Transcript Delivery System Authentication and Authorization Processes Do Not Adequately Protect Against Unauthorized Release of Tax Information

March 20, 2018

Reference Number: 2018-40-014

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

Redaction Legend:
1 = Tax Return/Return Information
2 = Law Enforcement Techniques/ Procedures and Guidelines for Law Enforcement Investigations or Prosecutions.
3 = Personal Privacy Information.
5 = Information Concerning a Pending Law Enforcement Proceeding

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

1-800-366-4484

By Web:

www.treasury.gov/tigta/

Or Write:

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

Information you provide is confidential and you may remain anonymous.

TRANSCRIPT DELIVERY SYSTEM AUTHENTICATION AND AUTHORIZATION PROCESSES DO NOT ADEQUATELY PROTECT AGAINST UNAUTHORIZED RELEASE OF TAX INFORMATION

Highlights

Final Report issued on March 20, 2018

Highlights of Reference Number: 2018-40-014 to the Internal Revenue Service Commissioner for the Wage and Investment Division.

IMPACT ON TAXPAYERS

The Transcript Delivery System (TDS) allows external third-party customers to view and obtain tax information on both individuals and businesses. Tax transcripts cannot be obtained using the TDS unless a requester successfully registers for e-Services and participates in electronic filing or is a participant of the Income and Verification Express Services (IVES) Program. During Calendar Years 2014 through 2016, a total of more than 168 million tax transcripts were requested.

WHY TIGTA DID THE AUDIT

In June 2016, TIGTA was notified of a potential refund fraud scheme affecting corporations and involving tax transcript information. As a result, this audit was initiated to evaluate the IRS's controls for verifying and validating tax transcript requests through the TDS.

WHAT TIGTA FOUND

TIGTA found that processes and procedures to authenticate e-Services users, including those users accessing the TDS application, do not comply with Federal Government information security standards. The IRS continued to use single-factor authentication to authenticate users even though a risk-assessment in both Calendar Years 2011 and 2015 rated e-Services as requiring multifactor authentication.

In an effort to improve authentication, in November 2016, the IRS implemented an interim process that required existing e-Services TDS users to re-authenticate their identity. However, management did not ensure that e-Services TDS users that did not complete the required interim authentication had their privileges revoked. Our analysis of tax transcript request logs from October 1, 2015, to March 31, 2017, identified 4,022 e-Services TDS users that requested tax transcripts that were not sent a letter to notify them of the new interim authentication requirements. As a result, 1,507 of the 4,022 users continued to request a total of 96,639 tax transcripts without being required to re-authenticate in compliance with the interim requirements.

In addition, tax transcript request processes and procedures do not minimize the risk of unauthorized release of tax transcript information. TIGTA's review of the TDS audit logs of tax transcript requests made between January 1, 2014, and December 31, 2016, identified anomalies that could be either misuse of the system or suspicious activity.

Finally, the IRS has ineffective processes and procedures to ensure that legitimate taxpayers authorized the release of their tax transcript information to IVES Program participants or their clients and that the IRS has delayed actions to reduce unnecessary taxpayer information from being disclosed on tax transcripts.

WHAT TIGTA RECOMMENDED

TIGTA recommended that the Commissioner, Wage and Investment Division, implement multifactor authentication; implement procedures to ensure that legitimate taxpayers authorize the release of their tax transcripts; and redact sensitive information from tax transcripts. TIGTA made six other recommendations to improve controls for requesting tax transcript information.

The IRS agreed with four recommendations. Actions taken by the IRS addressed the underlying concerns of another two. For the remaining three, the IRS did not agree or adequately address the recommendations. The IRS did not agree to implement additional procedures to ensure that legitimate taxpayers authorize the release of their tax transcripts and to improve controls for requesting tax transcript information.

