TREASURY INSPECTOR GENERAL FOR TAX ADMINISTRATION

Improved Tax Return Filing and Tax Account Access Authentication Processes and Procedures Are Needed

November 19, 2015

Reference Number: 2016-40-007

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

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

IMPROVED TAX RETURN FILING AND TAX ACCOUNT ACCESS AUTHENTICATION PROCESSES AND PROCEDURES ARE NEEDED

Highlights

Final Report issued on November 19, 2015

Highlights of Reference Number: 2016-40-007 to the Internal Revenue Service Deputy Commissioner for Services and Enforcement.

IMPACT ON TAXPAYERS

The increasing number of data breaches in the private and public sectors means more personal information than ever before is available to unscrupulous individuals. Much of these data are detailed enough to enable circumvention of most authentication processes. As such, it is critical that the methods the IRS uses to authenticate individuals' identities provide a high level of confidence that tax information and services are provided only to individuals who are entitled to receive them.

WHY TIGTA DID THE AUDIT

Failure to adequately authenticate taxpayers filing a tax return and accessing tax account services can lead to identity theft. The increased availability of personal information warrants an assessment of the authentication risk across IRS services. TIGTA performed this audit to assess IRS efforts to authenticate individual taxpayers' identities at the time tax returns are filed and when services are provided.

WHAT TIGTA FOUND

Taxpayers continue to desire electronic products and services that enable them to interact and communicate with the IRS. However, the continued challenge in expanding its portfolio of electronic products and services is that the IRS must ensure that tax account-related information and services are provided only to individuals who are entitled to receive them.

Although the IRS recognizes the growing challenge it faces in establishing effective authentication processes and procedures, it has not established a Service-wide approach to managing its authentication needs. The IRS should establish a function that is optimally placed in the organization and provide it with the authority needed to ensure that authentication policies and procedures are consistent and comply with Government information security standards Service-wide.

The IRS recognizes the need to establish a Service-wide approach to managing its authentication needs and has established two groups that focus on taxpayer authentication. However, neither of these groups provides for cross-functional management, oversight, and continued evaluation of the IRS's existing authentication processes to ensure that they address current and future needs.

In addition, authentication methods used for current online services do not comply with Government Information Security Standards. For example, TIGTA analysis of the e-Authentication processes used to authenticate users of the IRS online Get Transcript and Identity Protection Personal Identification Number applications found that the authentication methods provide only single-factor authentication despite the Government standards requiring multifactor authentication for such high-risk applications. As a result, unscrupulous individuals have gained unauthorized access to tax account information.

WHAT TIGTA RECOMMENDED

TIGTA recommended that the Deputy Commissioner for Services and Enforcement develop a Service-wide strategy that establishes consistent oversight of all authentication needs across IRS functions and programs, ensure that the level of authentication risk for all current and future online applications accurately reflects the risk, and ensure that the authentication processes meet Government Information Security Standards. The IRS agreed to implement all three recommendations.

TREASURY INSPECTOR GENERAL
FOR TAX ADMINISTRATION

DEPARTMENT OF THE TREASURY

WASHINGTON, D.C. 20220

November 19, 2015

MEMORANDUM FOR DEPUTY COMMISSIONER FOR SERVICES AND ENFORCEMENT

FROM: Michael E. McKenney
Deputy Inspector General for Audit

SUBJECT: Final Audit Report – Improved Tax Return Filing and Tax Account Access Authentication Processes and Procedures Are Needed (Audit # 201440016)

This report presents the results of our review to assess Internal Revenue Service efforts to authenticate individual taxpayers' identities at the time tax returns are filed and when obtaining services. This audit was included in our Fiscal Year 2015 Annual Audit Plan and addresses the major management challenge of Fraudulent Claims and Improper Payments.

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

Copies of this report are also being sent to the Internal Revenue Service managers affected by the report recommendations. If you have any questions, please contact me or Russell P. Martin, Assistant Inspector General for Audit (Returns Processing and Account Services).

Table of Contents

Abbreviations

IP PIN	Identity Protection Personal Identification Number
IRS	Internal Revenue Service
NIST	National Institute of Standards and Technology
OMB	Office of Management and Budget
SSN	Social Security Number
TIGTA	Treasury Inspector General for Tax Administration
TIN	Taxpayer Identification Number

Background

Taxpayers continue to desire electronic products and services that enable them to interact and communicate with the Internal Revenue Service (IRS). The IRS Oversight Board's[1] 2014 taxpayer attitude survey reported that 82 percent of taxpayers are likely to use a website, like the IRS public website (www.IRS.gov), to help them comply with their tax obligations. In its most recent Strategic Plan,[2] the IRS acknowledged that the current technology environment has raised taxpayers' expectations for online customer service interactions and it needs to meet these expectations. In response, the IRS continues to expand the information and tools available online to assist taxpayers. The IRS's goal is to provide taxpayers with dynamic online account access that includes viewing their recent payments, making minor changes and adjustments to their accounts in real-time, and corresponding digitally with the IRS to respond to notices or complete required forms.

However, the continued challenge in expanding its portfolio of electronic products and services is that the IRS must ensure that tax account-related information and services are provided only to individuals who are entitled to receive them. For individuals seeking online services, authentication methods consist of three components:

- *Identity Proofing* – The process of collecting and verifying information about an individual for the purpose of issuing credentials, *i.e.*, a username and password, to that individual.
- *Credential Issuance* – Issuing an individual the tools needed to be authenticated by a system such as a user identification number and password.
- *Authentication* – The process of ensuring that the person requesting access is who they say they are by checking the credentials issued to the person after the identity proofing process.

For the purposes of this report, these three processes are collectively referred to as "authentication."

[1] The IRS Oversight Board is an independent body charged with overseeing the IRS in its administration, management, conduct, direction, and supervision of the execution and application of Internal Revenue laws. The Board was created to provide long-term focus and specific expertise in guiding the IRS so it may best serve the public and meet the needs of taxpayers.

[2] IRS Publication 3744, *Internal Revenue Service Strategic Plan – Fiscal Year 2014-2017*, pp. 6-7 (June 2014).

Office of Management and Budget (OMB) guidance *E-Authentication*[3] *for Federal Agencies*[4] establishes criteria for determining the risk-based level of authentication assurance required for specific electronic applications and transactions. The guidance requires agencies to review new and existing electronic transactions to ensure that authentication processes provide the appropriate level of assurance. This guidance is intended to help agencies identify and analyze the risks associated with each step of the authentication process. As the outcome of an authentication error becomes more serious, the required level of assurance increases. The U.S. Department of Commerce National Institute of Standards and Technology (NIST)[5] Special Publication 800-63-2, *Electronic Authentication Guideline*,[6] provides the technical requirements for the four levels of assurance defined in OMB guidance. Figure 1 provides an overview of the technical requirements for the four NIST levels of e-Authentication assurance.

