Affordable Care Act: Improvements Are Needed to Strengthen Systems Development Controls for the Premium Tax Credit Project

September 27, 2013

Reference Number: 2013-23-119

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

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

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

AFFORDABLE CARE ACT: IMPROVEMENTS ARE NEEDED TO STRENGTHEN SYSTEMS DEVELOPMENT CONTROLS FOR THE PREMIUM TAX CREDIT PROJECT

Highlights

Final Report issued on September 27, 2013

Highlights of Reference Number: 2013-23-119 to the Internal Revenue Service Chief Technology Officer.

IMPACT ON TAXPAYERS

In March 2010, the President signed into law the Health Care and Education Reconciliation Act of 2010 and the Patient Protection and Affordable Care Act (ACA) (collectively referred to as the ACA). The ACA law seeks to provide more Americans with access to affordable health care. The Premium Tax Credit (PTC) Project falls under the IRS ACA Program. Beginning January 2014, eligible taxpayers who purchase health insurance through an Exchange may qualify for and request a refundable tax credit (the PTC) to assist with paying their health insurance premium. The credit is claimed on the taxpayer's Federal tax return at the end of each coverage year. Because it is a refundable credit, taxpayers who have little or no income tax liability can still benefit. The PTC can also be paid in advance to a taxpayer's health insurance provider to help cover the cost of premiums. This credit is referred to as the Advanced Premium Tax Credit (APTC).

WHY TIGTA DID THE AUDIT

The overall objective of this review was to determine if the IRS is adequately managing systems development risks for the PTC Project. TIGTA evaluated the IRS's key management controls and processes for risk management, requirements and change management, testing, security, and fraud detection for the PTC Project, which is being developed in the IRS's new Enterprise Life Cycle Iterative Path.

WHAT TIGTA FOUND

The IRS has completed development and testing for the PTC Computation Engine (PTC-CE) needed to calculate the APTC and the Remainder Benchmark Household Contribution. In addition, the IRS developed a process to verify the accuracy of the PTC-CE calculations. However, improvements are needed to ensure the long-term success of the PTC Project by adherence to systems development controls for: (1) configuration and change management; (2) interagency test management process; (3) security; and (4) fraud detection and mitigation, in accordance with applicable guidance.

WHAT TIGTA RECOMMENDED

TIGTA made seven recommendations to the IRS Chief Technology Officer. In management's response to the report, the IRS agreed with six of the recommendations and plans to implement corrective actions.

However, the IRS disagreed with one of our recommendations to ensure that the Cybersecurity organization resolves or develops an action plan for the failed security tests. TIGTA maintains that this recommendation should be addressed to verify that corrective measures for failed controls have been implemented.

TREASURY INSPECTOR GENERAL
FOR TAX ADMINISTRATION

DEPARTMENT OF THE TREASURY
WASHINGTON, D.C. 20220

September 27, 2013

MEMORANDUM FOR CHIEF TECHNOLOGY OFFICER

FROM: Michael E. McKenney
Acting Deputy Inspector General for Audit

SUBJECT: Final Audit Report – Affordable Care Act: Improvements Are Needed to Strengthen Systems Development Controls for the Premium Tax Credit Project (Audit # 201320312)

This report presents the results of our review of how the Premium Tax Credit (PTC) Project managed controls over systems development of the Premium Tax Credit Computation Engine. The overall objective of this review was to determine if the Internal Revenue Service (IRS) is adequately managing systems development risks for the PTC Project. Specifically, we evaluated the IRS's key management controls and processes over risk management, requirements and change management, testing, security, and fraud detection while the PTC Project followed the Enterprise Life Cycle Iterative Path systems development and testing process. This audit is included in the Treasury Inspector General for Tax Administration Fiscal Year 2013 Annual Audit Plan and addresses the following major management and performance challenges confronting the IRS: (1) Implementing the Affordable Care Act and Other Tax Law Changes and (2) Security for Taxpayer Data and Employees.

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

Copies of this report are also being sent to the IRS managers affected by the report recommendations. If you have questions, please contact me or Alan Duncan, Assistant Inspector General for Audit (Security and Information Technology Services).

Table of Contents

Abbreviations

ACA	Affordable Care Act
APTC	Advanced Premium Tax Credit
CE	Computation Engine
CMS	Centers for Medicare and Medicaid Services
CR	Change Request
FPL	Federal Poverty Level
HHS	Department of Health and Human Services
IRM	Internal Revenue Manual
IRS	Internal Revenue Service
IT	Information Technology
JBOSS	JavaBeans Open Source Software
PMO	Program Management Office
PTC	Premium Tax Credit
RBHC	Remainder Benchmark Household Contribution
RRP	Return Review Program
RTVM	Requirements Traceability Verification Matrix
TIGTA	Treasury Inspector General for Tax Administration

Background

In March 2010, Congress passed two pieces of legislation that the President later signed into law—the Health Care and Education Reconciliation Act of 2010 and the Patient Protection and Affordable Care Act (ACA).[1] Collectively, this legislation is referred to as the ACA. The ACA legislation seeks to provide more Americans with access to affordable health care by creating a new Health Insurance Marketplace, enforcing patient/consumer protections, and providing Government subsidies for people who cannot afford insurance. The Marketplace simplifies an applicant's search for health coverage by providing multiple options in one place and comparing plans based on price, benefits, quality, and other important features that help consumers make a choice. The Health Insurance Marketplace is commonly referred to as "Exchanges," which is the terminology we will use in this report.

The ACA legislation seeks to provide more Americans with access to affordable health care.

In order to enroll in health insurance coverage offered through an Exchange, taxpayers must complete an application and meet certain eligibility requirements defined by the ACA. For example, they must be U.S. citizens or legal immigrants. Exchanges offer insurance plans by private companies, and taxpayers can access qualified health plan information online, via a call center, or in person. The qualified health plans cover the same core set of benefits called "essential health benefits," and no plan can turn an applicant away or charge more because of a preexisting illness or medical condition. The Exchanges are intended to provide a place for Americans to shop for health insurance in a competitive environment.

The ACA requires that enrollment for the Exchanges begin on October 1, 2013, and that the Exchanges become operational and offer health coverage starting on January 1, 2014. Beginning January 2014, eligible taxpayers who purchase health insurance through an Exchange may qualify for and request a refundable tax credit[2] to assist with paying their health insurance premium. The credit is called the Premium Tax Credit (PTC) and is claimed on the taxpayer's

[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. See Appendix V for a glossary of terms.

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

Federal tax return at the end of each coverage year.[3] Because the PTC is a refundable credit, taxpayers who have little or no income tax liability can still benefit.[4]

The PTC can also be paid in advance to a taxpayer's health insurance provider to help cover the cost of premiums. This credit is referred to as the Advanced Premium Tax Credit (APTC). The APTC will be available for individuals and families without minimal essential coverage, whose incomes are at least 100 percent and up to 400 percent of the Federal Poverty Level (FPL). The APTC is paid monthly on behalf of the taxpayer to the health insurance provider to offset the costs of the premiums. Payments will be issued by the Federal Management Services branch of the Department of the Treasury. Starting in January 2015, taxpayers must include the amount of any APTC on their tax return and reconcile it to the allowable amount of PTC.