TREASURY INSPECTOR GENERAL
FOR TAX ADMINISTRATION

DEPARTMENT OF THE TREASURY
WASHINGTON, D.C. 20220

March 20 2018

MEMORANDUM FOR COMMISSIONER, WAGE AND INVESTMENT DIVISION

FROM: Michael E. McKenney
Deputy Inspector General for Audit

SUBJECT: Final Audit Report – Transcript Delivery System Authentication and Authorization Processes Do Not Adequately Protect Against Unauthorized Release of Tax Information (Audit # 201640032)

This report presents the results of our review to assess the Internal Revenue Service's controls for verifying and validating tax transcript requests through the Transcript Delivery System. This review was included in our Fiscal Year 2017 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

IRS	Internal Revenue Service
IVES	Income Verification Express Services
NIST	National Institute of Standards and Technology
SSN	Social Security Number
TDS	Transcript Delivery System
TIGTA	Treasury Inspector General for Tax Administration
TIN	Taxpayer Identification Number

Background

In October 2003, the Internal Revenue Service (IRS) began to deploy a suite of web-based products (referred to as e-Services). E-Services allows tax professionals, financial institutions, State taxing authorities, and government entities to conduct business with the IRS electronically.[1] E-Services are available 24 hours a day, 7 days a week, via the IRS's website. One of the products that can be accessed through e-Services since May 2005 is the Transcript Delivery System (TDS). The TDS allows external third-party customers to view and obtain tax information for both individuals and businesses (hereafter referred to as tax transcripts). The TDS is also used by IRS employees to provide tax transcripts to taxpayers who request this information when visiting Taxpayer Assistance Centers or in response to taxpayers requesting tax transcripts by calling the IRS. Figure 1 provides the volume of tax transcript requests processed via the TDS for Calendar Years 2014 through 2016.

Figure 1: TDS Tax Transcript Requests

Calendar Year	Volume[2]
2014	49,519,208
2015	53,955,071
2016	65,439,972
Total	**168,914,251**

Source: Treasury Inspector General for Tax Administration (TIGTA) analysis of IRS TDS data.

Registering for e-Services is necessary to request tax transcript information through the TDS

Tax transcripts cannot be obtained using the TDS unless a requester successfully registers for e-Services and participates in electronic filing or is a participant of the Income and Verification Express Services (IVES) Program. Registering online for e-Services includes the IRS collecting personal taxpayer information to authenticate a user's identity. For example, the following information must be provided to become a registered e-Services user:

[1] The following applications are also accessible through e-Services: Registration Services, Electronic File Application, and Taxpayer Identification Number Matching.
[2] Table includes successfully delivered transcripts excluding transcripts requested via Get Transcript Online.

- Legal name, Social Security Number (SSN), and date of birth. This information is verified using both IRS and Social Security Administration data to ensure that the identity information provided is valid.
- Adjusted Gross Income from the applicant's current year or prior year filed tax return which is verified with the IRS's records.
- Home mailing address which is verified with the IRS's records.
- Telephone number and e-mail address.

If the information provided matches the IRS's and Social Security Administration's data, then the applicant receives an on-screen acknowledgement confirming that they have successfully completed the initial e-Services registration process. For those applicants successfully completing the initial registration process, the IRS mails a registration notice containing a confirmation code to the applicant's address of record.[3] Once the applicant receives the registration notice, they must log back into e-Services within 28 days of the registration submission and enter this confirmation code to complete the registration process.

The IRS offers several ways external third-party customers can request tax transcripts through the TDS and other functions

The following are ways in which tax transcripts can be requested:

- *TDS* – Tax professionals, Electronic Return Originators,[4] Circular 230 practitioners,[5] reporting agents, State and local governments, and IRS employees submit tax transcript requests online to the IRS through the TDS e-Services application. Tax professionals, Electronic Return Originators, Circular 230 practitioners, and reporting agents are also required to submit an application that requires that they undergo additional suitability checks.[6] Once vetted and approved, users must access e-Services online and then access the TDS application to start requesting tax transcripts. Requested tax transcripts are delivered to the requestors by fax, mail,[7] or online via a secure mailbox in the TDS e-Services application.
- *IVES* – Participants complete Form 13803, *Application to Participate in the Income Verification Express Service (IVES) Program*, and undergo suitability checks similar to those for TDS users. Once approved, participants that include banks, mortgage lenders,

