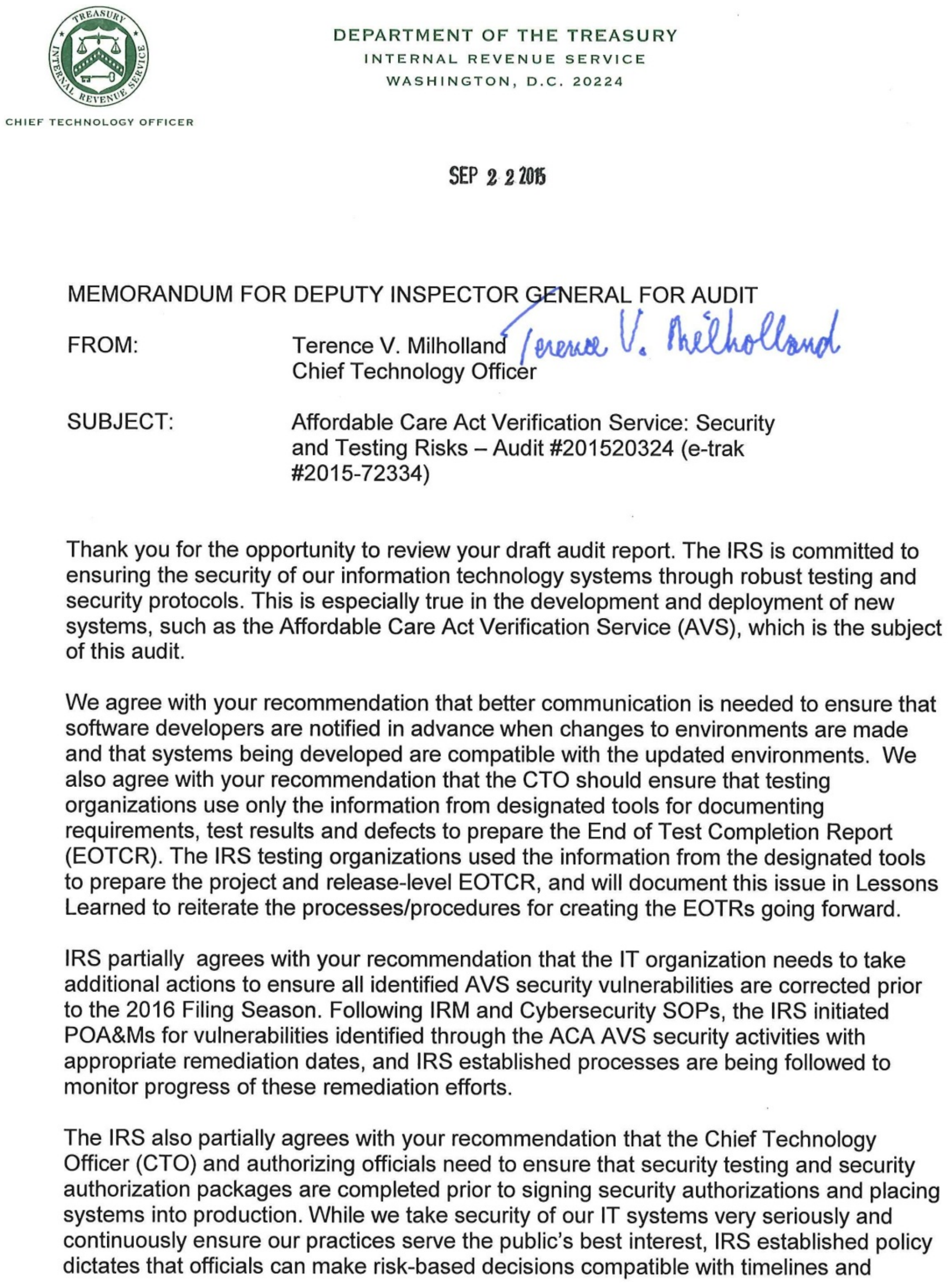
Term	Definition
Information Technology Organization ACA Program Management Office	The IRS office responsible for managing the strategic planning, development, implementation, and testing of new information systems in support of business requirements with regard to the ACA. It is within the Information Technology organization, which is a major organization under the Deputy Commissioner for Operations Support.
Integration Test	Integration testing is a software testing methodology used to test individual software components or units of code to verify interaction between various software components and detect interface defects. Components are tested as a single group or organized in an iterative manner. After the integration testing has been performed on the components, they are readily available for system testing.
Iterative Systems Development Path	An adaptive development approach in which projects start with initial planning and end with deployment, with repeated cycles of requirement discovery, development, and testing in between. It is a more flexible and adaptable process than traditional sequential development approaches.
Java Runtime Environment	Java is a newer programming language that is not natively supported by all operating systems. Therefore, Java Runtime Environment is needed for the Java application to run.
Knowledge Incident/Problem Service Asset Management System	An IRS application for reporting and managing problems with all applications developed by the IRS.
Mitigation Plan	A plan that documents how and when a condition, risk, issue, or action item will be resolved.
Modernized e-File	The IRS's electronic filing system that enables real-time processing of tax returns while improving error detection, standardizing business rules, and expediting acknowledgements to taxpayers. The system serves to streamline filing processes and reduce the costs associated with a paper-based process. The AVS interacts with Modernized e-File to perform checks on electronically filed tax returns.

