TREASURY INSPECTOR GENERAL FOR TAX ADMINISTRATION

Affordable Care Act Compliance Validation System: Security and Testing Risks

May 16, 2016

Reference Number: 2016-23-040

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

To report fraud, waste, or abuse, call our toll-free hotline at:

1-800-366-4484

By Web:

www.treasury.gov/tigta/

Or Write:

Treasury Inspector General for Tax Administration
P.O. Box 589
Ben Franklin Station
Washington, D.C. 20044-0589

Information you provide is confidential and you may remain anonymous.

AFFORDABLE CARE ACT COMPLIANCE VALIDATION SYSTEM: SECURITY AND TESTING RISKS

Highlights

Report issued on May 16, 2016

Highlights of Reference Number: 2016-23-040 to the Internal Revenue Service Chief Technology Officer and Director, Services and Enforcement Affordable Care Act Office.

IMPACT ON TAXPAYERS

Starting with 2014 individual income tax returns, the Affordable Care Act (ACA) requires taxpayers to report that they have qualifying health care coverage, are eligible for a health coverage exemption, or make a Shared Responsibility Payment. The ACA also created the Exchanges, *i.e.*, Federal and State, from which individuals can purchase health plans and, if eligible, obtain an advance payment of the Premium Tax Credit to help pay premiums. The IRS developed the ACA Compliance Validation System (ACV) to support post-filing compliance of the Premium Tax Credit and the Shared Responsibility Payment.

WHY TIGTA DID THE AUDIT

TIGTA initiated this audit to evaluate the IRS's responsibility in fulfilling certain ACA requirements for taxpayers receiving an advance payment of the Premium Tax Credit. The overall objective was to determine whether the IRS adequately developed and tested the ACV. Specifically, TIGTA evaluated policies, procedures, and processes for developing and testing the ACV that included functional requirements; changes; project and risk management; and performance, functional, and security testing.

WHAT TIGTA FOUND

The IRS successfully tested the functionality and security of the ACV prior to placing the system into production. In addition, the system was placed into production on September 10, 2015, prior to the mandatory due date of September 27, 2015.

The ACV project team followed system development procedures to identify functional requirements and design the first release of the ACV. By utilizing lessons learned from previous system development projects, the ACV project team was able to build the ACV and complete performance, integration, and release-level testing on schedule.

Following release-level testing, the IRS properly assessed the security of the ACV. The Cybersecurity organization provided all required documents and security testing results, including the identified security risks for the authorizing official to make an informed decision authorizing the system to operate.

While the security testing met all applicable requirements, TIGTA found examples of inaccurate security control descriptions in 29 (14.4 percent) of 201 controls in the ACA System Security Plan, a key security document. The errors TIGTA found did not cause any applicable security controls to be excluded from testing and did not affect the authorization decision to place the system into operation. During the audit, the Cybersecurity organization corrected the errors and updated the ACA System Security Plan.

WHAT TIGTA RECOMMENDED

TIGTA made no recommendations in this report. IRS officials reviewed the draft report and agreed with the facts presented.

TREASURY INSPECTOR GENERAL
FOR TAX ADMINISTRATION

DEPARTMENT OF THE TREASURY

WASHINGTON, D.C. 20220

May 16, 2016

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 Compliance Validation System: Security and Testing Risks (Audit # 201520318)

This report presents the results of our review of the Affordable Care Act Compliance Validation System. The overall objective of this review was to determine whether the Internal Revenue Service adequately developed and tested the Affordable Care Act[1] Compliance Validation System. This review is included in the Treasury Inspector General for Tax Administration's Fiscal Year 2016 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. If you have any questions, please contact 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 Internal Revenue Code and 42 U.S.C.), 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 Patient Protection and Affordable Care Act, infra)).