[3] The most current address the IRS has on record for a taxpayer where communications can be sent.
[4] The authorized IRS electronic file provider that originates the electronic submission of a return to the IRS.
[5] Individuals who are eligible to practice before the IRS, including attorneys, certified public accountants, enrolled agents, enrolled actuaries, and enrolled retirement plan agents.
[6] Suitability checks may include a criminal background check, credit history check, tax compliance check, and check for prior noncompliance with IRS electronic filing requirements.
[7] Postal delivery can be to the address of record, an alternate address, or to an authorized third party.

and financial institutions submit tax transcript requests by fax or mail using a Form 4506-T, *Request for Transcript of Tax Return*, or Form 4506T-EZ, *Short Form Request for Individual Tax Return Transcript*, signed by the taxpayer (or a person authorized by the taxpayer) for whom the tax transcript is requested. Tax transcripts are delivered to the requestor online via a secure mailbox in the e-Services application. Generally, the IVES participants serve as the intermediary in the process by obtaining the tax transcripts from the IRS and providing them to associated client businesses.

- *Return and Income Verification Services* – Taxpayers submit tax transcript requests by fax or mail using a Form 4506-T or Form 4506T-EZ signed by the taxpayer for whom the tax transcript is requested. Requested tax transcripts are delivered to the requestor by mail.
- *Practitioner Priority Service* – Tax professionals with authorizations (*e.g.*, Power of Attorney)[8] on file with the IRS request tax transcripts by telephone or taxpayers provide verbal consent to IRS employees to release their tax transcript information to the tax professional. Tax transcripts are delivered to the requestor by fax or mail.
- *Toll-Free Telephone* – Taxpayers request their own tax transcript information, tax professionals with authorizations on file with the IRS request tax transcript information for their clients, or taxpayers provide verbal consent to IRS employees to release their tax transcript information to the tax professional. Tax transcripts are delivered to the requestor by fax or mail.

This review was performed at the Wage and Investment Division offices located in Andover, Massachusetts; Covington, Kentucky; and Ogden, Utah, during the period June 2016 through August 2017. 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.

[8] An individual who is authorized to represent a taxpayer before the IRS.

Results of Review

We previously reported[9] that on May 14, 2015, IRS Computer Security Incident Response Center personnel identified a backlog of undeliverable confirmation code e-mails sent to individuals attempting to establish access to the Get Transcript application. The IRS identified that these undelivered e-mails were being sent from suspicious sources. As a result of these unauthorized accesses, the IRS deactivated the Get Transcript application on May 21, 2015. However, despite the IRS's awareness of the risk of online access to tax information, as a result of the Get Transcript data breach, neither immediate nor sufficient actions were taken to reduce the risk of unauthorized release of tax information associated with the TDS application. Only after IRS management became aware of a potential breach to the TDS application in September 2015, some four months after the Get Transcript breach, were actions taken in an effort to strengthen the authentication and authorization controls for gaining access to e-Services and the TDS. Our review of the actions taken found that some were ineffective in minimizing the risk for potential unauthorized release of sensitive tax information due to ineffective management oversight.

The Authentication Method for Accessing e-Services Does Not Comply With Federal Government Information Security Standards

Processes and procedures to authenticate e-Services users, including those users accessing the TDS application, do not comply with Federal Government information security standards. For example, the IRS continues to use single-factor authentication to authenticate users despite the IRS performing a risk-assessment, in both Calendar Years 2011 and 2015, rating the level of assurance at a Level 3.[10] Level 3 means authentication should provide a high confidence in the validity of an individual's identity and the only way to provide this level of confidence is by having users complete multifactor authentication.

Office of Management and Budget guidance, *E-Authentication*[11] *Guidance for Federal Agencies*,[12] establishes criteria for determining the risk-based level of authentication assurance required for specific electronic applications and transactions. As the outcome of an authentication error[13] becomes more serious, the required level of assurance increases. The

[9] TIGTA, Ref. No. 2016-40-007, *Improved Tax Return Filing and Tax Account Access Authentication Processes and Procedures Are Needed* (Nov. 2015).
[10] See Figure 2: Requirements for E-Authentication Levels of Assurance.
[11] E-Authentication is the process of establishing confidence in user identities electronically presented to an information system.
[12] Office of Management and Budget, M-04-04, *E-Authentication Guidance for Federal Agencies* (Dec. 2003).
[13] 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.