The Internal Revenue Service's (IRS) role with respect to the ACA is to implement and administer the ACA provisions that have an impact on tax administration. The IRS's implementation plan for ACA Exchange provisions includes providing information that will support the Department of Health and Human Services (HHS) and the Exchanges in three main areas: (1) eligibility and enrollment; (2) developing calculations for the maximum APTC; and (3) reconciling PTCs with reported taxable income. While the HHS is leading development efforts for ACA policy provisions, the legislation requires the IRS to build new computer applications, modify existing systems, create or revise business processes and fraud detection systems, and deploy and test new interagency communication portals to support ACA operations.

Recognizing the integral role that information technology plays in executing the IRS's portion of the ACA legislation, the IRS created the ACA Information Technology (IT) Program Management Office (ACA PMO) to ensure a dedicated focus on fulfilling ACA requirements. Within the ACA PMO are various project offices that focus on specific areas of ACA development. The PTC Project includes all PTC processes related to the development of the PTC Computation Engine (PTC-CE), and the IT Implementation and Testing organization verifies that the requirements and design for all PTC systems have been adequately tested and correctly implemented. The ACA PMO has segmented implementation of the ACA into various releases. ACA Release 3.0 (ACA 3.0) focuses on the Eligibility and Enrollment process area.

The IRS's overall objective for the PTC Project as part of ACA 3.0 is to receive requests from Exchanges, calculate maximum monthly APTCs and Remainder Benchmark Household Contributions (RBHC), and return the responses to the Exchanges via the HHS Hub. Within the PTC Project, the PTC-CE will calculate the maximum amount of APTC that a recipient is allowed in advance of tax filing and the resulting RBHC.

The IRS's calculation of the maximum allowable amount of the APTC is initiated with a request from an Exchange to the IRS PTC-CE. In the request, the Exchange passes four inputs to the

[3] The period that the taxpayer received coverage from a qualified health plan.
[4] A refundable credit can be claimed even if the taxpayer does not owe any tax during the coverage year.

IRS's PTC-CE: (1) household income; (2) coverage year; (3) income as a percentage of the FPL; and (4) the adjusted premium for the applicable Second Lowest Cost Silver Plan. The Exchange receives two outputs from the IRS PTC-CE: (1) the maximum monthly APTC and (2) the RBHC. Appendix IV provides a partial process diagram for ACA 3.0, including the maximum APTC calculation process.

The scope of our audit was limited to reviewing the PTC Project under ACA 3.0 activities. We conducted our review to determine if the IRS is adequately managing systems development risks for the PTC Project, which is considered a major component of the ACA Program. This review was performed at the ACA PMO in Lanham, Maryland, during the period November 2012 through July 2013. 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 IRS has completed development and testing for the PTC-CE, which is needed to calculate the APTC and the RBHC. To complete this project, the IRS also developed and implemented a process for verifying the accuracy of the PTC-CE calculations. However, improvements are needed to ensure the long-term success for the PTC Project by adherence to systems development controls for: (1) configuration and change management; (2) interagency test management process; (3) security; and (4) fraud detection and mitigation in accordance with applicable guidance.

The Internal Revenue Service Has Completed Development and Testing for the Premium Tax Credit Computation Engine Needed for the Advanced Premium Tax Credit

The IRS has completed functional development and testing of the PTC-CE, which will calculate the maximum APTC and the RBHC. This was accomplished by applying the IRS's new Iterative Systems Development Life Cycle through a requirements discovery, planning, design, development, and testing process known as "sprints." The IT Implementation and Testing organization conducted a PTC system test over three sprints to verify (1) the calculation of the maximum APTC and (2) the calculation of the RBHC. The IT Implementation and Testing organization's Consolidated Project-Level End-of-Test Completion Report, dated January 7, 2013, states that, "the results observed during the functional and regression testing efforts as well as during checkpoint reviews with business owners for PTC indicate the system satisfies the approved business requirements."

The Internal Revenue Service Developed a Process to Verify the Accuracy of the Premium Tax Credit Computation Engine Calculations

On April 15, 2013, the IRS provided an Excel spreadsheet that it used to manually calculate the PTC-CE outputs (Manual Calculator). The IRS compared the outputs from the Manual Calculator to the actual system results to validate the PTC-CE outputs. At the time of our review, based on a judgmental sample of eight test cases, we were able to replicate the IRS's process for validating that the PTC-CE accurately calculated the maximum APTC and RBHC

amounts.[5] To select the eight test cases, we judgmentally sampled four PTC requirements out of a total of 35. We selected these four requirements because they are the requirements that directly relate to the PTC-CE. Then, out of a total of 527 test cases related to the four requirements, we judgmentally sampled two functional test cases for each of the requirements, for a total of eight test cases. All eight test cases contained the four PTC-CE input values as required to properly calculate the maximum APTC and the RBHC. We ran the test case input values through the Manual Calculator and documented the maximum APTC and RBHC results. We then compared the manual results to the actual system results and they matched.

Overall Management's Response: The Chief Technology Officer stated in his written management response to the draft report, "I was pleased to read your observation acknowledging that our PTC-CE accurately calculated the maximum APTC."

Office of Audit Comment: We have one point of clarification related to the above statement. Our audit focused on systems development controls and testing processes developed by the IRS. Our review did not verify operational accuracy of the PTC-CE beyond the test environment that we considered. Specifically, during this review, the audit team replicated the IRS's verification process in a judgmental sample of eight test cases. Our sample considered specific test cases that included requirements and conditions being tested by the IRS during the time frame of our review. However, the audit scope did not include all functional test cases planned or completed by the IRS with the development of the PTC-CE. Further, verification of results for a judgmental sample of test cases is a nonstatistical sample and the results cannot be applied to the overall testing or system development processes.

Configuration and Change Management Controls Need Improvement to Ensure Long-Term Success for the Premium Tax Credit Project

Configuration management controls were not consistently followed

The purpose of configuration management controls is to establish and maintain the integrity of work products, including testing documentation, throughout their life cycle.[6] Configuration management controls are also needed to ensure that changes are authorized, controlled, and tracked for project documentation, hardware, and software. It is important that the IRS creates test cases to specify and document whether systems requirements and conditions are tested to validate that each system functions as intended.[7] Documentation for each test case should

[5] Our audit did not consider the completeness of IRS's total population of functional test cases related to the PTC-CE. A judgmental sample is a nonstatistical sample, the results of which cannot be used to project to the population.
[6] The *ACA Program Configuration Management Plan*, in accordance with Internal Revenue Manual (IRM) 2.27.1, *Configuration Management* (Jan. 2010), establishes configuration management policies, processes, and procedures.
[7] IRM 2.6.1, *Product Assurance, Test, Assurance, and Documentation Standards and Procedures* (Nov. 2010).

include the requirements being tested to help ensure that each requirement is included in a test case and properly tested.

In order for the IRS to calculate the maximum APTC amounts that it will provide to the Exchanges, a computation will be performed by the IRS based on four inputs, including the applicant's income as a percentage of the FPL. The FPL input value is one of the four inputs that determine the maximum APTC amount that an applicant can receive when applying for a tax credit under the ACA legislation.