[3] E-Authentication is the process of establishing confidence in user identities electronically presented to an information system.
[4] OMB, M-04-04, *E-Authentication for Federal Agencies* (Dec. 2003).
[5] The NIST is responsible for developing information security standards and guidelines, including minimum requirements for Federal information systems.
[6] NIST, NIST SP-800-63-2, *Electronic Authentication Guideline* (Aug. 2013).

Figure 1: Requirements for E-Authentication Levels of Assurance

Level of Assurance	Requirements	Level of Confidence
Level 1	No identity proofing is required.	Provides little or no confidence.
Level 2	Requires basic identity proofing data,[7] a valid current Government identification number,[8] and a valid financial or utility account number.[9] Access occurs only after identity proofing data and either the Government identification number or financial/utility account number are verified by the agency.	Provides some confidence in the validity of an individual's identity.
Level 3	Requires basic identity proofing data, a valid current Government identification number, and a valid financial or utility account number as well as the use of a second authentication factor such as a one-time supplemental code issued via text message or e-mail to the telephone number or e-mail address associated with the individual.	Provides high confidence in the validity of an individual's identity.
Level 4	Requires in-person identity proofing and verification.	Provides very high confidence in the validity of an individual's identity.

Source: NIST Special Publication 800-63-2 and OMB M-04-04.

IRS e-Authentication framework provides identity proofing for the applications included in the IRS's Service On Demand initiative

The IRS indicated that its e-Authentication framework once fully developed will enable the IRS to require multifactor authentication[10] for all applications that warrant a high level of assurance. The IRS is developing and implementing the e-Authentication framework in four phases referred to as releases. Each release provides additional functionality. The current e-Authentication framework allows for only single-factor authentication.[11] Taxpayers desiring to access IRS online applications are first required to verify their identity through the e-Authentication framework. Figure 2 describes the current single-factor process the e-Authentication framework uses for first-time users of IRS online applications.

[7] Name, address, date of birth, *etc*.
[8] A driver's license number, passport number, *etc*.
[9] A checking or savings account number, credit card account number, tax identification number, *etc*.
[10] Multifactor authentication is a characteristic of an authentication system or a token that uses two or more authentication factors to achieve authentication. The three types of authentication factors are something you know, something you have, and something you are.
[11] Single-factor authentication is a characteristic of an authentication system or a token that uses one of three authentication factors to achieve authentication – something you know, something you have, and something you are.

Figure 2: Current E-Authentication Framework Single-Factor Identity Verification Process for First-Time Users

Verification Steps	Description
E-Mail Confirmation	Individuals enter their first and last names and e-mail address. Prior to verifying their identity, the IRS sends a confirmation code to the e-mail provided by the individual. When they receive the code, they enter it into the appropriate field in the web page and continue with the identity verification process.
Identity Proofing (against IRS records)	The individuals enter their Taxpayer Identification Number (TIN),[12] date of birth, filing status, and address from their most recently filed tax return. This information must match IRS records before the system allows them to go to the next step. If the information provided matches IRS records, they are given the option to create a user identification and password or proceed as a guest.[13] Guest access will require them to re-verify their identity every time they access the system.
Knowledge-Based Authentication	Individuals seeking access to Get Transcript and Identity Protection Personal Identification Number (IP PIN) applications are required to complete this step. Once individuals pass the match against IRS records, they must answer correctly a series of questions in order to further verify their identity. These are questions pulled from their credit report and other data sources via a third-party vendor.
Profile Creation and Credentials Issued (login with user identification and password)	Once a user profile is created, taxpayers will use their username and password to access the system in the future.

Source: Treasury Inspector General for Tax Administration (TIGTA) review of IRS documentation.

Establishing effective authentication processes is a Governmentwide challenge

The need to authenticate individuals requesting benefits and services is a Governmentwide challenge. A number of other Federal agencies have or are in the process of developing innovative processes in an effort to verify the identity of individuals seeking access to Federal benefits and services. For example:

- Centers for Medicare and Medicaid Services Federal Healthcare Exchange – Individuals wishing to use the Exchange will receive a username and password from the Exchange to create an online account at healthcare.gov prior to identity proofing. Individuals must provide name, date of birth, and residential address to complete identity proofing by going online to healthcare.gov or calling the Exchange. In order to submit an application,

[12] A nine-digit number assigned to taxpayers for identification purposes. Depending upon the nature of the taxpayer, the TIN is an Employer Identification Number, a Social Security Number, or an Individual TIN.
[13] Subsequent to the completion of our testing, the IRS eliminated the ability for taxpayers to obtain guest access.

receive an eligibility determination notice, and enroll and obtain insurance, individuals must correctly answer out-of-wallet[14] questions provided by Experian Information Solutions, Inc. (an identity verifier).

Individuals who fail the online identity proofing session are instructed to call the Experian Verification Support Services Help Desk to validate their identity via the telephone. Individuals who are unable to have their identity validated by the Experian Verification Support Services Help Desk via telephone are offered other options to validate their identity such as manual authentication by mailing or uploading documentation.

- Department of Homeland Security *myE-Verify* application – Piloted in October 2014, *myE-Verify* allows individuals, using the Self-Lock feature, to lock their Social Security Number (SSN) so that no one else can use their SSN to get a job with an E-Verify employer,[15] *i.e.*, employment-related identity theft. To establish a *myE-Verify* account, an individual creates a username and password and passes an identity proofing quiz generated by an authentication service. The individual accesses their account using their username and password and also selects a communication channel they have access to for a second identity confirmation – a telephone call, text message, or e-mail message that contains a one-time passcode. As of April 2015, *myE-Verify* is available nationwide and will be available in Spanish in September 2015.

- *Connect.Gov* (formally the Federal Cloud Credential Exchange) – *Connect.Gov* is a Governmentwide identity shared service run by the General Services Administration in partnership with the U.S. Postal Service. *Connect.Gov* allows the public to use a Government-approved, third-party digital credential to securely access online services at multiple agencies.

- General Services Administration *MyUSA.gov* – *MyUSA.gov* is a single-sign on option that will allow users to use one login to access websites from partner agencies and to provide a basic set of services through which agencies can interact with individuals. Individuals establishing an account on *MyUSA.gov* will provide their existing e-mail address and may also provide basic personal identifying information such as name, address, and telephone number. Individuals will not need a new password to log in. *MyUSA.gov* provides level one authentication assurance resulting in very little identity proofing. The benefit of *MyUSA.gov* is to provide individuals with a single access point for a large volume of low level account services. According to General Services Administration representatives, as of July 2015, *MyUSA.gov* and *Connect.Gov* product

[14] Out-of-wallet questions refer to private information.
[15] E-Verify is an Internet-based system that compares information from an employee's Form I-9, *Employment Eligibility Verification*, to data from U.S. Department of Homeland Security and Social Security Administration records to confirm employment eligibility.

efforts were merged to create a single identification authentication shared service for the Federal Government. The *MyUSA.gov* standalone functionality is no longer available to Federal agencies.