U.S. Department of Commerce National Institute of Standards and Technology (NIST)[14] Special Publication 800-63-2, *Electronic Authentication Guideline*,[15] provides the technical requirements of the four levels of assurance defined in the Office of Management and Budget guidance. Figure 2 provides an overview of the technical requirements of the four NIST levels of e-Authentication assurance.

Figure 2: 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,[16] a valid current Government identification number,[17] and a valid financial or utility account number.[18] 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 Office of Management and Budget M-04-04.

When we discussed noncompliance with NIST standards with IRS management, they indicated that they originally had intended to have e-Services, including the TDS application, use the same multifactor authentication processes that were implemented in May 2016 in response to the Get Transcript breach. However, IRS management indicated that during the testing of implementing multifactor authentication for e-Services, the IRS identified unexpected barriers. These barriers included that other IRS applications would be impacted by the implementation of multifactor authentication requirements, and the IRS needed additional time to identify a solution. In addition, external stakeholders raised concerns that users would not be able to receive the

[14] The NIST is responsible for developing information security standards and guidelines, including minimum requirements for Federal information systems.
[15] NIST, NIST SP-800-63-2, *Electronic Authentication Guideline* (Aug. 2013).
[16] Name, address, date of birth, *etc.*
[17] A driver's license number, passport number, *etc.*
[18] A checking or savings account number, credit card account number, tax identification number, *etc.*

confirmation codes via text message because some businesses do not allow employees to have their personal cellphones at work. Therefore, management indicated that they proceeded with implementing an interim solution. Management stated that they were not foregoing the implementation of multifactor authentication, but rather were ensuring a successful implementation for both the IRS and its external stakeholders.

The IRS recently announced plans to migrate to Secure Access (*i.e.*, multifactor authentication)[19] for e-Services by the end of October 2017. In an August 30, 2017, update to e-Services users, the IRS stated the following, "this two-factor authentication makes it much harder for cybercriminals to takeover users' accounts, which puts taxpayer data at risk. In recent years, cybercriminals have targeted e-Services users, especially in the tax preparation community, in an effort to steal usernames and passwords." In light of the recent Equifax data breach, in which personally identifiable information for about 143 million individuals was stolen, it is of utmost importance that the IRS timely and successfully migrates to multifactor authentication for e-Services to ensure against unscrupulous individuals compromising this system to gain unauthorized access to tax information. As such, we will be monitoring and evaluating the IRS's response to this data breach and the impact it might have on the IRS's implementation of multi-factor authentication for e-Services.

Management did not ensure successful implementation of interim authentication requirements

In an effort to improve authentication, the IRS implemented an interim process that required existing e-Services TDS users to re-authenticate their identity. These interim requirements subjected existing e-Services TDS users to more rigorous identity proofing. It should be noted that although these interim requirements strengthened identity proofing they still did not meet the standard for multifactor authentication as required by NIST.

On November 29, 2016, the IRS published an important update about e-Services on its public website[20] that notified TDS users that they would receive letters by mail with instructions on how to re-authenticate their identity. During the first two weeks of December 2016, the IRS sent letters to TDS users that requested tax transcripts or updated their e-Services account between October 2015 and November 2016. The IRS considers these users to be active users. These letters instructed the users that re-authentication was required to be completed within 30 days or access to e-Services would be revoked. Users were provided with three options to re-authenticate:

[19] A rigorous identity-verification process that helps protect taxpayer data and IRS systems from automated cyberattacks. Before accessing certain IRS online self-help tools, users must first register through Secure Access and authenticate their identities. Thereafter, each time registered users return to the tool, they must enter both their credentials (username and password) plus a security code sent via mobile phone text. The Get Transcript application is one of the online tools that utilizes Secure Access authentication.
[20] www.IRS.gov.

