TREASURY INSPECTOR GENERAL FOR TAX ADMINISTRATION

While Efforts Are Ongoing to Deploy a Secure Mechanism to Verify Taxpayer Identities, the Public Still Cannot Access Their Tax Account Information Via the Internet

September 25, 2013

Reference Number: 2013-20-127

WHILE EFFORTS ARE ONGOING TO DEPLOY A SECURE MECHANISM TO VERIFY TAXPAYER IDENTITIES, THE PUBLIC STILL CANNOT ACCESS THEIR TAX ACCOUNT INFORMATION VIA THE INTERNET

Highlights

Final Report issued on September 25, 2013

Highlights of Reference Number: 2013-20-127 to the Internal Revenue Service Chief Technology Officer.

IMPACT ON TAXPAYERS

While the IRS Restructuring and Reform Act of 1998 (RRA 98) required the IRS to develop procedures to allow taxpayers filing returns electronically to review their accounts online by December 31, 2006, the IRS did not meet this requirement. Allowing taxpayers to securely access tax information online will modernize how the IRS interacts with taxpayers, allow for faster response to queries from the general public, and thereby greatly reduce taxpayer burden.

WHY TIGTA DID THE AUDIT

This audit was initiated at the request of the IRS Oversight Board to evaluate the IRS's progress in providing taxpayers with secure online access to their tax account information.

WHAT TIGTA FOUND

The IRS successfully implemented Release 1 of the eAuthentication application during Fiscal Year 2012, which allowed a small number of taxpayers to securely verify their identities with the IRS and participate in the eTranscripts for Banks application. While several applications have been developed and implemented by the IRS, none of these applications meet the RRA 98 requirements. However, TIGTA also determined that required capacity testing was not adequately completed to ensure that the eAuthentication application can support the expected number of users at any given time and noted deficiencies with the reporting functionality

in Release 1 of the eAuthentication application, which will be addressed in future releases. Finally, TIGTA noted that total cost information for the project is not readily obtainable for project management.

WHAT TIGTA RECOMMENDED

TIGTA recommended that the IRS reprioritize its efforts to develop and implement applications that both serve the taxpayer and comply with RRA 98 requirements. TIGTA also recommended that the IRS perform complete capacity testing of the eAuthentication application prior to Release 2 and continue its efforts in upgrading the reporting functionality of the eAuthentication application. Finally, TIGTA recommended that the IRS coordinate to develop a formal system to provide reports of actual costs received and accepted by Contracting Officer Representatives.

In their response, IRS management agreed with three of our four recommendations. The IRS plans to prioritize release of applications that meet the requirements of RRA 98, complete performance and capacity testing as part of Release 2 of the eAuthentication application, and to increase reporting functionality in Release 2 of the eAuthentication application.

Although IRS management agreed with the intent and spirit of the fourth recommendation, they disagreed with our finding, which they consider an isolated example and therefore no further action is necessary. During the audit, we found that the existing procurement system cannot track sufficient detail to the project cost levels for contracts serving multiple projects, such as the eAuthentication project. As such, we believe that this is not an isolated occurrence and that it needs to be addressed to ensure actual project costs can be readily identified and tracked for management and decision making purposes.

DEPARTMENT OF THE TREASURY

WASHINGTON, D.C. 20220

TREASURY INSPECTOR GENERAL
FOR TAX ADMINISTRATION

September 25, 2013

MEMORANDUM FOR CHIEF TECHNOLOGY OFFICER

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

SUBJECT: Final Audit Report – While Efforts Are Ongoing to Deploy a Secure
                        Mechanism to Verify Taxpayer Identities, the Public Still Cannot
                        Access Their Tax Account Information Via the Internet
                        (Audit # 201220003)

This report presents our review of the Internal Revenue Service's efforts to implement a secure mechanism to verify taxpayer identities and allow the public to access their tax account information via the internet. This audit was included in our Fiscal Year 2012 Annual Audit Plan addresses the major management challenge of Security for Taxpayer Data and Employees.

Management's complete response to the draft report is included in Appendix IV. Copies of this report are also being sent to the IRS managers affected by the report recommendations.

If you have any questions, please contact me or Alan Duncan, Assistant Inspector General for Audit (Security and Information Technology Services).