Term	Definition
Monthly Contribution for Health Care	The monthly contribution is computed in Part I of Form 8962, *Premium Tax Credit*. It is the amount the taxpayers would be required to pay as a share of their monthly premium if they enrolled in the Second Lowest Cost Silver Plan. The amount is not related to the amount of premiums they are paying out of pocket. The monthly contribution amount is used as part of the calculations in Part II of Form 8962 to determine the amount of the monthly PTC.
National Institute of Standards and Technology	The Information Technology Laboratory at the National Institute of Standards and Technology develops management, administrative, technical, and physical standards and guidelines for the cost-effective security and privacy of "other than national security"-related information in Federal information systems. The Institute is part of the U.S. Department of Commerce.
Premium Tax Credit	A refundable tax credit to help taxpayers and families afford health insurance coverage purchased through an Exchange.
Regression Test	A regression test ensures that a change did not cause system degradation or introduce new defects.
Release	A specific edition of software.
Requirements Traceability Verification Matrix	A tool that documents requirements and establishes the traceable relationships between the requirements to be tested and their associated test cases and test results.
Risk	An uncertain event or condition that, if it occurs, has a negative effect on the project.
Second Lowest Cost Silver Plan	Plans in the Exchanges are primarily separated into four health plan categories (Bronze, Silver, Gold, or Platinum) based on the percentage the plan pays of the average overall cost of providing essential health benefits to members. The PTC is calculated using the Second Lowest Cost Silver Plan, regardless of what plan the taxpayer ultimately selects. Because there could be more than one plan in the Silver category, the premium of the Silver Plan that has the second lowest cost is used.
Services and Enforcement ACA Office	The Services and Enforcement ACA Office is a major office under the Deputy Commissioner for Services and Enforcement. It is responsible for implementing the tax provisions of the ACA.

Term	Definition
Severity Level	In project-level testing, defects are assigned a severity level and prioritized. There are five defect severity levels and they are: • ***Severity 1 – Show Stopper:*** Testing cannot continue unless the defect is fixed. • ***Severity 2 – No Work Around:*** A piece of major functionality is not working and there is no workaround for it. • ***Severity 3 – Work Around Available:*** The defect affects a major functionality, but there is an acceptable workaround if migrated to production. • ***Severity 4 – Minor/Cosmetic:*** Relates to items that are cosmetic in nature. For example, there might be typographical errors on the page. • ***Severity 5 – Documentation:*** Functionality is working as expected, but the documentation needs to be changed.
Sprint	A process that develops a piece of functionality of the system with repeated cycles of requirements discovery, planning, design, development, and testing. ACA projects conduct a series of sprints, either sequentially or even in parallel, within each release. The goal of each sprint is to get a subset of the project's functionality to a production-ready state.
State Exchange	An Exchange operated by the individual State.
System Integration Test	A system test conducted to verify that the system is integrated properly and functions as required.
System Test Plan	The plan is an Enterprise Life Cycle requirement. The purpose of the plan is to provide a standard artifact to summarize the complete test effort for the release. The plan gives the project an opportunity to mitigate risks that may cause delays to project implementation.
Tax Year	A 12-month accounting period for keeping records on income and expenses used as the basis for calculating the annual taxes due. For most individual taxpayers, the tax year is synonymous with the calendar year.
Test Case	The foundation of a test. A test case references specific test data and the expected results associated with specific program criteria. It is used to verify a specific process in the application software and to test system requirements.
Unit Test	Tests of a program module, object class, or other unit of the solution performed by the developer prior to integration to verify that the unit works correctly and satisfies its requirements.