- Visit www.irs.gov/transcript and complete the "Get Transcript Online" registration process by following the prompts and entering information as requested. Information requested to be entered includes the user's Taxpayer Identification Number (TIN),[21] name, date of birth, filing status, and mailing address used on their most recent tax return. Users were also required to provide a personal account number, such as from a credit card or loan, and a U.S.-based, text-enabled mobile phone number to complete the authentication process.
- Call the e-Services Help Desk with the notification letter in hand. The users would then have to answer a series of basic identity-proofing questions along with providing the unique security code located on the first page of the letter. Once the security code was provided the user would then have to answer additional verification questions to re-authenticate their identity.
- Visit an IRS Taxpayer Assistance Center and verify their identity in person.

Our analysis of tax transcript request logs from October 1, 2015, to March 31, 2017, identified 4,022 e-Services TDS users that requested tax transcripts that were not sent a letter to notify them of the new interim authentication requirements. This occurred because management did not ensure that all users were identified and sent notification letters. As a result, 1,507 of the 4,022 users continued to request a total of 96,639 tax transcripts without being required to re-authenticate in compliance with the interim requirements; consequently, tax account information for 17,792 taxpayers was disclosed without proper authorization. When we brought our concerns to IRS management's attention, they could not explain why the 4,022 users were excluded from receiving notification of the interim authentication requirements and indicated that they would ensure that these users would be notified.

Management did not ensure that e-Services TDS users that did not complete the required interim authentication had their privileges revoked

Our review identified 138 users (134 IVES participants and four Electronic Return Originators) that failed to re-authenticate, but their access to e-Services was not revoked as required. Subsequent to the February 5, 2017, date on which these users should have been revoked, these 134 IVES participants requested 29,163 tax transcripts and the Electronic Return Originators requested 16 tax transcripts. These transcripts were requested from February 6, 2017, to April 30, 2017. When we brought to management's attention that the 138 users that should have been revoked had requested tax transcripts, IRS management noted that although the transcripts were requested these users may not have accessed their secure mailboxes to retrieve the requested transcripts. After repeated requests, the IRS has not provided any information that

[21] The TIN is a nine-digit number assigned to taxpayers for identification purposes. Depending upon the nature of the taxpayer, the TIN is an Employer Identification Number, an SSN, or an Individual TIN.

would support their assertion that these users in fact did not retrieve the tax transcripts. Figure 3 provides a breakdown of the e-Services users interim authentication.

Figure 3: E-Services TDS Users Authentication Results

TDS Users Required to Authenticate	TDS Users Notified
Total TDS Users	145,905
Completed Authentication	75,815
Did Not Complete Authentication	70,090
Revoked/Did Not Request Tax Transcripts	69,952
Not Revoked/Requested Tax Transcripts[22]	138

Source: TIGTA's analysis of IRS's e-Services Authentication data as of February 5, 2017.

During subsequent conversations with the IRS management, they advised us that their authentication efforts continued after February 5, 2017, and as of August 26, 2017, a total of 90,571 TDS users had completed authentication.

Recommendations

The Commissioner, Wage and Investment Division, should:

Recommendation 1**:** Send notification letters of interim authentication requirements to the 4,022 e-Services TDS users not notified and revoke access privileges for any users that do not complete the interim authentication requirements.

> ***Management's Response:*** The IRS disagreed with this recommendation. IRS management responded that the Level of Assurance 3 standards for the TDS application were deployed on December 10, 2017. All TDS users, including the 4,022 that did not receive interim authentication notification letters, are required to re-authenticate.
>
> ***Office of Audit Comment:*** Because all e-Services users, including TDS users, are required to re-authenticate at the Level of Assurance 3 standard, a separate notification to the 4,022 TDS users is no longer necessary. However, it should be noted that the IRS implemented these new requirements subsequent to the completion of our audit. As such,

[22] TIGTA analysis of TDS transcript request data from February 6, 2017, through April 30, 2017.

we cannot comment on the adequacy of the re-authentication process and confirm if all e-Services users were denied access to the system if they did not re-authenticate.