Attachment

Table of Contents

Abbreviations

COR	Contracting Officer Representative
ID	Identification
IRS	Internal Revenue Service
IT	Information Technology
MIRSA	My IRS Account
RRA 98	Restructuring and Reform Act of 1998

Background

The Internal Revenue Service (IRS) Restructuring and Reform Act of 1998 (RRA 98)[1] requires the IRS to allow taxpayers to access tax account information online. In addition, other Federal mandates, including the Office of Management and Budget Memorandum M-04-04 (eAuthentication[2] Guidance for Federal Agencies) and the President's National Strategy for Trusted Identities in Cyberspace, provide guidance to the IRS for undertaking such an endeavor. In April 2006, the IRS initiated the My IRS Account (MIRSA) project to provide taxpayers with an online system to view, access, update, and manage their tax accounts. In December 2008, after 32 months of development and the expenditure of approximately $10 million, the MIRSA project was cancelled due to a lack of an effective enterprise-wide eAuthentication strategy.

In its 2009 report,[3] the Treasury Inspector General for Tax Administration recommended that the IRS complete a long-term strategy for the MIRSA project. As part of the planned corrective actions to the MIRSA project, the IRS stated that it would develop a strategic approach that will provide individual taxpayers online access to their transcript information through the primary IRS website, IRS.gov, via the Registered User Portal.[4] Taxpayers would have the ability to view, download, and print their transcript information. In August 2010, the IRS completed the "Online Services Strategic Approach," which outlined the IRS's priorities for online services for individual taxpayers. While the strategic approach has been completed, it is a draft version and not ready for distribution.

In conjunction with the Online Services Strategic Approach, the eAuthentication application is a new effort in which the IRS plans to leverage the Registered User Portal authentication and registration processes to provide the desired identity verification services bolstered by selected commercial off-the-shelf software products. The objective of the IRS eAuthentication project is

---

[1] Restructuring and Reform Act of 1998, Pub. L. No. 105-206, 112 Stat. 685 (codified as amended in scattered sections of 2 U.S.C., 5 U.S.C. app., 16 U.S.C., 19 U.S.C., 22 U.S.C., 23 U.S.C., 26 U.S.C., 31 U.S.C., 38 U.S.C., and 49 U.S.C.).

[2] eAuthentication is defined as the process of establishing confidence in user identities electronically presented to an information system. Systems can use the authenticated identity to determine if that individual is authorized to perform an electronic transaction. In most cases, the authentication and transaction take place across an open network such as the Internet, however in some cases access to the network may be limited and access control decisions may take this into account.

[3] Treasury Inspector General for Tax Administration, Ref. No. 2009-20-102, *Changing Strategies Led to the Termination of the My IRS Account Project* 3, (August 2009)

[4] A portal is defined as a website that brings information together from diverse sources in a uniform way. Usually, each information source gets its dedicated area on the page for displaying information. The Registered User Portal is an IRS external portal that allows registered individuals and third-party users to access the IRS for interaction with selected tax processing and other sensitive systems, applications, and data.

to design and build a common service to proof and register individuals and to provide and validate credentials for ongoing system access using the Internet. The IRS expects that the eAuthentication project will be an enabling service to other applications that are accessible by the public. The eAuthentication project will not build end-user applications but will provide centralized security mechanisms for applications that are built.

The IRS estimated total costs for Release 1 and Release 2 of the eAuthentication application, including Operations and Maintenance through Fiscal Year 2017, at approximately $65.3 million. Release 1 was deployed at a total development cost of about $26.9 million and provided the core infrastructure (hardware and software) upon which subsequent releases are based. Release 2 development costs are estimated at approximately $8.5 million and should provide enhanced identity verification up to multifactor authentication.[5] The IRS estimates the base operations and maintenance costs for the eAuthentication application through Release 2 at approximately $29.9 million, not including per-transaction costs. A third release of the eAuthentication application is anticipated; however, no approved cost or schedule is currently available.

The responsibility for managing the eAuthentication application and implementing its rollout resides with the Information Technology (IT) Cybersecurity organization. The IT Cybersecurity organization manages the eAuthentication application by following the Enterprise Life Cycle[6] and is the overall business and program owner. The IRS uses its Transition Management processes to transfer the daily management of the eAuthentication application to the Enterprise Operations organization and other receiving organizations. To ensure the success of information technology projects, the IRS requires project managers to report to an executive governance committee for oversight and approval of key decisions. The Security Services and Privacy Executive Steering Committee provides this oversight and conducts Enterprise Life Cycle milestone exit reviews for the eAuthentication application.