Appendix V

Management's Response to the Draft Report



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

CHIEF TECHNOLOGY OFFICER

SEP 22 2015

MEMORANDUM FOR DEPUTY INSPECTOR GENERAL FOR AUDIT

FROM: Terence V. Milholland Terence V. Milholland
Chief Technology Officer

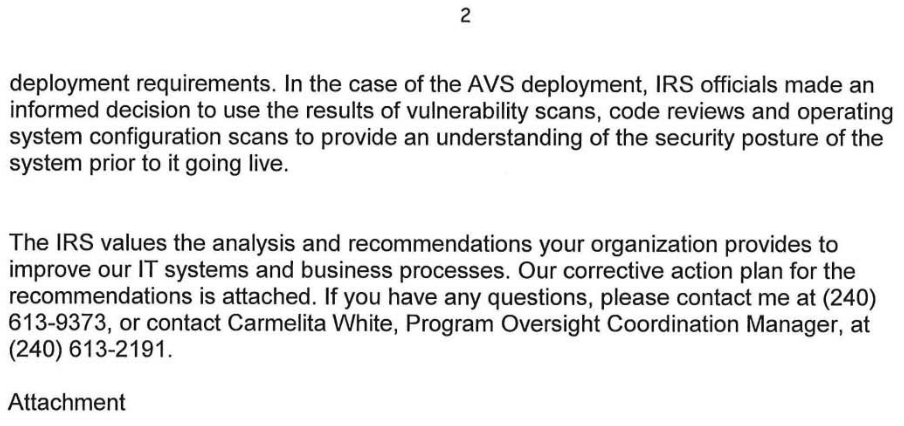
SUBJECT: Affordable Care Act Verification Service: Security and Testing Risks – Audit #201520324 (e-trak #2015-72334)

Thank you for the opportunity to review your draft audit report. The IRS is committed to ensuring the security of our information technology systems through robust testing and security protocols. This is especially true in the development and deployment of new systems, such as the Affordable Care Act Verification Service (AVS), which is the subject of this audit.

We agree with your recommendation that better communication is needed to ensure that software developers are notified in advance when changes to environments are made and that systems being developed are compatible with the updated environments. We also agree with your recommendation that the CTO should ensure that testing organizations use only the information from designated tools for documenting requirements, test results and defects to prepare the End of Test Completion Report (EOTCR). The IRS testing organizations used the information from the designated tools to prepare the project and release-level EOTCR, and will document this issue in Lessons Learned to reiterate the processes/procedures for creating the EOTRs going forward.

IRS partially agrees with your recommendation that the IT organization needs to take additional actions to ensure all identified AVS security vulnerabilities are corrected prior to the 2016 Filing Season. Following IRM and Cybersecurity SOPs, the IRS initiated POA&Ms for vulnerabilities identified through the ACA AVS security activities with appropriate remediation dates, and IRS established processes are being followed to monitor progress of these remediation efforts.