Configuration management controls were not followed with two test cases for the software code related to the FPL percentage requirement. IT Implementation and Testing organization management informed us that our audit prompted them to discover that the original Test Case 128 and its run history were inadvertently overwritten when updates were made to the test case after it was not properly controlled in the IT Implementation and Testing organization's test case repository. As a result, Test Case 128 and its run history were lost. Test Case 128 was later re-executed after updates were made to test the FPL software code change. Management also discovered that Test Case 130 was initially developed and executed with an outdated input data file, which necessitated that the test case be re-executed.

Based on our observation, we believe that if this control weakness had not been addressed prior to the implementation of the PTC-CE, the IRS would have tested this critical system requirement using incorrect input data. Further, this approach could have resulted in the PTC-CE incorrectly calculating the maximum APTC for applicants. This condition in turn could result in improper tax payments. Moreover, if test case documentation is not adequately controlled during systems development, the IRS may not have sufficient assurance that all mission-critical APTC requirements are adequately tested and that the PTC-CE system functions as intended.

Management Action: The IT Implementation and Testing organization stated that it is taking both short-term and long-term management action by identifying process improvements to make. For example, in the short term, it will change how input data files and test cases are stored in its repository and will add a date to the test case file names to help avoid overwriting a previously executed test case. It will also enhance testing peer reviews to (1) verify that the current input data file is stored in the main folder and that test cases include the current input data file and (2) check the run history of the test cases to ensure that they have not been overwritten. In the long term, it will use a test case tool for test case management that will provide version control over the test cases.

Change management controls need improvement

The IRS requires that a change request (CR) be prepared and approved to change baseline requirements.[8] According to the ACA Program Requirements Plan, requirements changes start with the initiation of a CR, which is the medium for requesting approval to change a baselined requirement. Once a CR is developed, it should be reviewed and dispositioned[9] by the appropriate Change Control Board.[10] Test cases are created to specify and document the conditions to be tested and to validate that a system functions as intended.[11] The test case should include the requirement(s) being tested to ensure that each requirement is included in a test case and properly tested to ensure that the system functions as intended. The Requirements Traceability Verification Matrix (RTVM) is an important management tool that the IRS relies on to ensure that all PTC requirements are included in test cases and adequately tested.

There were a total of 10 PTC CRs. Of these, we identified two CRs (PTC CR06 and PTC CR07) that modified requirements to the PTC-CE software code.[12] Details for these requirements are provided in Figure 1.

Figure 1: Details Regarding CRs PTC CR06 and PTC CR07

PTC CR #	Changed Requirement Number	Changed Requirement Name	Changed Requirement Description
2 **2**	***2***	********2******** *********2*****	**********2********** **********2********** **********2********.
2 **2**	***2***	********2******** *********2***** *********2*****	**********2********** **********2********** **********2********.
2 **2**	***2***	********2********	**********2********** **********2********** **********2********** **********2********** **********2**********

Source: CR numbers PTC CR06 and PTC CR07.

[8] The *ACA Program Configuration Management Plan*, in accordance with IRM 2.27.1 (Jan. 2010), requires that a CR be prepared and approved to change baseline requirements.
[9] According to the *ACA PMO Configuration Management Plan*, dispositioned is defined as to approve, conditionally approve, defer, disapprove, elevate, or remand a CR by the appropriate Change Control Board.
[10] A CR is reviewed and first dispositioned by the PTC Project Change Control Board. If the change exceeds the disposition approval authority for the Project Change Control Board, then the change will be reviewed and dispositioned by the ACA PMO Change Control Board.
[11] IRM 2.6.1, *Product Assurance, Test, Assurance, and Documentation Standards and Procedures* (Nov. 2010).
[12] The FPL value is one of the four inputs for calculating the maximum APTC amount.

Although the PTC Project Team prepared PTC CR06 and PTC CR07 for these two changed baselined requirements, these specific CRs did not include the affected requirement numbers or descriptions, which would have facilitated the traceability of requirements and test cases to the RTVM. PTC Project management explained that these CRs did not include the affected requirement numbers or descriptions because the CR template and the Change Request Tracking System do not include requirement number and description fields.

We believe that it is important to include the affected requirements in the CRs to ensure adequate traceability of requirements and test cases to the RTVM. This is particularly important to ensure that requirements are included in test cases and adequately tested. Without traceability from CRs, to requirements, and then to the RTVM, the IRS may not have the ability to verify that the changes to the software code were successfully tested. As a result, the PTC-CE could possibly calculate the maximum APTC incorrectly, which could potentially result in inaccurate maximum APTC amounts for individual applicants. This condition in turn could result in improper tax payments. Further, the IRS may not have complete assurance that all mission-critical APTC requirements are adequately tested to ensure that the ACA system functions as intended.

Management Action 2: Based on our discussions of this finding with the IRS, the PTC Project management team agreed to take immediate action by updating PTC CR06 and PTC CR07 to include the affected requirement numbers and to facilitate traceability from the CRs to the requirements and then to the RTVM.

Recommendations

Recommendation 1: The Chief Technology Officer should ensure that testing peer review guidance and other applicable guidelines are updated and that a test case management tool is used to ensure that APTC test case input data files, test cases, and test case run histories are properly controlled.

> ***Management's Response:*** The IRS agreed with this recommendation. The IRS stated that the ACA Strategic Test Management Plan and supporting procedures will be updated to reflect additional testing peer review guidance and other applicable guidelines to ensure that APTC test case input data files, test cases, and test case run histories are properly controlled.

Recommendation 2: The Chief Technology Officer should ensure that CR templates, tools, and applicable change management guidelines are updated to ensure that CRs include the affected requirement numbers and requirement descriptions for adequate traceability of requirements and test cases to the RTVM.

> ***Management's Response:*** The IRS agreed with this recommendation. The IRS stated that the PTC Project team has taken intermediate action to update the PTC Change Management Request template. They also will update their change management

guidelines and templates to ensure that CRs include the affected requirement numbers and descriptions for adequate traceability of requirements and test cases to the RTVM.

Interagency Test Management Process Controls Need Improvement to Ensure Long-Term Success of the Premium Tax Credit Project

Interagency test cases were not developed in accordance with test management procedures

The IRS conducted interagency testing to verify integration, interface, performance, and reliability requirements for major design components of the system. Interagency testing should include validating data formats and transmission, validating software and hardware interoperability, and using manufactured data to invoke user-like work streams in a simulated production environment. Staff in each agency is responsible for repairing defects in their respective systems and keeping the systems operational.

The interagency test cases that we analyzed contained user scenarios that were jointly developed by the Centers for Medicare and Medicaid Services (CMS) and the IRS. The test cases we considered were developed to validate the critical business processes for inbound requests from the CMS and outbound responses from the IRS. For example, a test case could require the submission of a single PTC request from the CMS Federal Exchange, ensure that the correct results are generated on the IRS systems, and verify those results are correctly returned and presented at the CMS Federal Exchange.

We observed that the IT Implementation and Testing organization personnel did not consistently follow appropriate test management procedures. Internal Revenue Manual (IRM) 2.6.1 requires that test cases be developed to support requirements testing. Test cases must specify and document the conditions to be tested and validate that system functions meet customer requirements as translated into a documented functional design. Test cases should also include the requirements being tested to ensure that each requirement is properly tested. During our review, the IRS stated that test cases are mapped to requirements in the requirements traceability matrix to ensure traceability. However, we reviewed five interagency test cases provided by the IT Implementation and Testing organization and found that they did not contain all key requirements that must be tested to verify system capabilities.