Table of Contents

Background ..... Page 1

Results of Review ..... Page 5

The Internal Revenue Service Properly Developed and Tested the Affordable Care Act Compliance Validation System ..... Page 5

The Internal Revenue Service Properly Assessed the Security of the Affordable Care Act Compliance Validation System ..... Page 9

Appendices

Appendix I – Detailed Objective, Scope, and Methodology ..... Page 12

Appendix II – Major Contributors to This Report ..... Page 14

Appendix III – Report Distribution List ..... Page 15

Appendix IV – Glossary of Terms ..... Page 16

Appendix V – Management's Response to the Draft Report ..... Page 20

Abbreviations

ACA	Affordable Care Act
ACV	ACA Compliance Validation System
FTR	Failure to Reconcile
IRS	Internal Revenue Service
IT	Information Technology
PTC	Premium Tax Credit
SRP	Shared Responsibility Payment
SSP	System Security Plan

Background

The Affordable Care Act (ACA)[1] 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, *i.e.*, Federal and State. 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. 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). The PTC is a refundable tax credit[2] created by the ACA to assist eligible taxpayers with paying their health insurance premiums.

The ACA also requires most legal residents of the United States to obtain health insurance. The ACA calls for the Internal Revenue Service (IRS) to implement and administer a large number of its provisions that will take effect over several years. Recognizing the critical role that information technology plays in executing the IRS's responsibilities under the ACA, the IRS created the ACA Program Management Office within the Information Technology (IT) 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. The ACA systems developed through these releases provided functionality to support the Exchange's eligibility and enrollment process, processing of PTC claims, and storing of Exchange data. Under ACA Release 6.1, the ACA Program Management Office developed Release 1.0 of the ACA Compliance Validation System (ACV) in support of post-filing compliance to perform the following:

- Identify individual returns that have failed to reconcile for receiving an advance payment of the PTC.
- Provide a calculation service to calculate the Shared Responsibility Payment (SRP).

[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 Internal Revenue Code and 42 U.S.C.), 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 Patient Protection and Affordable Care Act, infra)). Also, see Appendix IV for a glossary of terms.

[2] Refundable tax credits can be used to reduce a taxpayer's tax liability to zero. Any excess of the credit beyond the tax liability can be refunded to the taxpayer.

Validation of PTC reconciliation

Starting in January 2014, eligible taxpayers who purchased health insurance through an Exchange could qualify for an advance payment of the PTC to assist with paying their health insurance premium. An advance payment of the PTC is available to individuals and families not otherwise eligible for Minimum Essential Coverage whose incomes are at least 100 percent and up to 400 percent of the Federal poverty level. Beginning in January 2015, taxpayers who purchased insurance through an Exchange are required to include Form 8962, *Premium Tax Credit (PTC)*, with their tax return to claim the PTC and reconcile any advance payments of the PTC that were made to an insurer on their behalf. The PTC, excess advance payment of the PTC, or Net PTC is carried forward from Form 8962 to Form 1040, *U.S. Individual Income Tax Return*. If an advance payment of the PTC was received, Form 8962 and Form 1040 are required even if the taxpayer is not otherwise required to file a tax return.

One of the ACV's functionalities is to perform a check for individuals for whom advance payment of the PTC was paid on their behalf in the previous calendar year to determine whether they failed to reconcile. The initial ACV Failure to Reconcile (FTR) application analysis was designed to run prior to the open enrollment period for purchasing health care in November 2015 and then run monthly to analyze all policies with advance payment of the PTC that have not been reconciled for the calendar year under review. This analysis uses Exchange and taxpayer data collected by other ACA systems to determine whether the tax filer and tax filer spouse (as applicable) have not reconciled the advance payment of the PTC. The FTR analysis uses Exchange policy data with advance payment of the PTC paid for any month for the calendar tax year under review and each tax household with advance payment of the PTC paid within the policy.

After the system determines that an individual (tax filer and tax filer spouse, as applicable) has not reconciled one or more tax households within one or more policies, the individual (tax filer and tax filer spouse, as applicable) is assigned a FTR tag. The tag is associated with the tax filer's and tax filer spouse's (as applicable) Taxpayer Identification Numbers. The tag is applied and the data transferred by other ACA systems to the Department of Health and Human Services/Centers for Medicare and Medicaid Services. The Centers for Medicare and Medicaid Services has the responsibility to ensure advance payments of the PTC are made only for enrollees who paid their monthly premiums and reconciled the advanced payment of the PTC on their 1040 tax form.

SRP calculator

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 care coverage exemption, or make the SRP with their tax return. Taxpayers who had qualifying coverage for every month check a box on their tax return. Individual taxpayers must use Form 8965, *Health Coverage Exemptions*, to report a health care coverage exemption. Some health care coverage exemptions are available only from an

Exchange and others are available 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 and pay the SRP on their tax return.