This review was performed at the IRS Wage and Investment Division Customer Account Services function in Atlanta, Georgia. In addition, we obtained information from the U.S. Department of Health and Human Services Centers for Medicaid and Medicare Services, the U.S. Department of Homeland Security, the U.S. Postal Service, and the General Services Administration. This review was conducted during the period November 2014 through August 2015. We conducted this performance audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objective. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objective. Detailed information on our audit objective, scope, and methodology is presented in Appendix I. Major contributors to the report are listed in Appendix II.

Results of Review

Authentication Processes and Procedures Do Not Provide Sufficient Assurance That Only Legitimate Individuals Are Filing Tax Returns and Accessing Tax Account Information

Although the IRS recognizes the growing challenge it faces in establishing effective authentication processes and procedures, our review identified that the IRS has not established a Service-wide approach to managing its authentication needs. As a result, the level of authentication the IRS uses for its various services is not consistent. The IRS has a need to authenticate individuals' identities at two primary points of interaction—filing and processing a tax return, and providing account-related services. The IRS offers a number of methods for taxpayers to interact with the IRS, *e.g.*, online, in person, telephone. Different access methods may require different authentication processes. The existence of differing levels of authentication assurance among the various access methods increases the risk of unscrupulous individuals accessing and obtaining personal taxpayer information and/or defrauding the tax system. Unscrupulous individuals can identify the weakest points of authentication and exploit them to inappropriately gain access to tax account information.

Efforts to authenticate individuals filing a tax return are limited to taxpayers affected by identity theft

The only method the IRS uses to attempt to authenticate the identity of the tax return filer, *i.e.*, to ensure that the individual filing the tax return is the legitimate taxpayer, when processing a tax return is through its IP PIN process. The IRS issues an IP PIN to confirmed victims of identity theft as well as to individuals who may be at a high risk for identity theft, *e.g.*, stolen wallet, victim of a non-IRS data breach. Individuals are not issued an IP PIN until they successfully complete the IRS identity proofing processes.[16] The presence of a valid IP PIN on the tax return tells the IRS that the legitimate taxpayer is filing the tax return. According to the IRS, it issued more than 1.5 million IP PINs as of May 2, 2015, for use in filing a tax return during the 2015 Filing Season.

We recently reported that the IRS continues to improve its ability to detect identity theft-related tax returns.[17] However, these processes require a significant number of IRS resources to verify the identity of every potential identity theft victim. A more efficient way to prevent identity theft

[16] An explanation of the IP PIN identity theft proofing processes is provided on page 8 of this report.
[17] TIGTA, Ref. No. 2015-40-026, *Efforts Are Resulting in the Improved Identification of Fraudulent Tax Returns Involving Identity Theft* (Apr. 2015).

from occurring would be to establish a process that verifies the identity of the tax return filer at the time the tax return is accepted for processing. It has been suggested that the IRS expand the IP PIN program to all taxpayers. However, before doing so, the IRS must ensure that the IP PIN program will provide sufficient assurance that the individual who is requesting the IP PIN is who he or she claims to be. The IRS's current use of single-factor authentication processes to obtain access to request an IP PIN or to access an issued IP PIN does not ensure that it is accessible only to the legitimate taxpayer.

Processes used to authenticate individuals requesting access to similar information do not provide a consistent level of authentication assurance

The IRS has developed several methods to authenticate the identity of individuals accessing IRS services. However, we found that the various authentication processes used to gain access to similar information provide differing levels of authentication. For example, the processes the IRS has established to authenticate confirmed victims of identity theft for the purposes of issuing an IP PIN provide varying degrees of authentication assurance depending on how the IP PIN is obtained.

- The IRS directs identity theft victims whose Federal tax records have been affected to complete Form 14039, *Identity Theft Affidavit*, and submit it, by mail or fax, to the IRS along with a photocopy of at least one of four valid Federal or State Government-issued identification, *i.e.*, passport, driver's license, Social Security card, or other valid Federal or State-issued identification, to verify their identity. Once the IRS has verified an individual's identity, the IRS will send the individual a letter with the issued IP PIN for use in filing the next year's Federal tax returns.
- IRS confirmed victims of tax-related identity theft as well as residents of Florida, Georgia, and the District of Columbia have the option of receiving an IP PIN immediately by going online to the IP PIN page and verifying their identity through the e-Authentication framework. However, individuals who are authenticated by the e-Authentication framework are required to provide only basic identifying information and answer knowledge-based questions which can be circumvented by unscrupulous individuals. These individuals do not have to provide a photocopy of a valid Federal or State Government-issued identification.

We identified similar inconsistencies in the level of assurance provided by the processes the IRS uses to authenticate individuals requesting a tax account transcript. Figure 3 describes some of the most common services the IRS offers that require individuals to authenticate their identity before the requested service is provided.

Figure 3: IRS Services Requiring Authentication

Method of Access	Services Offered	Information Required for Authentication
***IRS.gov* and the e-Authentication Framework (Online Services)**	**Get Transcript** – Provides a tax account or tax return transcript for a specific year. **IP PIN** – Provides eligible taxpayers additional protection from the misuse of their SSN on fraudulent Federal income tax returns. **Online Payment Agreement** – Provides individuals the ability to apply for an installment agreement. **Direct Pay** – Provides individuals the option of paying their tax bill or making estimated tax payments directly from their checking or savings account. **Where's My Refund** – Provides refund status information.	TIN, name, date of birth, filing status, and mailing address from most recent tax return. Taxpayer also responds to personal questions, *i.e.*, prior addresses, car loan data, and mortgage information, generated from a third-party credit reporting company. Taxpayer provided tax-related data are matched against data maintained on IRS databases. Personal questions are matched to information provided by a third-party credit reporting company.
Toll-Free Services	**Tax Return, Tax Account Information, and Transcripts** – Individuals can obtain assistance with tax account information and preparation of their tax returns. They can also obtain copies of their tax account transcripts by mail through an automated transcript telephone line.	TIN, first and last name, date of birth, and address. Taxpayer provided tax-related data are matched against data maintained on IRS databases. If information provided does not match, additional questions are asked to verify taxpayer identity.
Walk-In Services (Taxpayer Assistance Centers)	**Tax Account Information** – Individuals can obtain assistance in resolving tax account inquiries and adjustments. **Payments** – Individuals can set up a payment plan and make payments on their tax account.	Government-issued photo identification. If not available, taxpayer provides TIN, first and last name, date of birth, and address. Taxpayer provided tax-related data are matched against data maintained on IRS databases. If information provided does not match, additional questions are asked to verify taxpayer identity.