Recommendation 2**:** Implement multifactor authentication for e-Services, which includes the TDS application, to comply with Federal Government Information Security Standards.

Management's Response: The IRS agreed with this recommendation. IRS management implemented the multifactor authentication for the TDS application on December 10, 2017.

Tax Transcript Request Processes and Procedures Do Not Minimize the Risk of Unauthorized Release of Tax Transcript Information

Our review of the processes that e-Services TDS users or taxpayers can complete to request and obtain tax transcripts identified that, other than requests made in person at a Taxpayer Assistance Center, the IRS cannot confirm with certainty that a taxpayer actually authorized the release of their tax information. The IRS is responsible for protecting taxpayer's data from unauthorized disclosure and, as such, needs to ensure that taxpayers in fact authorize the release of their tax information. The IRS has the authority to disclose taxpayer return information to a third party designated by the taxpayer. However, the taxpayer's signature or authorized person's signature must be on the request document in order to provide authorization for disclosure. In addition, the taxpayer's information may be provided only to a third party whose name and address is listed on the properly signed authorization.

The personal information (*i.e.*, TIN, name, address) required to be included in support of a tax transcript request can be readily obtained by unscrupulous individuals. Once obtained, a fraudster can use the personal information along with a falsified signature to fraudulently request taxpayer information. The IRS cannot verify the authenticity of the authorization prior to the release of an individual's tax transcripts. Figure 4 summarizes the methods for requesting tax transcripts other than in person at a Taxpayer Assistance Center, requirements to gain access to the system, and if the process the IRS uses minimizes the risk of potential unauthorized release of tax information.

Figure 4: Methods for Requesting Tax Transcripts and Level of Risk of Unauthorized Disclosures

System	Information Required to Authenticate	Risk of Potential Unauthorized Disclosure?
TDS	Register online for e-Services by providing basic identifying information such as SSN, name, date of birth, filing status, and mailing address from most recent tax return. Users must also submit an e-file application, pass a suitability check, electronically file five or more tax returns, and have the proper authorizations on file.	Yes – Multifactor authentication has not fully been implemented. In addition, ******5******* **********5********** **********5********** **********5********** *******5*******.
IVES	Register online for e-Services by providing basic identifying information such as SSN, name, date of birth, filing status, and mailing address from most recent tax return. Users must also submit an IVES application, and complete and fax Forms 4506-T or 4506T-EZ.	Yes – New certification requirements are not effective. In addition, the IRS does not have processes and procedures to ensure that the legitimate taxpayer in fact signed Form 4506-T to authorize the release of their tax transcripts.
Return and Income Verification Service	Complete and mail or fax a signed Form 4506-T or 4506T-EZ.	Yes – The IRS does not have processes and procedures to ensure that the legitimate taxpayer in fact signed Form 4506-T to authorize the release of their tax transcripts.
Practitioner Priority Service	Authorizations to request and receive taxpayer information must be on file. If not on file, they must be faxed to the IRS or taxpayer verbal consent must be given during the call. Identifying information must be given and match the IRS's records. Additional information can be requested, if warranted, but is not common.	Yes – The IRS verifies limited authentication information before releasing tax transcripts. In addition, we have ****2 and 5********** **********2 and 5********** **********2 and 5********** **********2 and 5********** **********2 and 5**********.[23]

[23] **********2********** **********2********** **********2********** **********2**********.

System	Information Required to Authenticate	Risk of Potential Unauthorized Disclosure?
Toll-Free	If the taxpayer is calling about their own account, verification includes TIN, name, filing status, date of birth, copy of tax return, and letters/notices from the IRS. If a third party is calling, verification includes verbal or written authorization from taxpayer, TIN, name, and proper authorization (*i*.e., Form 2848, *Power of Attorney and Declaration of Representative*, or Form 8821, *Tax Information Authorization*).	Yes – The IRS verifies limited authentication information before releasing tax transcripts.

Source: TIGTA's analysis of the IRS's Internal Revenue Manual procedures.