The ACV's individual coverage compliance calculator provides examiners the ability to recalculate and store the individual's SRP. Examiners may need to use the calculator during an audit if the return includes a self-reported SRP. Examiners use the Accounts Management Services system to research, document, adjust, and resolve taxpayers' inquiries related to taxpayer accounts. The Accounts Management Services system obtains Exchange Periodic Data that provides the periods in which the taxpayer had insurance coverage or an exemption. Data entered into the individual coverage compliance calculator allows the ACV to process the calculation. The ACV performs the individual calculation, and the SRP data returns to the Accounts Management Services system for display to the examiner.

ACV system development

The ACA Program Management Office designed and developed the ACV using the enterprise life cycle iterative path. The iterative path of system development starts with conceptual requirements and uses repetitive progression through each of its phases to evolve the requirements. The iterative path uses a set of three milestones to pass through three development phases: project initiation, design and system development, and system deployment.

A milestone is a decision point in which management determines whether a project can proceed to the next phase. The two major milestones for iterative path system development are Milestone 2 and Milestone 4B. During project initiation, the ACV team defines the project scope, forms the project teams, and starts drafting many of the enterprise life cycle documents. The team has to receive approval of a solution concept, system requirements, and system architecture to complete Milestone 2 and advance to the next phase. Then in the design and system development phase, the ACV team develops a logical and physical design of the system, which involves coding, integration, testing, and certification of the system. Once the team has completed Milestone 4B requirements and receives the authorization to place the system into production, the project enters the system deployment phase. In this phase, the developers deploy the system into the production environment and begin to transfer support for the system to another IT organization.

Figure 1 identifies the iterative development and testing process tasks. Task 1 is conducted prior to Milestone 2, tasks 2-4 are repeated for each sprint in the release, and task 5 is conducted at the end of the last sprint in the release prior to Milestone 4B.

Figure 1: The Iterative Path Process Tasks

Tasks	Activity	Completed Prior To
1	Conduct Development and Test Preparation and Planning Activities.	Milestone 2
2	Conduct Sprint Preparation and Planning Activities.	Milestone 4B
3	Conduct Sprint Development and Testing Activities.	
4	Plan and Conduct End of Sprint Checkpoint Review Activities.	
5	Conduct Development and Testing Closeout Activities.	

Source: IRS Enterprise Life Cycle Iterative Development and Testing Process Description.

During system development, testers work side by side with developers to perform incremental requirement verification and validation of the system. During the design and system development phase, projects will run through a series of sprints, either sequentially or in parallel. The goal of each sprint is to develop a subset of the project's functionality to a "production-ready" state. This allows developers to take advantage of learning from the development and testing of earlier portions or versions of the system. The repeated sprints build upon the evolving versions until a solution or a portion of the solution is ready for deployment. At the end of each sprint, the functionality developed will be fully tested and verified through an end of sprint checkpoint review.

In addition to testing as part of the iterative path process, the ACV is included in testing performed by other IRS IT organizations. Once project-level testing is complete, integration, performance, release-level, and security testing is performed. The Enterprise Systems Testing organization works in partnership with the Implementation and Testing organization to plan, prepare, and conduct release-level testing, which connects the ACV to the ACA system for more in-depth testing.

This review was performed at the IRS IT organization's Applications Development office in Austin, Texas, and information was obtained from the IT organization offices of Enterprise Program Management, Cybersecurity, and ACA Program Management in Lanham, Maryland, during the period August 2015 through March 2016. 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 Internal Revenue Service Properly Developed and Tested the Affordable Care Act Compliance Validation System

Internal Revenue Manual 2.16.1, *Enterprise Life Cycle*, defines the iterative software development path as an adaptive development approach in which projects start with a conceptual vision of the solution and, through a series of repeated sprints of requirements discovery, development, and test, ends with deployment. The iterative path enables development of a system through repeated sprints and in small increments. Due to the flexible nature of the iterative path, it is important to have rigorous tracking of performance metrics to ensure that the project is on track and delivered on schedule. Iterative metrics may include velocity, *i.e.*, average amount of work to complete a sprint; defects per iteration, *i.e.*, defects found during testing done within the iteration; and burn down rate, *i.e.*, functionality backlog completed versus remaining in iteration. The development team usually tracks traditional metrics such as person-days or recorded defects.