Source: TIGTA's review of IRS documentation.

While OMB guidance and NIST standards apply to online interactions with individuals, both provide a solid framework that the IRS can use to consistently evaluate the level of

authentication assurance needed when accessing tax-related information. Once an appropriate level of assurance is determined for the tax information being accessed, the IRS can use these guidance and standards to ensure that all of the authentication processes it develops for accessing the same or similar information provide the needed level of assurance regardless of the access method or processes used.

A Service-Wide Strategy Is Needed to Ensure Consistent Oversight of Authentication Efforts

To effectively manage its authentication risk, the IRS should establish a function that is optimally placed in the organization and provide it with the authority needed to ensure that authentication policies and procedures are consistent and comply with Government information security standards Service-wide. The rising number of data breaches in the private and public sectors means that more personal information than ever is available to unscrupulous individuals. The increased availability of personal information necessitates an immediate and ongoing assessment of the authentication risk across the IRS. Appropriate steps to mitigate that risk should be taken to prevent unauthorized access and ensure consistency across all interactions with individuals. While the most reliable method of authenticating individuals is through face-to-face interaction, this method of authentication is burdensome for taxpayers and would require substantial IRS resources.

The IRS must look at all of its authentication and detection needs across IRS functional and program lines including its need to authenticate individuals who file tax returns as well as those who interact with the IRS face-to-face, over the Internet, or on the telephone. The IRS recognizes the need to establish a Service-wide approach to managing its authentication needs and has established two groups that focus on taxpayer authentication. However, neither of these groups provides for cross-functional management, oversight, and continued evaluation of the IRS's existing authentication processes to ensure that they address current and future needs.

The organizational placement of the Authentication Group limits its ability to fulfill its mission

The IRS recognized that there was a lack of consistency in techniques it had employed for authentication. As such, in June 2014, the IRS Wage and Investment Division established the Authentication Group. The Group provides centralized oversight and facilitates decision making for the development and integration of all forms of authentication including frameworks, policies, and processes across the IRS.

Since establishment, the Authentication Group has worked with various IRS functions with authentication responsibilities to improve its e-Authentication process. The Authentication Group has also assessed a number of initiatives including:

- Exploring the use of data analytics to strengthen its ability to authenticate individuals. The Group recognizes that the most effective method for combating identity theft is to use multiple methods to detect and prevent identity theft, including various layers of authentication in combination with detection processes.
- Using a third-party company to pilot face-to-face authentication in order to obtain an IP PIN. The third-party company approached the IRS about conducting the pilot. The Authentication Group provided oversight.
- Using a verification code for submitting Forms W-2, *Wage and Tax Statement*, that will be issued through secure e-mail to employers or payroll providers to enable the IRS to validate electronically submitted Forms W-2. This project was in the developmental stage prior to the formation of the Authentication Group.
- Assessing ways to improve e-Authentication by partnering with the IRS's contracted credit bureau agency to stop fraudsters and identity thieves from passing out-of-wallet questions.

While the Authentication Group is evaluating potential improvements to existing authentication methods for the purpose of preventing identity theft, it is not developing overall strategies to enhance authentication methods across IRS functions and programs. In addition, the Authentication Group is not evaluating new trends and schemes used to commit tax-related identity theft for the purpose of anticipating the IRS's future authentication needs. IRS management stated that it envisioned the Authentication Group would address the IRS's authentication needs Service-wide and acknowledged that while the Authentication Group has made progress, it is not yet achieving its mission.

The Authentication Group has not been provided with the authority to set Service-wide authentication policy

The Authentication Group is not organizationally aligned within the IRS to effect cross-functional change. The Group is part of the IRS Wage and Investment Division, yet other functions across the IRS are responsible for different aspects of taxpayer authentication. For example:

- The IRS's Cybersecurity function is responsible for setting security policy and all of the technology work related to the e-Authentication framework.
- The IRS's Privacy function is responsible for policy related to protecting taxpayer account information from disclosure.
- The Online Services function's role is to work with the IRS business divisions and Information Technology organization to develop web applications and the authentication framework.

The Authentication Group does meet regularly with these functions to identify potential changes to the authentication processes needed in the Wage and Investment Division's programs and services. However, other IRS functions outside of the Wage and Investment Division also have a need to authenticate taxpayers or their representatives which is not addressed by the Authentication Group. In addition, the group is unable to develop and integrate these processes into Service-wide authentication frameworks, policies, and processes.

In April 2015, the Authentication Group requested delegated authority[18] from IRS executives to make limited changes to existing e-Authentication processes, as needed, based on analysis of e-Authentication usage data. IRS executives did not approve its request because they wanted to retain their authority to make authentication decisions.

The Security Summit Authentication Working Group was formed to identify both short-term and long-term solutions to combat identity theft

In March 2015, the IRS developed three working groups focused on combating tax-related identity theft across Federal, State, and private industry. The working groups include representatives from the IRS, State tax agencies, and the tax return preparation industry and are focused on three aspects of tax-related identity theft to find common areas of consensus and identify solutions.

- **Authentication Working Group** – This group was tasked with identifying opportunities for strengthening authentication practices, including identifying new ways to validate taxpayers and tax return information and new techniques for detecting and preventing identity theft refund fraud. The manager of the Wage and Investment Division's Authentication Group participated in this working group.
- **Information Sharing Working Group** – This group was tasked with identifying opportunities for sharing information that would improve the participants' capabilities for detecting and preventing identity theft refund fraud.
- **Strategic Threat Assessment and Response Group** – This group was tasked with taking a look across tax systems and best practices of other industries to identify points of vulnerabilities or risks and develop initiatives and solutions to detect and prevent identity theft refund fraud.

In June 2015, the IRS unveiled a multilayered approach to protect taxpayers from identity theft refund fraud across Federal and State tax systems and a series of recommendations covering six different areas for improvement for the 2016 Filing Season and beyond. These recommendations include efforts to authenticate taxpayers at the time Federal tax returns are filed and sharing of analytical data concerning fraud leads throughout the tax industry. Legislative proposals for Congressional consideration are listed in Appendix IV.

[18] The assignment of responsibility or authority to carry out specific activities.

Establishing a Service-wide approach to managing the IRS's authentication needs is needed to ensure that the Security Summit's Authentication Working Group recommendations and any changes to authentication policy needed Service-wide to prevent future data breaches are properly implemented and monitored both currently and in the future.