The IT Implementation and Testing organization staff explained that testing with another Federal agency, including the HHS, involves new processes, so everyone is learning as the work progresses with ACA systems development. Further, they explained that missing requirements were not included in the test cases because of an IRS decision to restrict certain data during the test case development process from the CMS.

However, if requirement numbers and descriptions are not included in test cases, traceability between requirements, test cases, and test results may not be accurate or complete. Based on our

review, we concluded that the IRS has not applied established systems development controls to verify that the HHS Hub and the IRS portal for ACA effectively transfer data[13] as needed by the IRS for calculating the maximum APTC.

Recommendation

Recommendation 3: The Chief Technology Officer should update test management procedures to include additional controls and processes to document how traceability between requirements, test cases, and test results will be achieved for interagency testing.

> ***Management's Response:*** The IRS agreed with this recommendation. The IRS stated that the ACA Strategic Test Management plan will be updated to formally document how traceability between requirements, test cases, and test results are achieved for testing with external entities.

Security Control Processes Need Improvement to Ensure Long-Term Success of the Premium Tax Credit Project

The IT Cybersecurity organization has contracted for security-related services, including ACA system testing support. The contract recognizes that the ACA impacts the IRS and the HHS, along with other Federal and State agencies. It also recognizes that there are new processes, functions, and information technology capabilities required at both the management and technical levels, including the implementation of complex technical and business changes in parallel work streams. The ACA system testing support provided through this contract reflects an IRS decision that contractor resources and expertise are needed to implement these capabilities and to manage the design, development, testing, deployment, integration, and maintenance of the associated systems.

Failed security controls identified by security control assessment testing require corrective actions prior to system implementation

The ACA System Security Plan identified 12 security controls that were only partially implemented during the APTC testing process that we reviewed. As a result, during the Security Control Assessment, some critical ACA infrastructure components included in the 12 security controls failed because they did not contain the appropriate baseline configurations and mandatory configuration settings as required by the National Institute of Standards and Technology and IRM guidelines. **********2**********
**********2**********
**********2**********
*********2****

[13] The HHS Hub is connected to IRS systems through the IRS's Transactional Portal Environment.

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

Many of the vulnerabilities in information systems can be traced to software flaws and misconfigurations of system components. During our observations of security testing for the PTC Project, IT Cybersecurity organization management ensured that the tests were conducted in accordance with the National Institute of Standards and Technology and IRM guidelines. However, the configuration baselines and configuration settings for the security controls were not adequately tested as discussed previously. We requested additional information on the corrective actions for the failed test controls. However, IT Cybersecurity organization management could not provide documentation to verify the corrective measures during our audit fieldwork. As a result, we are concerned that known risks associated with component misconfigurations might not have been mitigated for the PTC Project.

Change management guidelines were not consistently followed when baseline security requirements were withdrawn from the PTC Project

The ACA Program Configuration Management Plan, in accordance with IRM guidelines, also requires that a CR be prepared and approved to change baseline requirements. According to the ACA Program Requirements Plan, requirement changes start with the initiation of a CR and a change impact assessment to determine the potential impact of changed baselined requirements prior to approving and implementing the CR. Once a CR is developed, it should be reviewed and dispositioned by the appropriate Change Control Board.

During our review, we observed instances where change management guidelines were not followed to withdraw approved baseline security requirements from the PTC Project. For instance, the CR and impact assessment prepared to withdraw specific security requirements included only one of the seven baseline requirements removed from the PTC Project.

This specific CR removed the following security requirement from the PTC Project:

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

The security manager stated that this requirement was removed because the PTC Project does not have any application-level end users and that logical access to the application is provided by the infrastructure.

However, the CR did not include the following six security requirements that were withdrawn from the PTC Project:

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

During our review, IT Cybersecurity organization management stated that they did not have access to the Change Request Tracking System tool because the tool was maintained at the ACA Program level. Without this access, IT Cybersecurity organization staff explained that they were unable to ensure that the CRs were approved and processed. Due to this lack of transparency for the PTC change management process, IT Cybersecurity organization staff was unaware of when final changes to the baseline security requirements were implemented. As a result, the IRS may be unable to determine the potential impact of changed requirements on the security controls for the PTC-CE, which could negatively impact functionality and delay successful deployment of the PTC Project.

Recommendations

Recommendation 4: The Chief Technology Officer should ensure that the IT Cybersecurity organization resolves or develops an action plan with specific corrective actions and time periods for the failed security tests as part of the ACA Security Assessment and Authorization.

> ***Management's Response:*** The IRS disagreed with this recommendation. The IRS stated that it already does this process and it has documented policies in place in its IRM that address this recommendation, and that IRM 10.8.1.3.5.1 requires weaknesses identified during the Security Assessment and Authorization to be documented in a Plan of Actions and Milestones to include planned, implemented, and evaluated remedial actions to correct any deficiencies.
>
> ***Office of Audit Comment:*** We acknowledge that the IRS has a process in place to resolve or develop an action plan with specific corrective actions and time periods for failed security tests as part of the ACA Security Assessment and Authorization. However, we discussed this finding and recommendation with the PTC Project team and IT Cybersecurity organization officials during our audit closing conference. In the written management response to the draft report, the IRS did not address the audit conditions and finding that prompted our recommendation. TIGTA maintains that this recommendation should be addressed because during audit fieldwork, IT Cybersecurity organization officials could not provide documentation to verify the corrective measures for the failed test controls. By addressing this recommendation, the IRS could better ensure that known risks associated with component misconfigurations are consistently addressed for the PTC Project during the ACA Security Assessment and Authorization process. Moreover, TIGTA maintains that this recommendation requires that, going forward, the IT Cybersecurity organization follow its process to resolve or develop an action plan with specific corrective actions and time periods for the failed security tests that we reviewed as part of the ACA Security Assessment and Authorization. Such a resolution or an action plan with the corrective actions is needed to ensure that the IRS is addressing the vulnerabilities in information systems that can be traced to software flaws and misconfigurations of system components for the PTC Project and across other information technology projects being developed by the ACA Program.

Recommendation 5: The Chief Technology Officer should ensure that CRs and impact assessments are accurately prepared and processed as required by change management guidelines.

> ***Management's Response:*** The IRS agreed with this recommendation. The IRS stated that steps have been taken to provide IT Cybersecurity organization staff with access to the Change Request Tracking System so they are aware when final changes to the baseline security requirements have been implemented.

A Fraud Mitigation Strategy Is Not in Place to Guide Affordable Care Act Systems Development, Testing, Initial Deployment, and Long-Term Operations

The IRS's current IRMs do not address management's responsibility for managing, monitoring, and mitigating fraud risk with the development of new information technology systems for the ACA. Further, the ACA Program has not yet completed a fraud mitigation strategy to guide ongoing systems development. It is important for the IRS to thoroughly consider fraud threats and risks that could impact new ACA systems. For example, tax fraud is often defined as an intentional wrongdoing on the part of a taxpayer, with the specific purpose of evading a tax known or believed to be owed. Tax fraud requires both a tax due and owing and fraudulent intent. The Improper Payment Information Act of 2002[14] requires Federal agencies, including the IRS, to estimate and reduce the amount of improper payments made each year. Robust fraud mitigation controls and new systems are required to reduce improper and erroneous payments and fraud risk.