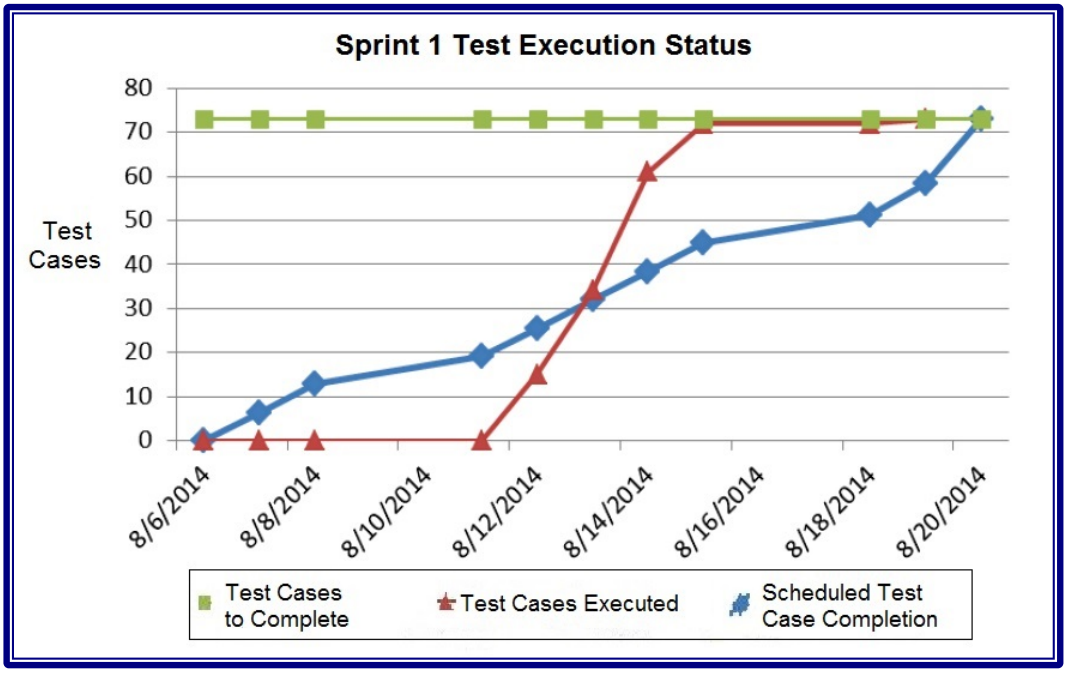
Projects using the iterative path should form integrated core teams consisting of business analysts, solution engineers, developers, testers, a dedicated process owner representative, and any other relevant functional or domain experts. Members of an integrated core team would join the team from the start of the project and contribute throughout the entire project. Iterative projects rely on the close involvement of business stakeholders to continuously provide feedback so that requirements can be clarified and the design can be improved continuously.

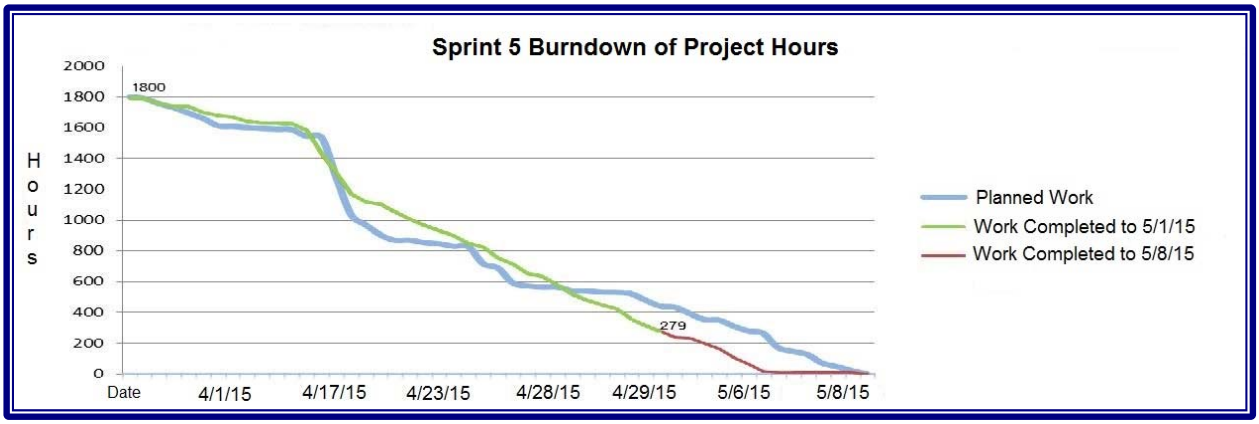
The ACV project team began the project initiation phase by coordinating efforts across the IRS IT organization to define the roles and responsibilities for the various phases of deployment. The project team also identified the system objectives, required capabilities, constraints, requirements, boundaries, and impacts to existing systems. The ACV project team properly completed all required systems development requirements and guidance documents prior to completing Milestone 2. These required documents include the project management plan, security package, business system report, and system deployment plan. The ACV project team properly completed its milestone exit review and proceeded to the design and development phase.