Recommendation

The Deputy Commissioner for Services and Enforcement should:

Recommendation 1: Develop a Service-wide strategy that establishes consistent oversight of all authentication needs across IRS functions and programs including all interactions with individuals face-to-face, online, and through the telephone. In addition, the IRS should ensure that responsibility for implementing the strategy is optimally aligned to provide centralized oversight and facilitate decision making for the development and integration of all forms of authentication including frameworks, policies, and processes across the IRS.

> ***Management's Response:*** The IRS agreed with this recommendation. The IRS has created a new position for an executive who will have responsibility for leading the development of this Service-wide strategy, and who will report to the Deputy Commissioner for Services and Enforcement to provide the necessary alignment and oversight of an integrated Service-wide approach.

Authentication Methods Used for Online Services Do Not Comply With Government Information Security Standards

Although the IRS has established processes and procedures to authenticate some tax return filers and individuals requesting online access to IRS services, these processes and procedures do not comply with Government information security standards. In particular, the processes and procedures do not comply with the standards for assessing authentication risk and establishing adequate authentication processes. For example, our analysis of the e-Authentication processes used to authenticate users of the IRS online Get Transcript and IP PIN applications found that the authentication methods provide only single-factor authentication despite NIST standards requiring multifactor authentication for such high-risk applications. As a result, unscrupulous individuals have gained unauthorized access to tax account information.

OMB standards require Federal agencies to conduct an assessment of the risk of authentication error for each online service or application they provide. An authentication error occurs when an agency incorrectly confirms the identity provided by an individual when in fact the individual is not who he or she proclaims to be. In addition, NIST Special Publication 800-63 establishes specific requirements that agencies' authentication processes must meet to provide a specific level of authentication assurance.

For the IP PIN application, an authentication risk assessment was not completed as required

The IRS did not complete an authentication risk assessment of the IP PIN application as required. According to IRS management, a risk assessment was not completed for the IP PIN application because the e-Authentication framework will provide for multifactor authentication once completed. However, the IRS does not anticipate having the technology in place to provide multifactor authentication capability before the summer of 2016. Multifactor authentication requires the use of at least two authentication factors: 1) basic identifying information, knowledge-based questions, and financial-related questions; and 2) a second authentication factor such as a supplemental code that is provided only after the successful verification of the first authentication factor.

While IRS management recognized the IP PIN application required the use of multifactor authentication, they believed that requiring multifactor authentication would further burden identity theft victims who are attempting to obtain an IP PIN. As a result, the IRS decided to implement the online IP PIN application using the single-factor authentication processes currently available through the e-Authentication framework. Had the IRS conducted an authentication risk assessment for the IP PIN application, we believe it would have concluded that the risk to victims and the IRS of having their IP PINs compromised outweighed the potential burden.

For the Get Transcript application, the authentication risk assessement does not accurately reflect the risk of authentication error

The IRS assessed the risk of the Get Transcript application as required. However, the IRS determined the authentication risk associated with Get Transcript was low to both the IRS and taxpayers. The IRS defines a low risk rating as one in which the likelihood of an imposter to obtain and use the information available on the Get Transcript application is low. In addition, a low risk concludes that controls are in place to prevent, or at least significantly impede, an imposter from accessing the information. As a result, the IRS implemented single-factor authentication to access the Get Transcript application. The IRS now knows that the authentication risk was in fact high to both the IRS and taxpayers and should have required multifactor authentication.

Current single-factor, multistep authentication is not multifactor authentication

In testimony before the Senate Finance Committee on June 2, 2015, the IRS Commissioner testified that to access Get Transcript, taxpayers must go through a multistep authentication process to prove their identity. While taxpayers may have to complete multiple steps to authenticate their identity, these steps do not meet the requirements for a multifactor authentication. For example, the IRS requests basic identifying information from individuals seeking access to the Get Transcript application and requires individuals to successfully answer knowledge-based questions provided by a third-party credit reporting agency. The IRS also asks

the individual attempting to access the Get Transcript application to provide an e-mail address to which the IRS sends a confirmation code. While the IRS sends a confirmation code to the individual, this process does not meet the requirements for multifactor authentication because the IRS does not send the confirmation code to the e-mail address on the taxpayer's record nor is it a confirmation code that serves as a second authentication factor to prove an individual's identity (see Figure 2 on page 4).

While single-factor authentication provides some assurance that an individual attempting to access the online Get Transcript and IP PIN applications is the legitimate individual, the information typically required to authenticate an identity can be obtained from other sources. On May 14, 2015, IRS Computer Security Incident Response Center personnel identified a backlog of undeliverable e-mails. These e-mails were the confirmation code e-mails sent to Get Transcript users attempting to establish an account on the Get Transcript application. The IRS identified the undelivered e-mails being sent from suspicious sources. As a result of these unauthorized accesses, the IRS deactivated the Get Transcript application on May 21, 2015.

The IRS reported an estimated 615,000 unauthorized access attempts with an estimated 334,000 that were successful in using the information of victims to obtain a copy of their tax transcript. A successful access is one in which an unauthorized individual successfully answers identity proofing and knowledge-based authentication questions. The information that can be viewed or obtained through the Get Transcript application includes:

- **Tax return information** – available for the current and three prior years and includes most of the line items from a tax return as it was originally filed with the IRS.
- **Tax account information** – available for the current and nine prior years and includes basic account information including return type, marital status, adjusted gross income, taxable income, and payments made.
- **Record of account** – available for the current and three prior years and includes a combination of information from tax return and tax account information.
- **Wage and income** – available for the current and nine prior years and includes data from information returns reported to the IRS, such as Form W-2 and the Form 1099 series of information returns.
- **Verification of nonfiling** – available for the current and three prior years and includes proof from the IRS that the individual did not file a return for the year.

The IRS believes that some of this information may have been gathered to file fraudulent tax returns during the upcoming 2016 Filing Season. Access to this information can enable an identity thief to file a fraudulent tax return that more closely resembles a legitimate tax return making it more difficult for the IRS to detect. Based on these factors, the IRS should have rated the risk associated with the Get Transcript application as high, requiring a NIST level three multifactor authentication before access is granted. An additional concern is that individuals

who successfully create a user account and access the Get Transcript application do not have to re-authenticate their identity to gain access to the IP PIN application.

The IRS current single-factor authentication still does not meet NIST standards

It should be noted that the single-factor e-Authentication framework currently in use by the IRS does not meet NIST standards because it is unable to provide all of the functionality required by NIST standards for single-factor authentication. For example, NIST standards require agencies to obtain basic personal identifying information, a valid current Government identification number, *e.g.*, driver's license, passport number, and a financial or utility account number, *e.g.*, checking account; savings account; utility account; loan, credit card, or tax identification number. In addition, NIST standards also require agencies to confirm that the address, name, and date of birth associated with the Government identification number or financial/utility account number matches the information on the individual's application for access.