Tax transcript information provides key taxpayer data that can be used to file fraudulent tax returns to obtain a refund

Tax transcripts, if obtained by unscrupulous individuals, provide valuable tax information that can be used to prepare and file fraudulent tax returns. Tax transcripts available via TDS include:

- *Account Transcript* – Provides financial tax account information such as payments made, penalty assessments, and adjustments made by the taxpayer or the IRS after a tax return was filed.
- *Return Transcript* – Provides information relating to most of the line items from a filed tax return.
- *Record of Account* – Provides the most detailed tax account information as it is a combination of the Account Transcript and Return Transcript.
- *Wage and Income Transcript* – Provides data from information returns such as Forms W-2, *Wage and Tax Statement;* Forms 1099, income series; Forms 1098, expense series; or Form 5498, *IRA*[24] *Contribution Information*.
- *Verification of Non-Filing* – Provides confirmation that a taxpayer did not file a return for a specific requested tax year.[25]

Although we are unable to conclusively determine that a tax transcript was not requested by the legitimate taxpayer or their representative, our comparison of tax transcript requests to tax returns identified by the IRS as fraudulent, raises concern as to the potential improper use of the

[24] IRA = Individual Retirement Account.
[25] A 12-month accounting period for keeping records on income and expenses used as the basis for calculating the annual taxes due. For most individual taxpayers, the tax year is synonymous with the calendar year.

TDS. Our comparison of Tax Years 2013 through 2016 tax transcript requests to taxpayer accounts that had confirmed identity theft found that 430,000 taxpayer accounts had a total of 1,472,369 tax transcripts requested for the tax year prior to the tax year with confirmed identity theft. In addition, we found 222,534 taxpayer accounts had a total of 647,208 tax transcripts requested for the same tax year as the tax year with confirmed identity theft.

In addition, on June 1, 2016, we were notified of a refund fraud scheme affecting corporate taxpayers whereby ********** 2 and 5********** ********** 2 and 5*********. For this corporate fraud scheme, **********2 and 5**********.[26] **** 2 and 5******** **********2 and 5********** **********2 and 5********** **********2 and 5********** **********2 and 5********** **********2 and 5********** **********2 and 5**********.

[26] At the request of a corporation, manual refunds can be issued by paper check or electronically deposited into an account at any bank or other financial institution such as a mutual fund, credit union, or brokerage firm.

Figure 5: **********2********

****
****
****
****
****
****
********** 2 **********
****
****
****
****
****
****

Source: TIGTA created hypothetical example.

Figure 6: **********2********

****

****

****

****

********** 2 **********

****

****

****

****

Source: TIGTA created hypothetical example.

On June 9, 2016, we notified IRS management of our concerns with the processing of ***2*** requests.[27] In response, the IRS immediately suspended processing of these refund requests until it could put additional safeguards in place. On July 1, 2016, new procedures were implemented that included an IRS employee contacting the corporation to verify submission of the ****2***.

On July 21, 2016, subsequent to our reviewing the new procedures, we expressed concerns about the process of calling the taxpayer twice prior to making a determination about the validity of the ***2***. We suggested that the IRS send a letter directing the taxpayer to contact the IRS to confirm the submission of their refund request on ***2***. The IRS agreed and implemented this new process. Further, the IRS created a spreadsheet to track, monitor, and quantify the results of reviewing the ***2*** it received for processing. As of June 30, 2017, the IRS rejected[28] and held from processing 349 ***2*** refund requests totaling more than $1 billion. In addition, the IRS's Criminal Investigation function confirmed 17 refund requests as fraudulent and stopped or recovered refunds totaling more than $49.9 million. Because the IRS

[27] We identified 15 ***2*** were submitted with refund requests totaling $40.3 million.
[28] Reasons for rejection included: returns had indicators of fraud, tax return already filed, form filed too late, duplicate form filed, unable to contact taxpayer, and unable to verify amounts reported on ***2***.

implemented corrective actions during the audit, we are not making any additional recommendations.