The project team began the system design and development phase by scheduling a series of sprints, which involve the coding, integration, and testing of the system. The project team appropriately conducted its sprints, even adjusting for late requirements that were added to the project. The project team monitored the ACV development progress and required system documentation through its end of sprint checkpoint reviews and weekly staff meetings. The project team kept rigorous tracking of performance metrics by capturing man-hours with burn

down rates for each sprint to ensure that the project was on track to be delivered timely. The project team also tracked test case status daily to ensure that each sprint was progressing on time. Figure 2 shows examples of the performance metrics that the ACV project team used during the sprints.

Figure 2: Tracking of Performance Metrics





Source: ACV 1.0 end of sprint checkpoint review presentations – Sprints 1 and 5.

The ACV project team tested Release 1.0 across eight sprints. The project-level system development testing occurred during Sprints 1 through 5, including Sprint 5B added to test new requirements. Sprints 6 and 7 were designed to test errors or issues found in external levels of testing, such as integration or performance testing. The ACV project team used these additional

two sprints to develop fixes for any defects found in external levels of testing. Adding these two additional sprints were an example of lessons learned from issues identified from a previous Treasury Inspector General for Tax Administration audit report[3] that found significant delays in testing prior to system deployment. Figure 3 shows the planned and actual sprint schedule for project-level testing of each sprint and any delays that occurred.

Figure 3: Schedule of ACV Development Sprints

Sprint	Planned Sprint Dates	Actual Sprint Dates	Variance Description
Sprint 1	06/06/2014 – 8/20/2014	06/06/2014 – 8/20/2014	
Sprint 2	08/25/2014 – 11/05/2014	08/28/2014 – 11/13/2014	Test execution delayed due to the implementation of a database architecture that required a change in test strategy and environment.
Sprint 3	11/14/2014 – 12/17/2014	11/14/2014 – 12/15/2014	
Sprint 4	12/26/2014 – 03/18/2015	12/19/2014 – 03/24/2015	Test execution delayed due to incomplete test environment setup related to deployment of database tables needed to complete the setup.
Sprint 5*	*03/24/2015 – 04/27/2015* 03/24/2015 – 05/08/2015	03/24/2015 – 05/08/2015	
Sprint 5B	01/28/2015 – 05/04/2015	01/28/2015 – 05/04/2015	
Sprint 6*	*05/05/2015 – 06/13/2015* 05/14/2015 – 06/12/2015	05/15/2015 – 06/12/2015	
Sprint 7*	*06/11/2015 – 07/14/2015* 06/18/2015 – 07/21/2015	06/16/2015 – 07/21/2015	

*Source: ACV 1.0 Project-Level End of Test Completion Report and various ACV status reports. *Planned dates adjusted due to an ACA Change Request.*

In one instance, the ACV project team had to adjust its sprint testing schedule due to a late change request to update the individual coverage compliance calculator's requirements to match an updated SRP worksheet. The new worksheet format, created by the Wage and Investment Division, included new fields that were not included in the original requirements. The ACV project team created an extra sprint, Sprint 5B, and adjusted the affected sprints' schedule to address this change. With the adjustments to its sprint schedule, the ACV project team properly used a requirements traceability verification matrix to track and ensure that all of its functional

[3] Treasury Inspector General for Tax Administration, Ref. No. 2015-23-081, *Affordable Care Act Verification Service: Security and Testing Risks* p. 19 (Sept. 2015).

business requirements were included in the system design. The ACV project team properly tested all functional business requirements as planned in its project-level testing.