However, the IRS's current e-Authentication framework does not require individuals to provide Government identification or a financial or utility account number as required by NIST standards. According to IRS management, the IRS decided to not request financial or utility account information because the information cannot currently be verified. IRS management informed us that the IRS obtained and verified the taxpayer filing status to mitigate the risk of being unable to use financial information to authenticate individuals. Although the IRS required taxpayers to provide a filing status, this does not bring the IRS into compliance with NIST standards and the IRS remains noncompliant with single-factor authentication requirements.

The IRS requires individuals to provide their TIN as a form of Government identification. The IRS verifies the individual's name, date of birth, address, filing status, and TIN. The IRS received guidance from the NIST at the time the e-Authentication framework was being developed indicating that a TIN was an acceptable form of identification. However, in August 2015, the NIST informed us that a TIN is not currently an acceptable Government identification number for the purpose of authentication. We brought this discrepancy to the IRS's attention and IRS management agreed that a TIN is no longer an acceptable form of identification. Management also indicated the IRS would take steps to conform to NIST standards for verifying an individual's identity.

The availability of personal information to unscrupulous individuals increases the need for stronger authentication processes

The IRS's verification of knowledge-based questions in lieu of obtaining and verifying a valid Government identification and financial/utility account information does not make the IRS compliant with NIST standards for single-factor authentication. While the IRS cannot currently verify financial or utility account information, the requirement to obtain this information from individuals, regardless of whether it is verified, can serve as an added deterrent to discourage unscrupulous individuals from attempting to access tax information.

In addition, the requirement to provide financial information and a supplemental code for multifactor authentication is intended to make it more difficult for individuals who are not the legitimate taxpayer to bypass authentication processes. These added requirements can alert the valid taxpayer that someone is attempting to access their personal information, *i.e.*, when an unsolicited code is sent to them. Had the IRS required multifactor authentication, unscrupulous individuals may not have been able to access tax return information through the Get Transcript application.

Challenges exist in implementing the use of financial information and expanding to multifactor authentication

According to IRS management, the IRS will have the technical capability to use financial information to authenticate individuals as early as August 2015. The IRS anticipates it will have the technology to provide multifactor authentication as early as the summer of 2016. However, the IRS faces a number of challenges in being able to implement the use of financial information when authenticating individuals and expanding to multifactor authentication. For example, IRS management informed us that there are contractual issues related to the validation of financial data which need to be resolved before e-Authentication can be approved to operate at a higher level. In addition, once the technology to require financial information and multifactor authentication is available, the IRS still has to develop and implement the business processes needed to use financial information and multifactor authentication. For example, the IRS cannot efficiently and effectively provide a second factor of authentication, such as issuing a one-time code or token, to authenticate the individual's identity because it does not currently communicate with taxpayers via e-mail or text.

As a result, the use of multifactor authentication will require the IRS to send taxpayers the second authentication factor through the traditional mail, delaying access to needed services and negating the efficiency of using online services. The IRS is in the process of exploring secure methods to communicate with taxpayers through e-mail.

The IRS is pursuing a number of options to strengthen the online authentication processes

For more than a year, the IRS Authentication Group has been working collaboratively with functions across the IRS to identify options for strengthening the online authentication process provided by e-Authentication. As a result of the IRS's analysis of the Get Transcript event, the IRS has established controls to prevent concurrent attempts at authentication and increased its monitoring of repeated access attempts. The IRS has also blocked all identified questionable e-mail addresses and is planning to restrict access to one e-mail address per account registration. In addition, the IRS will now send a registration confirmation letter, *i.e.*, confirming the individual created a user account, to the taxpayer's address of record after a user profile has been created using the taxpayer's identity and will continue to do so after Get Transcript is

re-launched. As of July 21, 2015, the IRS had not established a target date for bringing the Get Transcript application back online.

IRS management informed us that the IRS is also evaluating additional options identified by the Authentication Group including a requirement for individuals to answer additional financial questions, requiring a credit card be linked to the user as an additional authentication factor, charging a nominal fee on a credit card for Get Transcript transactions as an additional authentication control, and sending an activation code via mail (and eventually e-mail and/or text message) to taxpayers' address of record after they pass identity proofing online and before allowing access to Get Transcript.

In considering these options, IRS management stated that they must balance strengthened authentication processes with ensuring that legitimate taxpayers are able to access services successfully without excessive burden. According to IRS management, the IRS is still in the process of finalizing its plans for strengthening its online authentication processes. IRS management stated that each new process the IRS implements will be tested and monitored to see how taxpayers respond and whether or not the desired result is being achieved.

Conclusion

No single authentication method or process will prevent unscrupulous individuals from filing identity theft tax returns or attempting to inappropriately access IRS services. However, strong authentication processes can reduce the risk of such activity by making it harder and more costly for unscrupulous individuals to gain access to resources and information. Therefore, it is important that the IRS ensure that its authentication processes are in compliance with NIST standards to provide the highest degree of assurance required and ensure that authentication processes used to verify individuals' identities are consistent among all methods used to access tax account information. NIST standards follow OMB guidance that require the level of authentication provided for electronic or online services be consistent with the risk to a Federal agency should an authentication error occur. Tax account information disclosed to unauthorized individuals can be used by identity thieves to prepare identity theft tax returns that more accurately reflect a valid return increasing the risk that fraudulent returns will not be detected by the IRS.

Recommendations

The Deputy Commissioner for Services and Enforcement should:

Recommendation 2: Ensure that the level of authentication risk for all current and future IRS online applications accurately reflects the risk to the IRS and taxpayers should an authentication error occur.

> ***Management's Response:*** The IRS agreed with this recommendation. The IRS will review the e-Authentication risk assessment process to ensure that the level of

authentication risk for all current and future IRS online applications accurately reflects the risk to the IRS and taxpayers should an authentication error occur.

Recommendation 3: Ensure that the implemented authentication processes used for all current and future online applications provide the level of assurance required by NIST standards for the determined level of authentication risk.

Management's Response: The IRS agreed with this recommendation. The IRS will leverage NIST standards to ensure that implemented authentication processes used for all current and future online applications provide the required level of assurance for the determined level of authentication risk.

Appendix I

Detailed Objective, Scope, and Methodology

Our overall objective was to assess IRS efforts to authenticate individual taxpayers' identities at the time tax returns are filed and when obtaining services. To accomplish this objective, we:

I. Identified and reviewed the methods and controls used by the IRS to authenticate taxpayers.

A. Researched IRS information, the Internal Revenue Manual, and interviewed IRS management and determined the processes in place to authenticate individuals' identity for both electronically filed returns and paper returns.

B. Determined the methods that the IRS uses to authenticate individuals using the *e-Authentication* program as well as taxpayers seeking tax account information using IRS toll-free telephone and walk-in services.