The rollout of IRS online applications to be protected by the eAuthentication framework is shared by the Office of Online Services, the Wage and Investment Division, the Office of Privacy, Governmental Liaison and Disclosure, and IT organizations including Applications Development and Cybersecurity. The Office of Online Services, which reports directly to the Office of the Deputy Commissioner for Services and Enforcement, is an IRS-wide group dedicated to providing online (web or mobile) self-service tools for the taxpayer.

---

[5] Multifactor authentication is defined as a security system in which more than one form of authentication is implemented to verify the legitimacy of a transaction. Multifactor authentication is achieved by combining two or three independent credentials: what the user knows (knowledge-based authentication), what the user has (security token or smart card) and what the user is (biometric verification).

[6] Enterprise Life Cycle is defined as the approach used by IRS to manage and implement business changes through information systems initiatives.

This review was performed at the IRS National Headquarters in Washington, D.C., and the IRS IT Cybersecurity function and the Office of Online Services in New Carrollton, Maryland, during the period November 2012 through June 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

Applications Were Created to Increase Online Taxpayer Functionality; However, These Applications Do Not Meet the Criteria of the Restructuring and Reform Act of 1998

The RRA 98 required the IRS to develop procedures to allow taxpayers filing returns electronically to review their account online by December 31, 2006. The IRS did not meet this requirement, and we determined that the IRS has not made adequate progress in allowing taxpayers to access tax accounts. Currently, taxpayers cannot review account information electronically. The IRS Oversight Board is aware that a disparity exists between what is required by Congress and the amount of Internet accessibility currently available to taxpayers. In April 2012, the Oversight Board requested that the Treasury Inspector General for Tax Administration audit the IRS's progress to provide taxpayers with the ability to review tax account records and report any findings. The eTranscripts for Banks application does not meet the intent of the RRA 98 because it only allows taxpayers to request that their tax account and tax return transcripts be sent to their lending institution electronically versus a hardcopy request. It does not provide the ability to view, print, or perform any other functions.

We believe that IRS leadership did not prioritize the applications that meet the requirements of the RRA 98. Rather, the IRS devoted resources to the development and implementation of several applications that do not meet the intent of the RRA 98. These are the eTranscripts for Banks, Where's My Refund?, and Where's My Amended Return? applications. The eTranscripts for Banks application, which was deployed in August 2012, allows taxpayers to request that a tax transcript be sent to a lending institution electronically. The Where's My Refund? application allows taxpayers to track the status of their refund. This application, originally deployed in 2002, was called the Internet Refund Fact of Filing application, and was redeployed with enhancements in January 2013. The Where's My Amended Return? application allows taxpayers to track the status of an amended return and was deployed in March 2013. While the applications do not directly address the requirements of account review, the applications do provide ancillary benefits to taxpayers.

The IRS online Get Transcript application is expected to be the first application to meet the intent of the RRA 98. The Get Transcript application will allow taxpayers to access their tax account information via the Internet. Through discussions with Get Transcript application personnel, we were informed that the application is expected to be deployed in January 2014.

In its April 2013 report, the Government Accountability Office[7] stated that while the IRS's efforts have already benefited taxpayers and hold the promise of additional benefits in the future, the IRS does not have a long-term strategy for enhancing its website that explains how its ongoing and new efforts fit together. No overall cost estimate exists, and there are not enough details on goals, deliverables, future online services, and time frames to be able to assess progress.

Because the deadlines proposed in the RRA 98 were not met, taxpayers' ability to electronically fulfill their tax responsibilities and review their tax account information using the Internet is diminished. In addition, there is an increased burden on IRS customer service representatives answering taxpayer's calls and questions for transcript requests by not implementing an online application that is RRA 98 compliant.

Recommendation

Recommendation 1: The Office of the Deputy Commissioner for Services and Enforcement should reprioritize future applications to meet the RRA 98 requirements on or before January 2014. The prioritization will need to be coordinated with the IT organization.