Within each phase of development, the ACV project team properly conducted enterprise life cycle reviews and completed the required documentation, such as the business systems report, system deployment plan, and end of testing completion reports. The ACV project team properly completed all required documentation for Milestone 4B. The ACV project team provided system builds to external areas for testing, such as integration, performance, release-level, and security testing after completing the development sprints.

The developmental systems integration test tests all of the ACV's functional and nonfunctional requirements when connected to the other systems in ACA Release 6.1. The ACV project team completed the developmental systems integration testing for the ACV on July 10, 2015. The system received a recommendation to proceed to the next phase of testing because integration testing successfully completed all test cases.

The Performance Engineering organization was responsible for conducting performance tests for ACA Release 6.1, which included the ACV. Performance testing consisted of three categories of tests: Component Level Phase 1, Component Level Phase 2, and Release Level. Each performance test category included volume testing, which tested the system under expected volumes, and capacity testing, which pushed the system above the expected volumes to determine maximum capacity before system degradation. The expected volumes and workload mix were determined using the ACA performance engineering model and business systems report. The performance testing objectives were met with the conclusion that the ACV can process data at the expected service level agreement, and the Performance Engineering organization recommended that the release be deployed into production.

The Enterprise Systems Testing organization was responsible for designing and conducting release-level testing to validate business functionality between ACA Release 6.1 components and legacy IRS systems. Release-level testing verified that the ACV FTR functionality was able to perform the analysis to determine if individuals who previously received an advance payment of the PTC failed to reconcile through its utilization of multiple technologies. Release-level testing also verified that the individual coverage compliance calculator was able to provide Accounts Management Services function tax examiners access to the calculator, perform the individual SRP calculation analysis, and display the SRP calculation analysis results via web services. Release-level testing concluded on August 26, 2015, in accordance with the approved ACA 6.1 Release Level Test Plan. Based upon the results of testing, the system satisfied the approved business requirements.

The ACV was deployed into the production environment on September 10, 2015, prior to the mandatory date of September 27, 2015, to provide FTR data to the Department of Health and Human Services. Both the individual coverage compliance calculator and the FTR applications have been running as expected. The FTR application completed its first run in the production

environment on September 10, 2015. The FTR application was run again as scheduled in October 2015.

The Internal Revenue Service Properly Assessed the Security of the Affordable Care Act Compliance Validation System

Internal Revenue Manual 10.8.1, *Information Technology Security, Policy and Guidance*, requires a review of system security controls at regular intervals or when a change in the system will affect the security of the system. The Internal Revenue Manual also requires that the IRS use the security assessment and authorization process provided in the National Institute of Standards and Technology Special Publication (SP) 800-37 Revision 1, *Guide for Applying the Risk Management Framework to Federal Information Systems*. The purpose of the assessment is to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the established security requirements. A security controls assessment is designed to assess the impact of the change to the system by identifying threats, vulnerabilities, risks, and corrective actions and 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. A reauthorization required by a change in a system targets only the specific security controls affected by the changes. All security assessment and authorization tasks are completed prior to placing the information system into operation or continuing its operation.

The addition of the ACV to the ACA Release 6.1 is an example of a system change that required a security controls assessment. The IRS's Cybersecurity organization conducted and documented a security controls assessment to identify and document the security impact of adding the ACV to the ACA Release 6.1. The Cybersecurity organization performed the security assessment on the final production build of the ACV and conducted the assessment in compliance with the requirements of the Internal Revenue Manual and National Institute of Standards and Technology guidelines. Security assessment activities included testing a selection of information technology security controls, an ACV source code security review, and policy checker scans of the operating system on two ACV production servers.