C. Evaluated the authentication processes the IRS is currently using and determined which processes resulted in the IRS verifying identities before a tax return is accepted for processing.

II. Evaluated IRS plans to strengthen authentication procedures.

A. Obtained IRS plans to improve authentication controls used to prevent identity theft tax returns at the time of filing and other authentication controls currently in place. We interviewed IRS personnel, including those in the Wage and Investment Division Authentication Group, and identified authentication procedures being considered, developed, tested, or recently implemented.

B. Determined if taxpayers could obtain a Personal Identification Number from the IP PIN pilot program through the mail or by telephone.

C. Evaluated the current processes the IRS uses to authenticate taxpayers' identities before providing access to IRS services. We evaluated IRS plans to expand or strengthen existing processes used to verify the identity of taxpayers seeking services from the IRS, *i.e.*, e-Authentication, toll-free, walk-in services, as well as those processes used to electronically sign a tax return.

III. Assessed methods used by States and Federal agencies to authenticate individuals.

A. Determined the authentication methods currently used and planned by interviewing representatives from selected States (Georgia, Indiana, Massachusetts, and the District of Columbia) and selected Federal agencies (Centers for Medicare and

Medicaid Services Federal Healthcare Exchange, Department of Homeland Security, General Services Administration, and the *Connect.Gov* initiative).

B. Met with representatives from organizations these State and Federal agencies work with (LexisNexis and Early Warning) and determined the services these organizations provide.

C. Evaluated the *Connect.Gov* program (formally the Federal Cloud Credential Exchange) used to authenticate individuals.

D. Evaluated the *myE-Verify* program used to authenticate individuals.

Internal controls methodology

Internal controls relate to management's plans, methods, and procedures used to meet their mission, goals, and objectives. Internal controls include the processes and procedures for planning, organizing, directing, and controlling program operations. They include the systems for measuring, reporting, and monitoring program performance. We determined that the following internal controls were relevant to our audit objective: the IRS's methods and controls in place to authenticate taxpayers at the time tax returns are processed and when accessing IRS services and plans to strengthen authentication. We evaluated these controls by interviewing IRS management, reviewing current authentication methods, and reviewing authentication methods being developed.

Appendix II

Major Contributors to This Report

Russell P. Martin, Assistant Inspector General for Audit (Returns Processing and Account Services)
Deann L. Baiza, Director
Bill R. Russell, Audit Manager
Wilma Figueroa, Lead Auditor
Sandra L. Hinton, Senior Auditor
Mark V. Willoughby, Senior Auditor
Kimberly Holloway, Auditor

Appendix III

Report Distribution List

Commissioner C
Office of the Commissioner – Attn: Chief of Staff C
Deputy Commissioner for Operations Support OS
Commissioner, Wage and Investment Division SE:W
Director, Office of Online Services SE:OLS
Director, Customer Account Services, Wage and Investment Division SE:W:CAS
Director, Privacy and Policy Compliance OS:P:PPC
Director, Return Integrity and Compliance Services, Wage and Investment Division SE:W:RICS
Director, Cybersecurity Operation OS:CTO:C:O
Chief Counsel CC
National Taxpayer Advocate TA
Director, Office of Program Evaluation and Risk Analysis RAS:O
Director, Office of Audit Coordination OS:PPAC:AC
Office of Internal Control OS:CFO:CPIC:IC
Audit Liaison: Chief, Program Evaluation and Improvement, Wage and Investment Division SE:W:S:PEI

Appendix IV

List of Legislative Proposals for Congressional Consideration

In June 2015, the IRS *2015 Security Summit – Protecting Taxpayers from Identity Theft Refund Fraud* report identified the following six existing legislative proposals for congressional consideration to help fight against identify theft refund fraud:

- *Acceleration of information return (Forms W-2, Wage and Tax Statement, Form 1099 series of information returns, etc.) filing due dates* – Earlier receipt of information returns would enable the IRS to match wage and withholding information before releasing tax return refunds. The proposal would accelerate the filing due date for most information returns to January 31. Currently, most information returns are due by the last day of February after many taxpayers have already filed. As of March 6, 2015, the IRS had received more than 66.7 million tax returns.[1] This prohibits the IRS from effectively matching wage and withholding information prior to releasing tax return refunds.
- *Extending IRS authority to require truncated SSNs on Forms W-2* – Truncated SSNs on Forms W-2 would reduce the unnecessary risk of exposing SSNs to identity theft. Current legislation requires the inclusion of an employee's SSN on Forms W-2. The proposal would revise legislation to require employers to truncate the SSN by replacing the first five digits of the SSN with "x" or "*".
- *Expanded access to the Directory of New Hires* – The proposal would expand IRS access to the National Directory of New Hires database maintained by the Department of Health and Human Services. The database includes employment data and other valuable information for general tax administration purposes and would improve the IRS's ability to identify fraudulent returns at the time the return is processed.
- *Modifying criminal tax penalties for identity theft refund fraud* – The proposal would increase the maximum penalty from three years imprisonment and a $100,000 fine to five years imprisonment and a $250,000 fine. The proposal would also add a $5,000 civil penalty (current law does not impose a civil penalty) on the individual who filed the fraudulent return and would be assessed immediately for each incidence of identity theft.
- *Correctable error authority* – The proposal would permit the IRS to adjust tax returns without performing an audit when the information provided by the taxpayer does not match the information contained in Government databases, the taxpayer has exceeded the

[1] TIGTA, Ref. No. 2015-40-032, *Interim Results of the 2015 Filing Season* p. 3 (Mar. 2015).

lifetime limit for claiming a deduction or credit, or the taxpayer has failed to include documentation with his or her return that is required by statute.

- *Authority to regulate tax return preparers* – Incompetent and dishonest paid tax return preparers potentially subject taxpayers to penalties and interest as a result of incorrect returns and undermine confidence in the tax system. The proposal to regulate paid tax return preparers is designed to promote high quality services, improve voluntary compliance, and foster taxpayer confidence in the fairness of the tax system.

Appendix V

Management's Response to the Draft Report

COMMISSIONER
WAGE AND INVESTMENT DIVISION

DEPARTMENT OF THE TREASURY
INTERNAL REVENUE SERVICE
ATLANTA, GA 30308

NOV 0 3 2015

MEMORANDUM FOR MICHAEL E. MCKENNEY
DEPUTY INSPECTOR GENERAL FOR AUDIT

FROM: Debra Holland
Commissioner, Wage and Investment Division

SUBJECT: Draft Audit Report – Improved Tax Return Filing and Tax Account Access Authentication Processes and Procedures Are Needed (Audit # 201440016)

Thank you for the opportunity to review and comment on the subject draft report. We appreciate your insight on authentication, and as you will see reflected in the attachment, we agree with all of your recommendations and are taking actions to implement them. We also appreciate the information you shared with regard to the efforts of other federal agencies to authenticate identities in their online environments. We reviewed this information and are continuing to work with other federal agencies to identify best practices, leverage information, and identify broader solutions.