> ***Management's Response:*** The IRS agreed with this recommendation. The IRS has prioritized future applications based on internal and external stakeholder needs, information technology constraints and safeguards, and requirements such as RRA 98. The Get Transcript application is scheduled to launch in January 2014 and will give taxpayers the ability to view, print and download their tax transcripts. The IRS also plans to increase interactive capabilities and identify additional features associated with an account. Using available resources cost effectively, the IRS will prioritize the rollout of features by delivering the most impactful capabilities first.

Release 1 of the eAuthentication Application Was Successfully Deployed in Fiscal Year 2012

The E-Government Act of 2002[8] requires Government agencies to increase their presence on the Internet. The purpose of the act is "to promote use of the Internet and other information technologies to provide increased opportunities for citizen participation in Government" and "to promote the use of the Internet and emerging technologies within and across Government agencies to provide citizen-centric Government information and services." Additionally, the RRA 98 requires the IRS to develop procedures under which taxpayers filing returns

---

[7] Government Accountability Office, GAO-13-435, *IRS WEBSITE*: *Long-Term Strategy Needed to Improve Interactive Services* (Apr. 2013).
[8] E-Government Act of 2002, Pub.L. 107–347, 116 Stat. 2899, 44 U.S.C. § 101, H.R. 2458/S. 803

electronically would be able to review their accounts electronically. The eAuthentication application is essentially the first step for the IRS to meet these legislative requirements.

In Fiscal Year 2012, the IRS developed the first release of an enterprise solution for authenticating taxpayers via the Internet through its eAuthentication application. The main function of the eAuthentication application is to provide a uniform way taxpayers can authenticate[9] themselves to the IRS before accessing any of the IRS's online applications. Taxpayers create an account with a user identification (ID) and password which is then used to authenticate to the applications that use the eAuthentication application. To create an account, a taxpayer must provide some basic information about themselves such as name, address, date of birth, Social Security Number or other Taxpayer Identification Number, and filing status. The IRS uses the attributes to verify the identity of the taxpayer. Once the taxpayer's identity has been verified, they are allowed to create an eAuthentication account.

In August 2012, the first application to use the eAuthentication application was deployed, eTranscripts for Banks. The successful deployment of Release 1 of the eAuthentication application is due to the coordinated efforts across the IRS organization. The Cybersecurity organization led the effort and coordinated with the Applications Development organization on the eAuthentication application and the deployment of eTranscripts for Banks as the first projected application. The Office of Online Services coordinated the implementation of the eAuthentication application with the eTranscripts for Banks application by establishing and managing a proof of concept with banking partners to validate the concept of online identity proofing and authentication.

The eTranscripts for Banks application allows taxpayers to request that tax transcripts be sent to their lending institution online. Currently, there are three lending institutions that are enrolled to use the eTranscripts for Banks application, and others are expected to use the application as well. Release 2 of the eAuthentication application was formally started on October 24, 2012. Release 2 is expected to provide additional functionality and security and should allow more applications to use the eAuthentication application for identity proofing. As more applications use the eAuthentication application, the taxpayer experience online should be expanded.

Despite the successful deployment of Release 1 of the eAuthentication application, we identified some areas of concern and improvement that will contribute to further successes in future releases of the eAuthentication application.

---

[9] Authentication is the process of determining whether someone or something is, in fact, who or what it is declared to be. In private and public computer networks (including the Internet), authentication is commonly done through the use of logon passwords.

Complete Capacity Testing for the eAuthentication Application Was Not Performed

The Internal Revenue Manual states that capacity testing is a required part of system integration testing. The purpose of capacity testing is to determine if the application can support the expected number of users authenticating at any given time.

We determined that the IRS eAuthentication project team did not perform complete capacity testing on Release 1 of the eAuthentication application. Without capacity testing, the IRS does not know how many users can access the eAuthentication application at once before it fails. The IRS estimated a total of 30,000 users would register to use the eAuthentication application to access the eTranscripts for Banks application between August 2012 and November 2012. However, the IRS reported that a total of 96 users requested to use the eAuthentication application in that time period, and only 52 of the 96 users were successful in using the eAuthentication application.