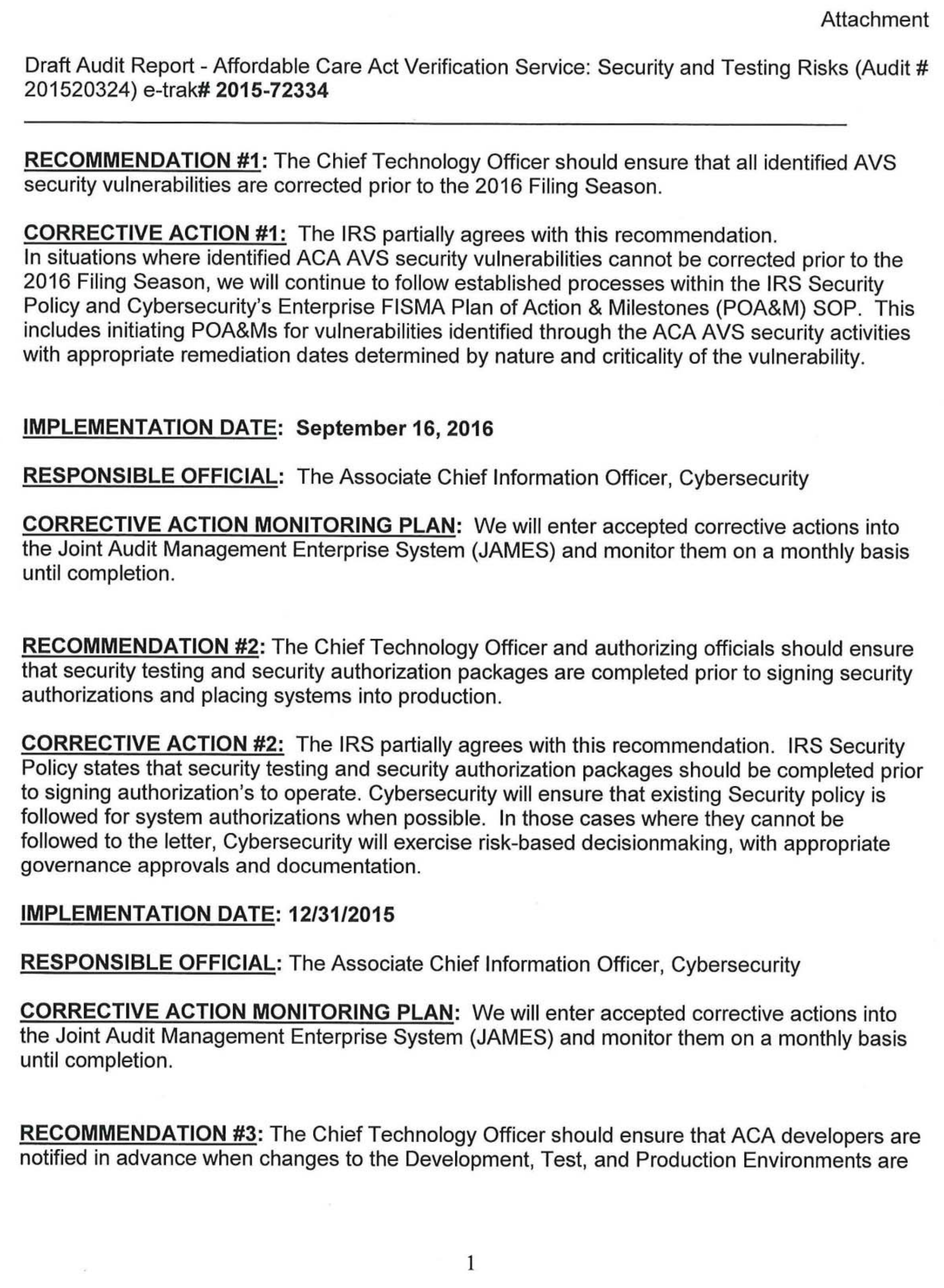
The IRS also partially agrees with your recommendation that the Chief Technology Officer (CTO) and authorizing officials need to ensure that security testing and security authorization packages are completed prior to signing security authorizations and placing systems into production. While we take security of our IT systems very seriously and continuously ensure our practices serve the public's best interest, IRS established policy dictates that officials can make risk-based decisions compatible with timelines and



deployment requirements. In the case of the AVS deployment, IRS officials made an informed decision to use the results of vulnerability scans, code reviews and operating system configuration scans to provide an understanding of the security posture of the system prior to it going live.

The IRS values the analysis and recommendations your organization provides to improve our IT systems and business processes. Our corrective action plan for the recommendations is attached. If you have any questions, please contact me at (240) 613-9373, or contact Carmelita White, Program Oversight Coordination Manager, at (240) 613-2191.

Attachment



Attachment

Draft Audit Report - Affordable Care Act Verification Service: Security and Testing Risks (Audit # 201520324) e-trak**# 2015-72334**

RECOMMENDATION #1: The Chief Technology Officer should ensure that all identified AVS security vulnerabilities are corrected prior to the 2016 Filing Season.

CORRECTIVE ACTION #1: The IRS partially agrees with this recommendation.
In situations where identified ACA AVS security vulnerabilities cannot be corrected prior to the 2016 Filing Season, we will continue to follow established processes within the IRS Security Policy and Cybersecurity's Enterprise FISMA Plan of Action & Milestones (POA&M) SOP. This includes initiating POA&Ms for vulnerabilities identified through the ACA AVS security activities with appropriate remediation dates determined by nature and criticality of the vulnerability.

IMPLEMENTATION DATE: September 16, 2016

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 and authorizing officials should ensure that security testing and security authorization packages are completed prior to signing security authorizations and placing systems into production.

CORRECTIVE ACTION #2: The IRS partially agrees with this recommendation. IRS Security Policy states that security testing and security authorization packages should be completed prior to signing authorization's to operate. Cybersecurity will ensure that existing Security policy is followed for system authorizations when possible. In those cases where they cannot be followed to the letter, Cybersecurity will exercise risk-based decisionmaking, with appropriate governance approvals and documentation.