IRM 25.1.1, *Fraud Handbook, Overview/Definitions*, provides an overview of fraud, defines the elements of fraud, and is a comprehensive guide for IRS employees in the recognition and development of potential fraud issues. IRM 25.1.2, *Recognizing and Developing Fraud*, provides direction to IRS employees on how to recognize the signs of fraud and the development process used to prove fraud. However, neither of these IRMs addresses management's responsibility for developing new systems to combat fraud risks.

A pre-decisional briefing document prepared by the ACA PMO in response to our audit outlined the IRS's ongoing fraud mitigation approach for its new ACA systems and applications. However, the ACA program management team acknowledged that this approach is not part of an established fraud mitigation strategy for ACA systems. Such a strategy is needed to guide systems development including fraud controls for new ACA systems.

During this audit, the IRS also informed us that two new systems, the Return Review Program (RRP)[15] System and the ACA Validation Service System, are under development and will address ACA tax refund fraud risk. However, until these new systems are successfully developed and tested, TIGTA remains concerned that the IRS's existing fraud detection system[16]

[14] Pub. L. No. 107-300, 116 Stat. 2350.
[15] The RRP is the key automated component of the IRS's pre-refund initiative and will implement the IRS's new business model for a coordinated criminal and civil tax noncompliance approach to prevent, detect, and resolve tax refund fraud.
[16] The IRS's current fraud detection system is the Electronic Fraud Detection System.

may not be capable of identifying ACA refund fraud or schemes prior to the issuance of tax return refunds. Further, our recent audit[17] of the RRP system reported the following:

- Roles for program-level governance were not yet established for the RRP and the key role of system integrator was not documented or clearly communicated.
- RRP Prototype Management Plans and critical systems development products were not completed or approved by major stakeholders before significant resources were committed to prototyping activities.
- Uncertainty about the systems development path for the RRP and the absence of Enterprise Life Cycle guidance for prototypes hindered initial systems development efforts.
- Alternative commercial software products were not fully considered prior to selecting technology solutions for the RRP system.
- The IRS reported that the long-term limitations of its existing fraud detection system include its inability to keep pace with increasing levels of fraud and to serve the organization's evolving compliance needs.

Without a fraud detection and mitigation strategy, the ACA Program may not have assurances that ACA systems adequately address emerging fraud control requirements. Further, without adequate fraud mitigation controls, the IRS may be unable to identify ACA refund fraud or schemes prior to the issuance of erroneous refunds.

Recommendations

Recommendation 6: The Chief Technology Officer should ensure that the IRM is updated to provide specific guidance on how IRS management is to effectively manage, monitor, and mitigate fraud risk for information technology systems.

> ***Management's Response:*** The IRS agreed with this recommendation. The IRS stated that the appropriate IRM sections will be updated to ensure that fraud risk is considered in developing requirements and systems capabilities as part of every legislative implementation project.

Recommendation 7: The Chief Technology Officer should ensure that the ACA Program completes a comprehensive fraud mitigation strategy to guide ACA systems development, testing, and implementation.

[17] TIGTA, Ref. No. 2013-20-063, *Improvements Are Needed to Ensure Successful Development and System Integration for the Return Review Program* (Jul. 2013).

Management's Response: The IRS agreed with this recommendation and stated that it will be implemented for every ACA release. The IRS stated that in the development of ACA 3.0, which is scheduled to go live in October 2013, they have already determined there is no tax fraud risk with the APTC calculator or the Income and Family Size Verification process.

Appendix I

Detailed Objective, Scope, and Methodology

Our overall objective was to determine if the IRS is adequately managing systems development risks for the PTC[1] Project under the ACA Program. To accomplish our objective, we:

I. Determined whether the PTC Project has established key systems development, management and control processes over risk management, requirements and change management, and testing while following the Enterprise Life Cycle Iterative Path process.

- A. Determined whether PTC Project risks were properly identified, monitored, and mitigated in accordance with applicable guidance.
- B. Determined whether risks were being adequately managed regarding requirements and change management in accordance with applicable guidance.
- C. Determined whether risks have been adequately managed regarding the PTC Project system testing activities in accordance with applicable guidance.
  1. Determined the accuracy of the PTC-CE. We judgmentally sampled[2] four PTC requirements from a total of 35. We selected these four requirements because they are the requirements that directly relate to the PTC-CE. We then selected two functional test cases for each of the four requirements, for a total of eight test cases.
  2. Reviewed the adequacy of the Interagency Testing for the PTC Project.

II. Determined whether security controls for the PTC Project were designed and properly tested to protect taxpayer data in accordance with applicable guidance.

III. Determined whether fraud detection controls were designed into the PTC system in accordance with applicable guidance.

- A. Interviewed PTC Project personnel about fraud detection controls for the PTC Project. We obtained and reviewed supporting documentation.
- B. Determined the PTC Project's strategy for building fraud detection controls into the PTC system.

[1] See Appendix V for a glossary of terms.
[2] A judgmental sample is a nonstatistical sample, the results of which cannot be used to project to the population.

Internal controls methodology

Internal controls relate to management's plans, methods, and procedures used to meet their mission, goals, and objectives. Internal controls include the processes and procedures for planning, organizing, directing, and controlling program operations. They include the systems for measuring, reporting, and monitoring program performance. We determined the following internal controls were relevant to our audit objective: IRM and related IRS guidelines and the processes followed in the development of information technology projects using the Iterative Path as they apply to the ACA Program's PTC Project.

We evaluated these controls by conducting interviews with management and staff, making observations of system development and testing activities, and reviewing relevant documentation. Documents reviewed include the PTC Project Management Plan, the ACA Program Configuration Management Plan, and other documents that provided evidence of whether the IRS is adequately managing systems development risks for the PTC Project.

Appendix II

Major Contributors to This Report

Alan Duncan, Assistant Inspector General for Audit (Security and Information Technology Services)
Gwendolyn McGowan, Director, Systems Modernization and Applications Development
Suzanne Westcott, Audit Manager, Systems Modernization and Applications Development
Kevin Liu, Audit Manager, Technical Assistance Group
David Allen, Lead Auditor
Andrea Barnes, Senior Auditor
Wallace Sims, Senior Auditor
Allen Henry, Program Analyst
Linda Nethery, Information Technology Specialist
Nicholas Reyes, Information Technology Specialist

Appendix III

Report Distribution List

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

Appendix IV

Partial Process Diagram for Affordable Care Act 3.0, Including the Maximum Advanced Premium Tax Credit Calculation Process

The following figures provide a partial process diagram for ACA 3.0, including the maximum APTC calculation process.

TIGTA developed this diagram based on our review and analysis of various documents provided by the IRS, and IRS and HHS comments on a draft version of this diagram. Specifically, this includes the following documents:

- IRS ACA Release 3 End-to-End Overview (dated January 6, 2013).
- ACA orientation for TIGTA (February 7, 2013).
- ACA Program, Baseline Requirements, Solution Architecture, and IT Roadmap, Version 2.2 (March 23, 2012).
- ACA Release 3.0 System Security Plan (dated April 15, 2013).
- IRS comments on a draft version of this diagram (dated June 19, 2013; June 20, 2013; June 21, 2013; and July 9, 2013).
- HHS comments on a draft version of this diagram (dated July 2, 2013).