Capacity testing of the eAuthentication application was not fully performed due to instability of the IRS information technology Development, Integration and Testing infrastructure, concerns over the security of data in the testing environment, and scheduling delays caused by technical issues in the eAuthentication application servers. Because of this, full scope capacity testing could not be completed. Also, the test environment that would be used to conduct capacity testing is shared by other testing organizations. Therefore, it would be impossible to secure the environment and adequately protect the Personally Identifiable Information that would be contained in the test data. Finally, the project team experienced technical difficulties that took longer than expected to resolve. Due to these difficulties, management decided to move forward with the project rather than delay implementation of the project.

Without performing adequate capacity testing, the IRS is unable to verify that the eAuthentication application will function as intended. The system could become unresponsive and make it impossible for taxpayers to access any application that relies upon the eAuthentication application as the means to authenticate taxpayer identities. As the enterprise wide solution for authentication, this lack of capacity testing could have far-reaching implications. Any application using the eAuthentication application for identity proofing could be taken offline due to bandwidth restrictions, thus making any IRS online application inaccessible via the Internet to taxpayers.

The IRS has seen dramatic increases in the number of taxpayers who have attempted to access their information via the IRS website, IRS.gov. The Where's My Refund? application on IRS.gov had 79 million attempted accesses by taxpayers in the 2011 Filing Season, 140 million attempts in the 2012 Filing Season, and 218 million attempted accesses in the 2013 Filing Season. If the IRS expects a similar response by taxpayers to the applications that will be supported by Release 2 of the eAuthentication application, it is imperative that the IRS perform

capacity testing prior to its release. Through discussions with the eAuthentication project team, we noted capacity testing has been included as part of the testing and verification portfolio for Release 2 of the eAuthentication application.

Recommendation

Recommendation 2: The Associate Chief Information Officer, Cybersecurity, should ensure that capacity testing is adequately performed for the eAuthentication application prior to Release 2 being deployed.

> **Management's Response:** The IRS agreed with this recommendation. The eAuthentication Release 2 project, as already planned, includes performance and capacity testing as part of its Release 2 go-Live activities.

Reporting Functionality Will Be Improved in Release 2 of the eAuthentication Application

The National Institute of Standards and Technology Special Publication 800-53, *Recommended Security Controls for Federal Information Systems and Organizations*, states that an organization should review and analyze information system audit records for indications of inappropriate or unusual activity and report findings to designated organizational officials. It also states that an information system should provide an audit report generation capability that provides support for near real-time audit review, analysis, and reporting requirements and after-the-fact investigations of security incidents.

We determined that Release 1 of the eAuthentication application has limited reporting functionality. While actions taken by users within the eAuthentication application are identified by user ID, these actions are not associated to a user's actual name and, therefore, cannot be associated to a specific taxpayer. Also, the user information captured by the application may contain Personally Identifiable Information and, therefore, must be encrypted when it is stored on the server. However, the IRS does not have a mechanism to make the encrypted data readable. The IRS does have an Enterprise Security Audit Trail that has the ability to log auditable events for each taxpayer transaction that does track the individual with their Social Security Number. These transactions are available for designated security and audit individuals but not generally available for management review.

For Release 2 of the eAuthentication application, the project team plans to use the internal Business Objects Enterprise shared services infrastructure, which uses SAP Business Objects suite of products, to meet reporting requirements. The Business Objects Enterprise capability should enable the project team to provide stakeholders access to more useful reports for both customer usage reporting and process effectiveness purposes.

Without adequate reporting functionality, the IRS is able to see minimal details about taxpayers using the eAuthentication application. The expanded reporting functionality should provide the IRS with application specific reports, taxpayer account reports, and system infrastructure reports.

Recommendation

Recommendation 3: The Associate Chief Information Officer, Cybersecurity, should continue the efforts to acquire appropriate software to enable additional reporting functionality.

> **Management's Response:** The IRS agreed with this recommendation. The eAuthentication Release 2 project, as already planned, includes integration with the existing IRS internal Business Objects Enterprise capability to enable broad management information system reporting. This will allow the project to configure the system to produce the following business approved reports, such as application specific reports, taxpayer account reports and system infrastructure reports.