The National Institute of Standards and Technology Special Publication 800-37 Revision 1 requires the authorizing official to use a security authorization package that includes comprehensive information on the security state of the information system. The System Security Plan (SSP) and security assessment report are key documents in the authorization package and are the basis for the authorization decision. The SSP provides an overview of the security requirements for the information system and describes the security controls in place or planned to meet those requirements. At the completion of the security assessment, the SSP is updated based on the findings of the security assessment and contains an accurate list and description of the security controls implemented and a list of residual vulnerabilities. The security assessment

report summarizes the risks associated with the vulnerabilities identified during the security assessment activities.

The assessment team correctly identified and selected the ACA security controls affected by the addition of the ACV. The team selected 11 of 201 security controls listed in the ACA Release 6.1 SSP for updated testing. The updated ACA SSP reflected the results of the security assessment, and the ACA security assessment report clearly described and reported all identified security risks.

While the security testing met all applicable requirements and the appropriate security controls were selected and tested, we found examples of incomplete and incorrect information for 29 (14.4 percent) of the 201 security controls in the ACA SSP. The SSP did not correctly describe the implementation status of the controls for the ACV component. Descriptions of the security controls in the ACA SSP were often generalized to cover many ACA components but were not "fine-tuned" when the controls were implemented differently for the ACV component. We found the following.

- For 15 controls, the ACA SSP stated, "the implementation status and documentation for this control is unique, and is therefore documented in the component SSPs." The controls were not in the ACV SSP Addendum. Cybersecurity organization management informed us that these controls were not "unique" for the ACV but were "unique" for other ACA components.
- For 11 controls, the ACA SSP stated, "the implementation status and documentation for this control is unique, and is therefore documented in the component SSPs." The controls were not included in the ACV SSP Addendum. Cybersecurity organization management informed us that they copied the wrong phrase into the ACA SSP. For these controls, the correct phrase is "the implementation status and documentation for this control is consistent for all components."
- For two controls, the ACA SSP stated, "the implementation status and documentation for this control is consistent for all components." However, Cybersecurity organization management stated the controls were not applicable to the ACV, but were "consistent" for other ACA components.
- For one control, the ACA SSP stated, "the implementation status and documentation for this control is consistent for all components" and listed several ACA components for which the control was not applicable, none of which was the ACV. Cybersecurity organization management informed us that the control was also not applicable to the ACV, but they overlooked adding the ACV to the list.

The IRS acknowledged the errors we identified in the control descriptions in the ACA SSP. During the audit, the IRS issued a revised ACA SSP, dated November 16, 2015, with corrections to all errors we identified. The errors we found in the control descriptions in the ACA SSP did not cause any applicable security controls to be excluded from testing. The errors and

corrections would not have altered the authorizing official's decision to place the system into operation.

The Cybersecurity organization provided the authorizing official for the ACA with all required documents and security assessment results to make an informed authorization decision. As a result, the authorizing official granted the system an Authorization to Operate on September 9, 2015, with complete information about the security risks, and the IRS placed the system into production on September 10, 2015. We verified that the system owner added all ACV security weaknesses to the ACA Plan of Action and Milestones for monitoring.

The IRS properly assessed, documented, and reported the impact of the ACV on the security of the ACA system because the IRS implemented and followed a disciplined and structured process that integrated information security and risk management activities into the systems development life cycle.

Appendix I

Detailed Objective, Scope, and Methodology

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

I. Obtained and reviewed systems development requirements and guidance.

- A. Obtained and reviewed requirements and standards for systems development using the iterative path.
- B. Obtained and reviewed system testing requirements, such as Internal Revenue Manuals and Enterprise Life Cycle guidance.
- C. Obtained and analyzed the requirements and ACV Release 1.0 project planning documentation, covering areas such as requirement management plans, risk management plans, and testing plans.

II. Determined the adequacy of the ACV Release 1.0 testing.

- A. Obtained ACA and ACV planning documentation to determine all functional business requirements of ACV Release 1.0.
- B. Reviewed the project design specification report and determined if functional business requirements were designed into Release 1.0.
- C. Reviewed ACV Release 1.0 sprint testing results.
- D. Reviewed interagency test results and error and defect logs to determine if requirements were tested, failed tests were properly resolved, and key controls were not deferred or waived.

III. Determined if security testing was performed and if security control vulnerabilities were corrected prior to the ACV Release 1.0 receiving a security authorization to operate and being placed into production.