Additional acronyms shown in this diagram but not used elsewhere in the report include the following:

AGI = Adjusted Gross Income.

DHS = Department of Homeland Security.

FMS = Financial Management Service (a bureau of the Department of the Treasury).

ID = Identification.

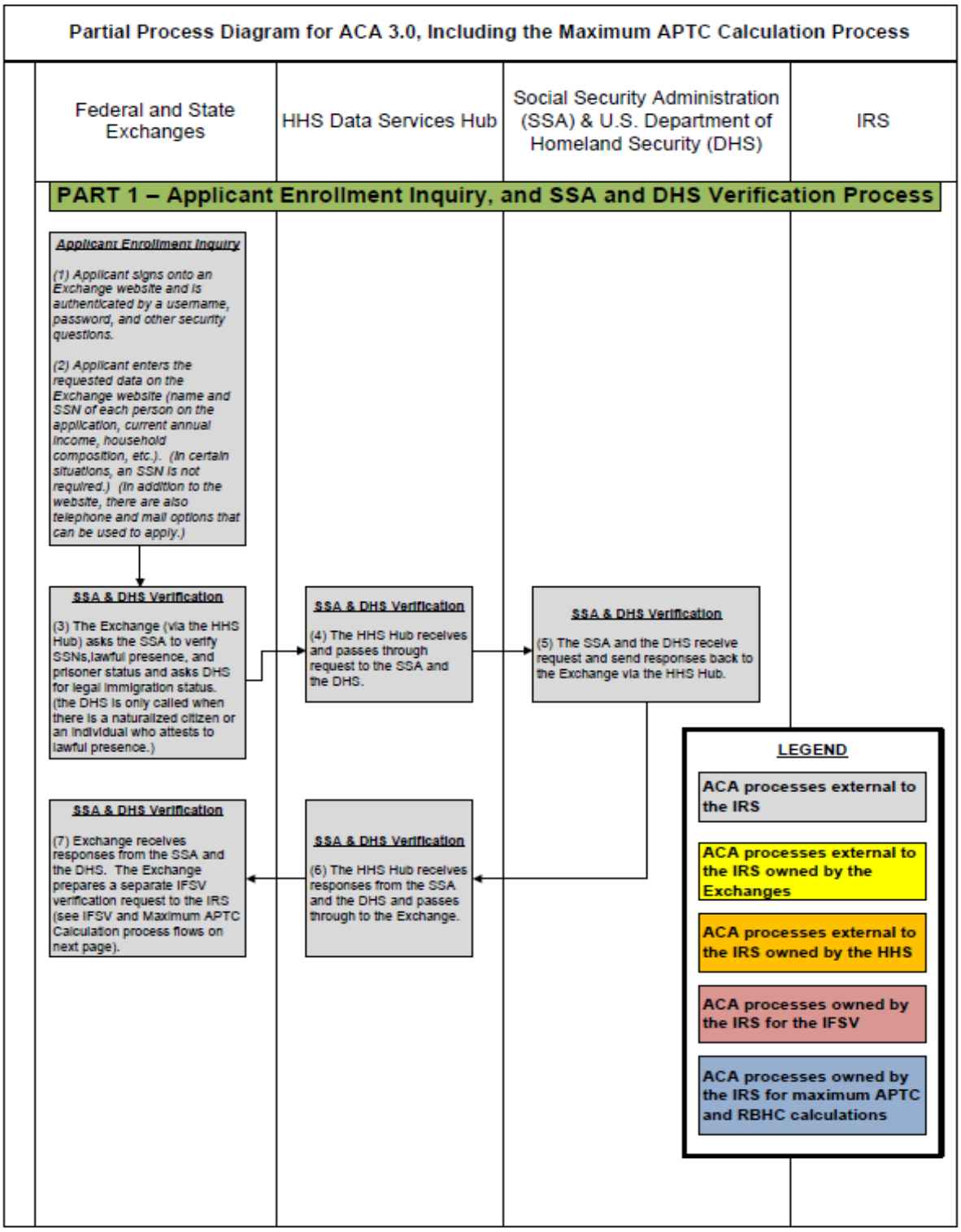
IFSV = Income and Family Size Verification.

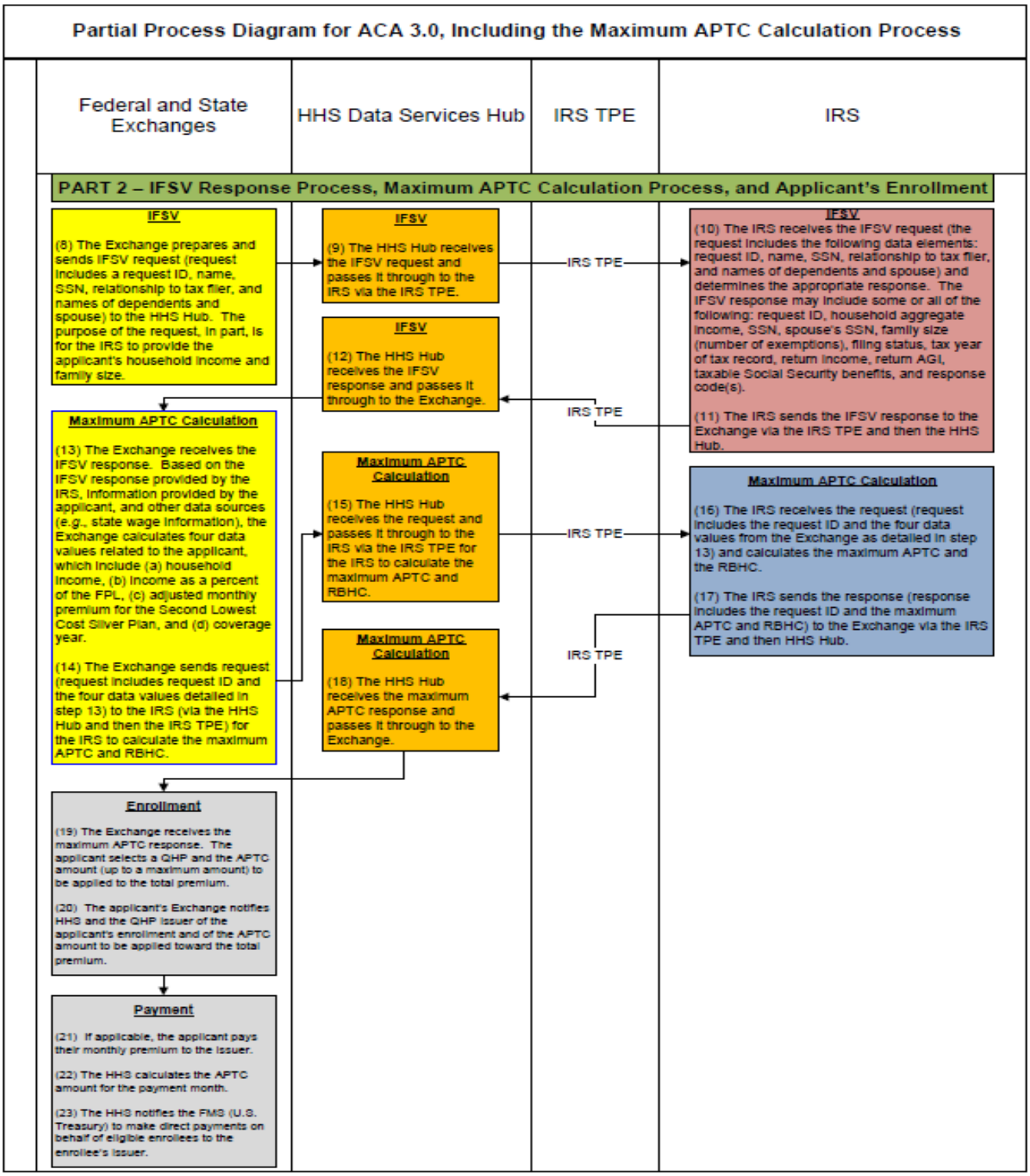
QHP = Qualified Health Plan.