Actual Cost Information Is Not Readily Available for Project Management Purposes

The Cybersecurity organization requires its projects to be tracked, monitoring baselines and actual project costs on a monthly basis using the Cybersecurity Project Lifecycle Cost Performance Table. This information is used to report project cost information to the various governance boards. Additionally, the Cybersecurity organization required the project managers to debrief management on the project baselines as it relates to scope, cost, and Enterprise Life Cycle schedule within the months of December 2012 through March 2013. This debrief ensures that the projects are able to provide realistic information for assessment.

We determined that actual cost information is not readily available for eAuthentication project management. We were informed that the project office has no formal system to obtain actual costs. The project manager uses a less formal approach (*e.g.*, calling people or manually tracking expenses) to obtain actual cost information.

The IRS has not implemented a system to provide project managers with timely, accurate project cost information. Contracting Officer Representatives (COR), who have been delegated responsibility for approving invoices and monitoring contractor payments, did not provide the Cybersecurity eAuthentication project manager information on invoices they approved for contracts used by the eAuthentication project on a monthly or any other basis.

Due to the informal nature of the process used, the cost information the project manager obtains and ultimately reports to Cybersecurity organization executive management are estimates and may be inaccurate and unreliable. Executive management should be given the best information possible when making key resource decisions.

Recommendation

Recommendation 4: The Chief Technology Officer and Chief, Agency-Wide Shared
Services, should coordinate to develop a formal system to provide reports of actual costs
received and accepted by CORs.

> **_Management's Response:_** While the IRS agreed with the spirit and intent of this
> recommendation, it does not agree with the finding, which was based on an isolated example
> of a single COR managing project cost. All Receipt and Acceptance transactions are done
> within the Integrated Procurement System. A reports module, accessible by all CORs, allows
> the COR to track Receipt and Acceptance transactions completed for each project. This
> standard business practice is already being followed at the IRS; thus, no further action is
> needed.

> **_Office of Audit Comment:_** During our audit, the Cybersecurity eAuthentication project
> manager was not able to provide us with actual cost information for the eAuthentication
> project. Subsequent discussions yielded that the Integrated Procurement System itself cannot
> track sufficient details to project cost levels for contracts that serve multiple projects, such as
> the eAuthentication project. As such, we believe this is not an isolated occurrence and needs
> to be addressed to ensure actual project costs can be readily identified and tracked for
> management and decision-making purposes.

Detailed Objective, Scope, and Methodology

Our overall objective was to assess the development and implementation of an effective eAuthentication solution for taxpayers to access their tax information. To accomplish our objective, we:

I.   Evaluated security testing and capacity testing to determine whether National Institute of Standards and Technology Special Publication 800-53 security controls, capacity limits, and the Internal Revenue Manual password policies over the eAuthentication application are operating effectively.

  A. Determined whether the IRS properly conducted performance/capacity testing for the eAuthentication application.

  B. Obtained and reviewed documentation related to the security risk assessment for the eAuthentication application and assessed selected National Institute of Standards and Technology Special Publication 800-53 controls.

II.   Determined whether only appropriate users have the ability to authenticate with the eAuthentication application, per the National Institute of Standards and Technology Special Publication 800-63.

  A. Determine whether only appropriate users have the ability to authenticate with the eAuthentication application. User populations were not obtainable and, therefore, no sample was taken.

  B. Determined through online observation/testing whether users are authenticated to the eAuthentication application using the following attributes: name, Social Security Number or other Taxpayer Identification Number, date of birth, address, and filing status.

III. Determined the status of expanding the eAuthentication application to additional online applications and expanding the eTranscripts for Banks application to additional banks.

  A. Interviewed the eAuthentication project manager and Applications Development organization officials to determine their roles and responsibilities in the deployment of the eAuthentication application and the current plans and schedule to roll out the eAuthentication application to additional online applications and the eTranscripts for Banks application to additional banks.

  B. Interviewed Office of Online Services personnel, including the business project manager, to determine their roles and responsibilities in the deployment of the

eAuthentication application, and the current plans and schedule to roll out the eAuthentication application to additional online applications and to additional banks.

C. Determined how the eTranscripts for Banks application with Chase Bank works and where communication with Chase Bank occurs within the eAuthentication application.

D. Determined whether the current eTranscripts for Banks application meets the intent of RRA 98[1] and the E-Government Act of 2002[2] requirements.

IV. Determined costs for the full deployment of the eAuthentication application.

A. Obtained total costs to date by fiscal year for the eAuthentication application from the eAuthentication project manager or other responsible IRS officials.