As the demand for IRS services increases and resources have diminished, we have been focused on developing strategies to further improve taxpayer service. While we already actively engage with taxpayers across numerous communication channels, we are working diligently to meet taxpayers' increasing demands by expanding the range of self-service options, especially through lower-cost, higher-volume online channels. These options require significant investment to transform our services to secure digital interfaces, while simultaneously strengthening our cybersecurity efforts and expanding identity theft (IDT) work and related activities.

Securing our systems and protecting taxpayers' information is a top priority for the IRS. As criminals become more proficient at obtaining personal taxpayer information, authentication protocols need to be more sophisticated, moving beyond information that used to be known only to individuals, but now in many cases, is readily available to criminal organizations from various sources. We must balance the strongest possible authentication processes with the ability of taxpayers to legitimately access their data and use IRS services online.

In recognition of the critical importance of having a strong, coordinated and evolving authentication framework across the IRS, we have recently created a new position that is tasked with the responsibility for developing our Service-wide approach to authentication. Rene Schwartzman, an executive with almost 30 years of experience, has been chosen for this role, and she will have responsibility to and authority from the Deputy Commissioner for Services and Enforcement (DCSE) on this initiative.

In addition, we have engaged with the U.S. Digital Service (USDS), which uses the best of product design, engineering practices and technology professionals to build effective, efficient and secure digital channels to transform the way government works for the American people. We are joining forces with a team from USDS as we develop the future taxpayer digital experience and the foundational authentication standards that will enable secure digital exchanges between IRS and taxpayers. Rene has been tasked as the IRS lead for this effort, and she will be serving in this critical capacity on behalf of the entire enterprise, keeping the IRS Digital Subcommittee, DCSE and Commissioner apprised about the direction, status and progress of this effort on a regular basis.

To improve our efforts to fight against threats to the entire tax system by criminals who are able to undermine and circumvent authentication protocols, the Commissioner convened a security summit in March with leaders of the electronic tax industry, the software industry and State tax administrators. The group formed a public-private partnership committed to, among other things, working together to fortify authentication defenses and protocols across the board to protect taxpayers and thwart the criminals' access. The effort culminated in several recommendations for the upcoming filing season, which will strengthen authentication at time of filing. The IRS executive tasked with leading this cross-functional effort reports to the Commissioner and the DCSE on this important initiative. The partnership has expanded and is continuing its robust collaboration, because issues such as identity proofing and authentication are never-ending challenges that compel continuous evaluation, since identity thieves have proven to be resourceful and creative in compromising even the best multi-layered controls designed to protect against infiltration.

As noted above, we agree with your recommendations and are taking actions to implement them. We note, however, that we do not agree that the existence of differing levels of authentication assurance among the various access methods increases the risk of unscrupulous individuals accessing and obtaining personal taxpayer information. The National Institute of Standards and Technology (NIST) standards anticipate and require varying levels of assurance depending on the nature of the transaction and the information being exchanged. In addition, there are strong assurance processes easily available in some channels, but not others. For instance, in our Taxpayer Assistance Centers, IRS employees are able to verify the identity of taxpayers with photo identification, which provides a strong degree of authentication assurance; however, that method would not be feasible via Web and telephone interactions. Therefore, both the nature of the service channel and the service need drive variation in authentication

methods. Inconsistencies in the authentication methods/channels lead to favorable results. These inconsistencies actually strengthen authentication and, conversely, forced consistency could weaken it.

We appreciate the audit team accepting the guidance we provided from NIST showing that a Taxpayer Identification Number (TIN) was an acceptable form of identification at the time the e-Authentication framework was being developed. We relied on this guidance at the time of our initial decision regarding use of the TIN as government identification, but have recently learned that the NIST opinion on this matter has changed. Going forward, we will adjust our authentication protocols accordingly. Indeed, the realities of today's cybercriminals and identity thieves – who are constantly evolving, growing in sophistication and increasing their warehousing of stolen personal information – will require us to continually reassess and recalibrate our authentication protocols.

Attached are our comments to your recommendations. If you have any questions, please contact me, or a member of your staff may contact Ivy McChesney, Director, Customer Account Services, Wage and Investment Division, at (404) 338-8910.

Attachment

Attachment

Recommendation:

The Deputy Commissioner for Services and Enforcement should:

RECOMMENDATION 1
Develop a Service-wide strategy that establishes consistent oversight of all authentication needs across IRS functions and programs including all interactions with individuals face-to-face, online, and through the telephone. In addition, the IRS should ensure that responsibility for implementing the strategy is optimally aligned so as to provide centralized oversight and facilitate decision making for the development and integration of all forms of authentication including frameworks, policies, and processes across the IRS.

CORRECTIVE ACTION
We agree with this recommendation, and have created a new position for an executive who will have responsibility for leading the development of this service-wide strategy, and who will report to the DCSE to provide the necessary alignment and oversight of an integrated Service-wide approach.

IMPLEMENTATION DATE
Implemented

RESPONSIBLE OFFICIAL
Deputy Commissioner for Services and Enforcement

CORRECTIVE ACTION MONITORING PLAN
N/A

Recommendations:

The Deputy Commissioner for Services and Enforcement should:

RECOMMENDATION 2
Ensure that the level of authentication risk for all current and future IRS online applications accurately reflects the risk to the IRS and taxpayers should an authentication error occur.

CORRECTIVE ACTION
We agree with this recommendation and will review the e-Authentication risk assessment process to ensure that the level of authentication risk for all current and future IRS online applications accurately reflects the risk to the IRS and taxpayers should an authentication error occur.

IMPLEMENTATION DATE
December 15, 2016

RESPONSIBLE OFFICIAL
Associate Chief Information Officer, Cybersecurity

CORRECTIVE ACTION MONITORING PLAN
We will monitor this corrective action as part of our internal management control system.

RECOMMENDATION 3
Ensure that the implemented authentication processes used for all current and future online applications provide the level of assurance required by the NIST standards for the determined level of authentication risk.

CORRECTIVE ACTION
We agree with this recommendation and will leverage National Institute of Standards and Technology standards to ensure implemented authentication processes used for all current and future online applications provide the required level of assurance for the determined level of authentication risk.

IMPLEMENTATION DATE
December 15, 2015

RESPONSIBLE OFFICIAL
Associate Chief Information Officer, Cybersecurity

CORRECTIVE ACTION MONITORING PLAN
We will monitor this corrective action as part of our internal management control system.