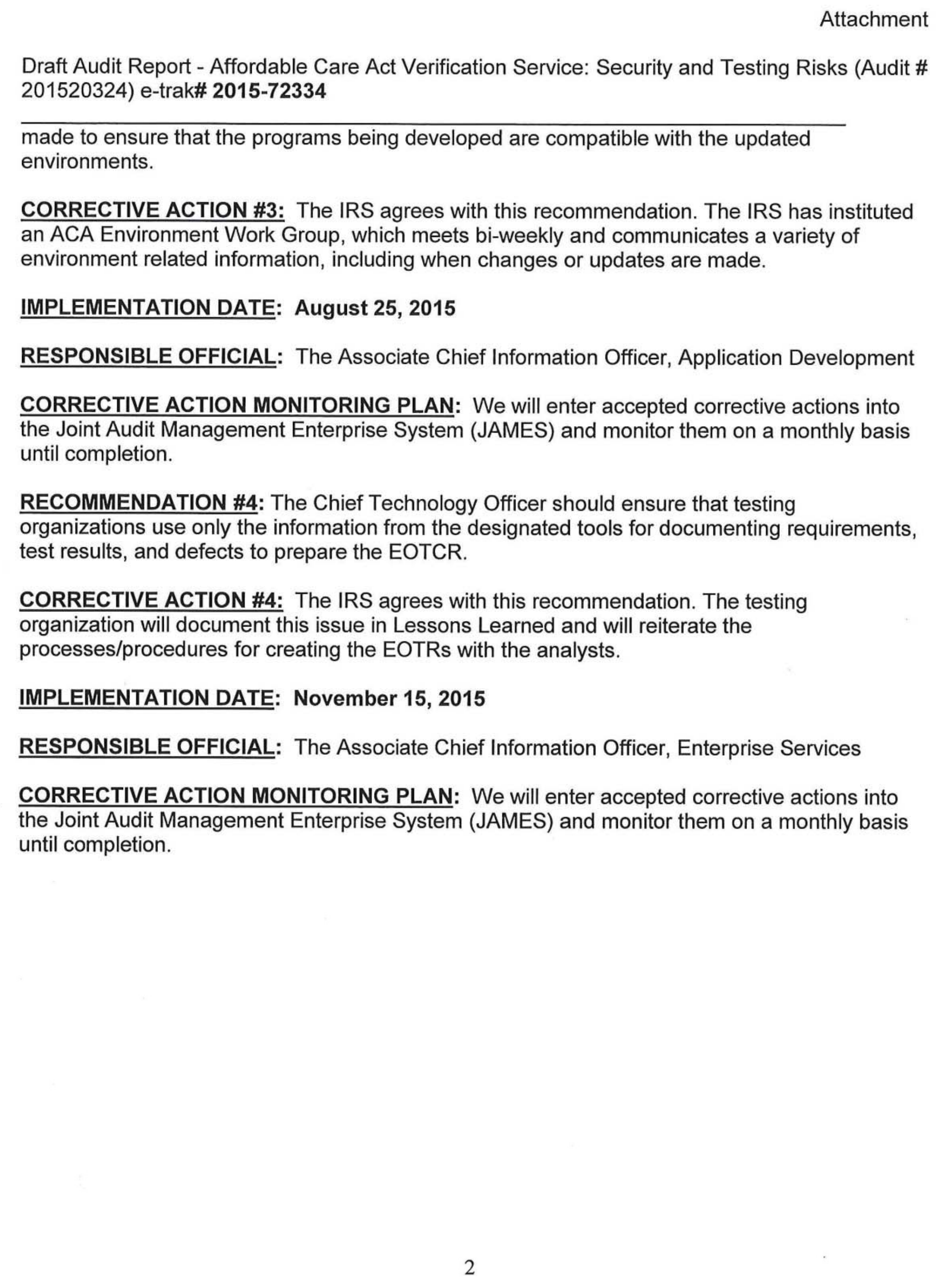
IMPLEMENTATION DATE: 12/31/2015

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 #3: The Chief Technology Officer should ensure that ACA developers are notified in advance when changes to the Development, Test, and Production Environments are

1



Attachment

Draft Audit Report - Affordable Care Act Verification Service: Security and Testing Risks (Audit # 201520324) e-trak# **2015-72334**

made to ensure that the programs being developed are compatible with the updated environments.

CORRECTIVE ACTION #3: The IRS agrees with this recommendation. The IRS has instituted an ACA Environment Work Group, which meets bi-weekly and communicates a variety of environment related information, including when changes or updates are made.

IMPLEMENTATION DATE: **August 25, 2015**

RESPONSIBLE OFFICIAL: The Associate Chief Information Officer, Application Development

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 that testing organizations use only the information from the designated tools for documenting requirements, test results, and defects to prepare the EOTCR.

CORRECTIVE ACTION #4: The IRS agrees with this recommendation. The testing organization will document this issue in Lessons Learned and will reiterate the processes/procedures for creating the EOTRs with the analysts.

IMPLEMENTATION DATE: **November 15, 2015**

RESPONSIBLE OFFICIAL: The Associate Chief Information Officer, Enterprise Services

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.