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: the plans, policies, and processes of the IRS Cybersecurity, Applications Development, Office of Online Services, and Procurement organizations to manage, monitor, and report on the status and progress of efforts to provide taxpayers with secure online access to their tax account information. We evaluated these controls by conducting interviews and meetings with management and staff, performing independent analysis of controls in place, and reviewing documentation such as standard operating procedures, meeting minutes, and Enterprise Life Cycle artifacts.

---

[1] Restructuring and Reform Act of 1998, Pub. L. No. 105-206, 112 Stat. 685 (codified as amended in scattered sections of 2 U.S.C., 5 U.S.C. app., 16 U.S.C., 19 U.S.C., 22 U.S.C., 23 U.S.C., 26 U.S.C., 31 U.S.C., 38 U.S.C., and 49 U.S.C.).

[2] E-Government Act of 2002, Pub.L. 107–347, 116 Stat. 2899, 44 U.S.C. § 101, H.R. 2458/S. 803.

Major Contributors to This Report

Alan R. Duncan, Assistant Inspector General for Audit (Security and Information Technology Services)
Kent Sagara, Director
Myron Gulley, Acting Audit Manager
W. Allen Gray, Audit Manager
Charles O. Ekunwe, Lead Auditor
Samuel C. Mettauer, Information Technology Auditor
Linda Nethery, Information Technology Auditor
Larry Reimer, Information Technology Auditor

While Efforts Are Ongoing to Deploy a Secure Mechanism to Verify Taxpayer Identities, the Public Still Cannot Access Their Tax Account Information Via the Internet

Appendix III

Report Distribution List

Acting Commissioner
Office of the Commissioner – Attn: Chief of Staff C
Chief, Agency-Wide Shared Services OS:A
Deputy Commissioner for Operations Support OS
Deputy Commissioner for Services and Enforcement SE
Director, Office of Research, Analysis and Statistics RAS
Chief, Criminal Investigations SE:CI
Director, Statistics of Income RAS:S
Human Capital Officer OS:HC
Associate Chief Information Officer, Applications Development OS:CTO:AD
Associate Chief Information Officer, Cybersecurity OS:CTO:C
Associate Chief Information Officer, Enterprise Operations OS:CTO:EO
Associate Chief Information Officer, Enterprise Services OS:CTO:ES
Associate Chief Information Officer, Strategy and Planning OS:CTO:SP
Associate Chief Information Officer, User and Network Services OS:CTO:UNS
Chief Counsel CC
National Taxpayer Advocate TA
Director, Office of Legislative Affairs CL:LA
Director, Office of Program Evaluation and Risk Analysis RAS:O
Office of Internal Control OS:CFO:CPIC:IC
Audit Liaison: Director, Risk Management Division OS:CTO:SP:RM

Management's Response to the Draft Report

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

CHIEF TECHNOLOGY OFFICER

September 11, 2013

MEMORANDUM FOR DEPUTY INSPECTOR GENERAL FOR AUDIT

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

SUBJECT: Draft Audit Report – While Efforts Are Ongoing to
                     Deploy a Secure Mechanism to Verify Taxpayer
                     Identities, the Public Still Cannot Access Their Tax
                     Account Information Via the Internet, (Audit # 201220003)
                     (e-trak #2013-46297)

Thank you for the opportunity to review your draft audit report and meet with the audit team to discuss earlier report observations. We are pleased your report acknowledged that the IRS has successfully implemented Release 1 of the eAuthentication application. This Release allowed a number of taxpayers to securely verify their identities with the IRS and to participate in the eTranscripts for Banks application process. In the future, taxpayers filing returns electronically will be able to review their account information online.

Attached are our responses and corrective action plans with respect to your specific recommendations. The IRS agrees with your recommendations, including Recommendations 2 and 3, which acknowledge the risk-based decisions conducted for Release 1. Capacity and performance testing was conducted to mitigate the risk of going live for the 40,000 subscribers expected for the Send My Transcripts Proof of Concept. In fact, the actual subscriber volume realized was much lower. The IRS believes that the reporting capabilities developed for Release 1 were sufficient. At the time of the audit, execution of eAuthentication Release 2 was underway and improvements were occurring in these areas.