SSA = Social Security Administration.

SSN = Social Security Number.

TPE = Transactional Portal Environment.


Partial Process Diagram for ACA 3.0, Including the Maximum APTC Calculation Process
Federal and State Exchanges
HHS Data Services Hub
Social Security Administration (SSA) & U.S. Department of Homeland Security (DHS)
IRS
PART 1 – Applicant Enrollment Inquiry, and SSA and DHS Verification Process
Applicant Enrollment Inquiry
(1) Applicant signs onto an Exchange website and is authenticated by a username, password, and other security questions.
(2) Applicant enters the requested data on the Exchange website (name and SSN of each person on the application, current annual income, household composition, etc.). (In certain situations, an SSN is not required.) (In addition to the website, there are also telephone and mail options that can be used to apply.)
SSA & DHS Verification
(3) The Exchange (via the HHS Hub) asks the SSA to verify SSNs,lawful presence, and prisoner status and asks DHS for legal immigration status. (the DHS is only called when there is a naturalized citizen or an individual who attests to lawful presence.)
SSA & DHS Verification
(4) The HHS Hub receives and passes through request to the SSA and the DHS.
SSA & DHS Verification
(5) The SSA and the DHS receive request and send responses back to the Exchange via the HHS Hub.
SSA & DHS Verification
(6) The HHS Hub receives responses from the SSA and the DHS and passes through to the Exchange.
SSA & DHS Verification
(7) Exchange receives responses from the SSA and the DHS. The Exchange prepares a separate IFSV verification request to the IRS (see IFSV and Maximum APTC Calculation process flows on next page).
LEGEND
ACA processes external to the IRS
ACA processes external to the IRS owned by the Exchanges
ACA processes external to the IRS owned by the HHS
ACA processes owned by the IRS for the IFSV
ACA processes owned by the IRS for maximum APTC and RBHC calculations



Source: TIGTA diagram based on information provided by the IRS and HHS.

Appendix V

Glossary of Terms

Adjusted Gross Income	The total of an individual's wages, salaries, interest, dividends, *etc.*, minus allowable deductions.
Affordable Care Act (ACA)	In March 2010, the President signed into law the Patient Protection and Affordable Care Act to provide more Americans with access to affordable health care by January 1, 2014.
Advanced Premium Tax Credit	Paid in advance to a taxpayer's insurance company to help cover the cost of premiums.
Auditable Events	Actions taken on IRS systems that shall be captured and recorded for subsequent audit review based on the impact level of the system (high, moderate, or low) as determined by the guidelines in the National Institute of Standards and Technology Federal Information Processing Standards 199, Standards for Security Categorization of Federal Information and Information Systems. IRM 10.8.3 contains lists of auditable events applicable to the systems categorized as high, moderate, or low based on the National Institute of Standards and Technology Federal Information Processing Standards 199.
Baseline Configuration	A set of specifications for a system, or configuration item within a system, that has been formally reviewed and agreed on at a given point in time, and which can be changed only through change control procedures. The baseline configuration is used as a basis for future builds, releases, and/or changes.
Centers for Medicare and Medicaid Services (CMS)	A division of the HHS, the CMS provides health coverage for 100 million people through Medicare, Medicaid, and the Children's Health Insurance Program.
Change Management	The transition of a changed or new product through development to deployment into the current production environment with minimum disruption to users. This can occur in a number of ways including, but not limited to: (1) implementation of a change to a product baseline; (2) establishing a new product baseline; and (3) a change to a Service Level Agreement.

Change Request	The method for requesting approval to change a baselined product or other controlled item.
Configuration Settings	The set of parameters that can be changed in hardware, software, and/or firmware that affect the security posture and/or functionality of the information system.
Electronic Fraud Detection System	An IRS automated compliance system designed to maximize fraud detection at the time tax returns are filed to prevent the issuance of questionable refunds. The primary information system used to support the Criminal Investigation Questionable Refund Program.
Enterprise Life Cycle	The Enterprise Life Cycle is the approach used by the IRS to manage and implement business change through information systems initiatives.
Exchange	Exchanges are intended to provide a place for Americans to shop for health insurance in a competitive environment.
Federal Poverty Level (FPL)	Guidelines published and updated periodically in the Federal Register by the Secretary of the HHS. The APTC will be available for individuals and families whose incomes are at least 100 percent and up to 400 percent of the FPL who do not have minimal essential coverage.
Health and Human Services	The U.S. Government's principal agency for protecting the health of all Americans and providing essential human services.
Hub	Supports the exchanges by providing a single point where exchanges may access data from different sources, primarily Federal agencies.
Income and Family Size Verification	Will verify income and family size for individuals requesting eligibility for an APTC for health insurance.
Infrastructure	The fundamental structure of a system or organization. The basic, fundamental architecture of any system (electronic, mechanical, social, political, *etc.*) determines how it functions and how flexible it is to meet future requirements.
Iterative Systems Development Life Cycle	The Iterative Path is 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.

JavaBeans Open Source Software	A platform for developing and deploying enterprise applications, Web applications, and services and portals.
Logical Access	The ability to interact with data through access control procedures such as identification, authentication, and authorization.
Low Impact System	An information system in which all three security objectives (*i.e.*, confidentiality, integrity, and availability) are assigned a Federal Information Processing Standards 199 potential impact value of low.
Minimum Essential Coverage	The type of coverage an individual needs to have to meet the individual responsibility requirement under the ACA. This includes individual market policies, job-based coverage, Medicare, Medicaid, and certain other coverage.
National Institute of Standards and Technology	A nonregulatory Federal agency within the Department of Commerce responsible for developing standards and guidelines, including minimum requirements, for providing adequate information security for all Federal Government agency operations and assets.
Oracle	An object-relational database management system.
Premium Tax Credit	A new refundable tax credit to help taxpayers and families afford health insurance coverage purchased through an Exchange.
Remainder Benchmark Household Contribution	The household's contribution towards the monthly insurance premium.
Requirement	A formalization of a need and the statement of a capability or condition that a system, subsystem, or system component must have or meet to satisfy a contract, standard, or specification.
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.
Second Lowest Cost Silver Plan	Plans in the Marketplace 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.

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. At the end of the sprint, the functionality developed is fully tested (although it will not be put into production until a later date).
Test Case	Created to specify and document the conditions to be tested and to validate that a system functions as intended.
Transactional Portal Environment	A portal environment to service ACA information system needs. The IRS uses the Transactional Portal Environment for mediating transaction requests between the Hub and the IRS.
UNIX Policy Checker	A policy checking tool used to examine servers or mainframe systems and compare their operating system configuration settings to the IRS Cybersecurity policies or interim guidance.
webMethods	Provides a business process integration software for the enterprise, such as a platform, which is an underlying computer system on which application programs can run.