- A. Obtained and reviewed Internal Revenue Manual and National Institute of Standards and Technology security testing requirements that must be met prior to a system receiving a security authorization to operate and being placed into production.
- B. Obtained and reviewed the ACA Release 6.1 Cybersecurity organization concurrence memorandum, the security authorization memorandum signed by the system owner, and Cybersecurity organization testing reports.

C. Used the security testing requirements and testing reports to determine if the Cybersecurity organization security assessment was properly completed and if major security control vulnerabilities were corrected prior to ACV Release 1.0 receiving a security authorization and being placed into production.

D. Reviewed security testing results to determine if vulnerabilities existed with audit trail security controls at the time ACV Release 1.0 received a security authorization and was placed into production.

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, and IRS IT organization security policies and guidance for developing and testing the ACV. We evaluated these controls by interviewing ACA Program Management Office security and testing management about ACV functions, risk management, development and testing activities, security testing, and defects management. We reviewed policies and procedures on system development, testing, security testing, and the IRS systems development life cycle. We also interviewed IRS Cybersecurity organization management, and reviewed the security controls assessment and system authorization requirements.

Appendix II

Major Contributors to This Report

Danny Verneuille, Acting Assistant Inspector General for Audit (Security and Information Technology Services)
Myron Gulley, Acting Director
John Ledford, Audit Manager
Louis Lee, Acting Audit Manager
Kasey Koontz, Lead Auditor
Joan Bonomi, Senior Auditor
Richard Borst, Senior Auditor

Appendix III

Report Distribution List

Commissioner
Office of the Commissioner – Attn: Chief of Staff
Deputy Commissioner for Operations Support
Deputy Commissioner for Services and Enforcement
Deputy Chief Information Officer for Operations
Associate Chief Information Officer, Applications Development
Associate Chief Information Officer, Cybersecurity
Director, Affordable Care Act
Director, Core Application Systems
Director, Office of Audit Coordination

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.
Centers for Medicare and Medicaid Services	The division of the Department of Health and Human Services responsible for oversight of the Medicare program, the Federal portion of the Medicaid program and State Children's Health Insurance Program, the Health Insurance Marketplace, and related quality assurance activities.
Cybersecurity Organization	The Cybersecurity organization, within the IRS IT 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.

[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.
Enterprise Life Cycle	The Enterprise Life Cycle establishes a set of repeatable processes and a system of reviews, checkpoints, and milestones that reduce the risks of system development, and ensures alignment with the overall business strategy.
Exchange	A Federal or State operated insurance exchange in which individuals and small businesses can buy affordable, competitive, 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. Exchange Periodic Data flows are cumulative, meaning each submission will contain data for each month from January up to and including the current month being submitted.
Failure to Reconcile	The process to identify individuals who received an advance payment of the PTC during the coverage year and assign a tag to those individuals who have not reconciled.
Federal Poverty Level	A measure of income level issued annually by the Department of Health and Human Services. Federal poverty levels are used to determine eligibility for certain programs and benefits. Guidelines are published and updated periodically in the Federal Register by the Department of Health and Human Services. The advance payment of PTC will be available for individuals and families whose incomes are at least 100 percent and up to 400 percent of the Federal poverty level who do not have minimum essential coverage.
Information Technology Organization	The IRS organization responsible for delivering information technology services and solutions that drive effective tax administration to ensure public confidence.

Term	Definition
Information Technology Organization Affordable Care Act 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 IT organization, which is a major organization under the Deputy Commissioner for Operations Support.
Integration Test	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 Path	An adaptive development approach in which projects start with initial planning and end with deployment, with repeated cycles of requirements discovery, development, and testing in between. It is a more flexible and adaptable process than traditional sequential development approaches.
Policy Checker	Validates the operating system security configuration of computers to IRS policy.
Premium Tax Credit	A refundable tax credit to help taxpayers and families afford health insurance coverage purchased through an Exchange.
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.

Term	Definition
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.
System Integration Test	A system test conducted to verify that the system is integrated properly and functions as required.
Taxpayer Identification Number	A nine-digit number assigned to taxpayers for identification purposes. Depending upon the nature of the taxpayer, the Taxpayer Identification Number is either an Employer Identification Number, a Social Security Number, or an Individual Taxpayer Identification Number.
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.