While we agree with the spirit and intent of Recommendation 4, we do not believe that the section on "actual cost information" accurately depicts the IRS's processes. This assessment was based on an isolated example of a single Contractor Officer's Representative (COR) managing project cost. All Receipt and Acceptance (R&A) transactions are done within the Integrated Procurement System. A reports module, accessible by all COR, allows the COR to track R&A completed for each project. This standard process is already being followed at the IRS; we therefore do not believe any further action is needed.

2

The IRS is committed to continuously improving the security of our information
technology systems and upgrading the functionality of the eAuthentication application.
The IRS values your continued support and the assistance our organization provides.

If you have any questions, please contact me or a member of your staff may contact
John Allen, Director of Risk Management, at (202) 622-1127.

Attachment

Draft Audit Report – While Efforts Are Ongoing to Deploy a Secure Mechanism to Verify Taxpayer Identities, the Public Still Cannot Access Their Tax Account Information Via the Internet (Audit # 201220003) (e-trak #2013-46297)

RECOMMENDATION #1: The Office of the Deputy Commissioner for Services and Enforcement should reprioritize future applications to meet the RRA 98 requirements on or before January 2014. The prioritization will need to be coordinated with the IT organization.

CORRECTIVE ACTION #1: The IRS agrees with this recommendation. We have prioritized future applications based on internal and external stakeholder needs, information technology constraints and safeguards, and requirements such as RRA 98. As the report notes, the Get Transcript application is scheduled to launch in January 2014. This will give taxpayers the ability to view, print and download their tax transcripts. It is the first step toward expanding transcript access on-line. The IRS also plans to increase interactive capabilities and identify additional features associated with an account. Using available resources cost effectively, we will prioritize the rollout of features by delivering the most impactful capabilities first.

IMPLEMENTATION DATE: February 15, 2014

RESPONSIBLE OFFICIAL: Director, Online Services

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

RECOMMENDATION #2: The Associate Chief Information Officer, Cybersecurity, should ensure that capacity testing is adequately performed for the eAuthentication application prior to Release 2 being deployed.

CORRECTIVE ACTION #2: The IRS agrees with this recommendation. The eAuthentication Release 2 project, as already planned, includes performance and capacity testing as part of its Release 2 go-live activities.

IMPLEMENTATION DATE: January 25, 2014

RESPONSIBLE OFFICIALS: Associate Chief Information Officer, Cybersecurity

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

RECOMMENDATION #3: The Associate Chief Information Officer, Cybersecurity, should continue the efforts to acquire appropriate software to enable additional reporting functionality.

CORRECTIVE ACTION #3: The IRS agrees with this recommendation. The eAuthentication Release 2 project, as already planned, includes integration with the existing IRS internal

Draft Audit Report – While Efforts Are Ongoing to Deploy a Secure Mechanism to Verify Taxpayer Identities, the Public Still Cannot Access Their Tax Account Information Via the Internet (Audit # 201220003) (e-trak #2013-46297)

CORRECTIVE ACTION #3: The IRS agrees with this recommendation. The eAuthentication Release 2 project, as already planned, includes integration with the existing IRS internal Business Objects Enterprise (BOE) capability to enable broad Management Information System (MIS) Reporting. This will allow the project to configure the system to produce the following business approved reports -- application specific reports, taxpayer account reports and system infrastructure reports.

IMPLEMENTATION DATE: January 25, 2014

RESPONSIBLE OFFICIAL: Associate Chief Information Officer, Cybersecurity

CORRECTIVE ACTION MONITORING PLAN: We 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 and Chief, Agency-Wide Shared Services, should coordinate to develop a formal system to provide reports of actual costs received and accepted by Contracting Officer Representatives.

CORRECTIVE ACTION #4: While IRS agrees with the spirit and intent of this recommendation, we do not agree with the finding, which was based on an isolated example of a single Contracting Officer's Representative (COR) managing project cost. All Receipt and Acceptance (R&A) transactions are done within the Integrated Procurement System (IPS). A reports module, accessible by all (CORs), allows the COR to track R&A transactions completed for each project. This standard business practice is already being followed at the IRS; thus, no further action is needed.

IMPLEMENTATION DATE: N/A

RESPONSIBLE OFFICIALS: N/A

CORRECTIVE ACTION MONITORING PLAN: N/A