Appendix VI

Management's Response to the Draft Report

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

CHIEF TECHNOLOGY OFFICER

September 12, 2013

MEMORANDUM FOR DEPUTY INSPECTOR GENERAL FOR AUDIT

FROM: Terence V. Milholland
Chief Technology Officer

SUBJECT: Affordable Care Act: Improvements Are Needed to Strengthen Systems Development Controls for the Premium Tax Credit Project – Audit# 201320312 (e-trak #2013-46418)

Thank you for the opportunity to review your draft audit report and to discuss earlier draft report observations with the audit team. I was pleased to read your observation acknowledging that our premium tax credit computation engine accurately calculated the maximum advance premium tax credit.

The Affordable Care Act (ACA) Program Management Office has put in place sound management practices that have been recognized by the Treasury Inspector General for Tax Administration (TIGTA) in earlier reviews. There are always opportunities for improvement, and we appreciate TIGTA's observations in the areas of change management and testing.

The IRS has a consistently strong focus on both securing our information technology systems and guarding against tax administration fraud. In conducting its fieldwork, the audit team observed the IRS while it conducted the Security Control Assessment (SCA). In line with our current practice and procedures, we developed an action plan for any issues identified at the conclusion of the SCA. As part of our process, our Cybersecurity organization has completed the Security Assessment Report and a risk mitigation plan since the close of the audit in accordance with National Institute of Standards and Technology guidelines.

I am committed to continuously improving the IRS information technology systems and processes. We value your continued support and the assistance, and guidance your team provides. Our corrective action plan for the recommendations is attached. If you have any questions, please contact me at (202) 622-6800, or a member of your staff may contact Lisa Starr, Program Oversight Coordination Manager, at (240) 613-4219.

Attachment

Attachment

Draft Audit Report - Affordable Care Act: Improvements Are Needed to Strengthen Systems Development Controls for the Premium Tax Credit Project (Audit # 201320312) (e-trak# **2013-46418**)

RECOMMENDATION #1: The Chief Technology Officer should ensure that testing peer review guidance and other applicable guidelines are updated and that a test case management tool is used to ensure that APTC test case input data files, test cases, and test case run histories are properly controlled.

CORRECTIVE ACTION #1: The IRS agrees. The ACA Strategic Test Management Plan and supporting procedures will be updated to reflect additional testing peer review guidance and other applicable guidelines to ensure that APTC test case input data files, test cases, and test case run histories are properly controlled.

IMPLEMENTATION DATE: February 25, 2014

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

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

RECOMMENDATION #2: The Chief Technology Officer should ensure that change request templates, tools, and applicable change management guidelines are updated to ensure that change requests include the affected requirement numbers and requirement descriptions for adequate traceability of requirements and test cases to the RTVM.

CORRECTIVE ACTION #2: The IRS agrees. The Premium Tax Credit (PTC) Project Team has taken intermediate action as of May 2013, to add the requirement traceability field under the Implementer section of the PTC Change Management Request template. This change ensures that requirements are adequately traceable from the Change Management Request to the requirement stored in the RequisitePro repository. In addition, we will update our change management guidelines and templates to ensure that change requests include the affected requirement numbers and descriptions for adequate traceability of requirements and test cases to the RTVM.

IMPLEMENTATION DATE: February 25, 2014

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

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 update test management procedures to include additional controls and processes to document how traceability between requirements, test cases, and test results will be achieved for interagency testing.

Attachment

Draft Audit Report - Affordable Care Act: Improvements Are Needed to Strengthen Systems Development Controls for the Premium Tax Credit Project (Audit # 201320312) (e-trak# **2013-46418**)

CORRECTIVE ACTION #3: The IRS agrees. The ACA Strategic Test Management Plan will be updated to formally document how traceability between requirements, test cases, and test results are achieved for testing with external entities.

IMPLEMENTATION DATE: February 25, 2014

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

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 the Cybersecurity organization resolves or develops an action plan with specific corrective actions and time periods for the failed security tests as part of the ACA Security Assessment and Authorization.

CORRECTIVE ACTION #4: The IRS disagrees with this recommendation as we already do this process. As discussed during the audit, we already have documented policies in place in our Internal Revenue Manual (IRM) that address this recommendation. IRM 10.8.1.3.5.1 requires weaknesses, identified during the Security Assessment and Authorization, to be documented in a POA&M to include planned, implemented and evaluated remedial actions to correct any deficiencies.

IMPLEMENTATION DATE: N/A

RESPONSIBLE OFFICIAL: The Associate Chief Information Officer, Cybersecurity (CS)

CORRECTIVE ACTION MONITORING PLAN: N/A

RECOMMENDATION #5: The Chief Technology Officer should ensure that change requests and impact assessments are accurately prepared and processed as required by change management guidelines.

CORRECTIVE ACTION #5: The IRS agrees. Steps have been taken to provide Cybersecurity staff with access to the Change Request Tracking System so that they are aware when final changes to the baseline security requirements have been implemented.

IMPLEMENTATION DATE: February 25, 2014

RESPONSIBLE OFFICIAL: The Associate Chief Information Officer, Cybersecurity (CS)

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

Attachment

Draft Audit Report - Affordable Care Act: Improvements Are Needed to Strengthen Systems Development Controls for the Premium Tax Credit Project (Audit # 201320312) (e-trak# **2013-46418**)

RECOMMENDATION #6: The Chief Technology Officer should ensure that the IRM is updated to provide specific guidance on how IRS management is to effectively manage, monitor, and mitigate fraud risk for information technology systems.

CORRECTIVE ACTION #6: The IRS agrees with this recommendation. This analysis is already occurring in the implementation of ACA, and we agree that the appropriate IRM sections should be up to date to ensure that fraud risk is considered in developing requirements and systems capabilities as part of every legislative implementation project.

IMPLEMENTATION DATE: September 25, 2014

RESPONSIBLE OFFICIAL: The Associate Chief Information Officer, Strategy and Planning

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 #7: The Chief Technology Officer should ensure that the ACA Program completes a comprehensive fraud mitigation strategy to guide ACA systems development, testing, and implementation.

CORRECTIVE ACTION #7: The IRS agrees that this recommendation will be implemented for every ACA release. In the development of ACA 3.0, which goes live in October 2013, we have already determined there is no tax fraud risk with the Advanced Premium Tax Credit (APTC) calculator nor the Income and Family Size Verification (IFSV) process. The IFSV is merely providing data in answer to a factual query; the IRS does not interface with the citizen, the tax data is not displayed on Exchange screens, and the IRS is not part of the Exchange determination of predicted 2014 income. The APTC computation service does not identify the citizen to the IRS and does not use tax data. The IRS takes in anonymous inputs from the Exchange and returns a math answer. The IRS does not retain the answers to the queries as the answers may or may not equal what is in the Exchange account once all Exchange processes are completed.

IMPLEMENTATION DATE: N/A

RESPONSIBLE OFFICIAL: The Director, Affordable Care Act Office (Services & Enforcement)

CORRECTIVE ACTION MONITORING PLAN: N/A