Tax transcript request audit logs provide further indications of potential misuse of the TDS

Our review of the TDS audit logs of tax transcript requests made between January 1, 2014, and December 31, 2016, identified the following anomalies that could be an indication of either misuse of the system or potentially suspicious activity:

- ***********************************3********************************* of the more than 51 million total tax transcripts requested by this segment of users. We provided this information to IRS management and they informed us that *****3***** uses data scraping programs to automate the tax transcript request process, thereby mimicking human interaction. Management further stated that they do not prohibit TDS participants from using this type of technology.

  There is currently no limit on the number of tax transcripts that can be obtained by a TDS participant for the same taxpayer. For example, seven unique TDS users requested tax transcripts for 58 unique taxpayers ranging from 10,000 to almost 48,000 for each taxpayer. This indicates that these seven TDS users may be using similar data scraping programs as the *********3********** previously discussed. IRS management indicated that they are currently monitoring the use of this type of technology among their TDS users, but there are no plans to limit its use. The IRS believes that changing its policy would compromise its customers' business model. Management's rationale as to disrupting a business model whereby ******************3********************* *****3***** and others request more than 10,000 tax transcripts for the same taxpayer is highly problematic and it results in a failure to mitigate the risks associated with these types of users.

- From Calendar Year 2014 to Calendar Year 2016, the IVES program experienced an approximate 135 percent increase in the volume[29] of Wage and Income Transcript requests. As previously discussed, *******************2********************** ***********************************2************************************** ***********************************2************************************** ***********************************2************************************** ***********************************2************************************** ***********************************2************************************** ***********************************2************************************** *********2**********.

[29] The volume increased from 3,224,129 in Calendar Year 2014 to 7,571,467 in Calendar Year 2016.

- There were 169 TDS participants and three IVES participants that registered with e-Services using e-mail addresses that had been identified during our previous Get Transcript audit[30] as suspicious, and associated with potential identity theft victims.

Recommendations

The Commissioner, Wage and Investment Division, should:

Recommendation 3**:** Implement processes and procedures to ensure that legitimate taxpayers authorize the release of their tax transcripts. In addition, discontinue offering tax transcripts via those processes in which the IRS cannot confirm whether legitimate taxpayers authorized the release of their tax transcripts.

> ***Management's Response:*** The IRS agreed with this recommendation. IRS management established new certification requirements for IVES participants on June 30, 2016. These requirements included more rigorous steps for IVES participants to verify the legitimacy of clients and individuals requesting transcripts. The e-Services suite of applications is now protected by Secure Access Authentication so all IVES participants are behind a two-factor authentication process. IRS management also plans to continue to evaluate the effectiveness of their process and determine where improvements can be made.

Recommendation 4: Implement processes and procedures that prevent the use of data scraping programs to request tax transcripts.

> ***Management's Response:*** The IRS disagreed with this recommendation. IRS management responded that neither TIGTA's nor their analysis has identified illegitimate transcript requests associated with the use of data scraping programs. The TDS application uses protective analytics that monitors system activity to detect anomalous activity. IRS management has not seen any evidence of increased fraud risk involving this retrieval technique and preventing the use of the technique would adversely affect IVES participants and the taxpayers they represent without a compelling reason for doing so.
>
> ***Office of Audit Comment:*** Management's continued assertions that it does not want to prevent the use of data scraping programs because it would adversely affect IVES participants' business models is problematic given that it has a responsibility to protect taxpayer information. Continuing to allow data scraping programs to request an unlimited number of tax transcripts unnecessarily puts taxpayer information at risk.

[30] TIGTA, Ref. No. 2016-40-037, *The Internal Revenue Service Did Not Identify and Assist All Individuals Potentially Affected by the Get Transcript Application Data Breach* (May 2016).

Requests via the Income and Verification Express Services Presents the Greatest Risk for Unauthorized Release of Tax Transcript Information

Our review identified that the IRS has ineffective processes and procedures to ensure that legitimate taxpayers in fact authorized the release of their tax transcript information to IVES participants or their clients. As discussed previously, the IRS is responsible for protecting taxpayer's data from unauthorized disclosure. IVES participants frequently are intermediaries in the transcript request process as they obtain the tax transcripts from the IRS and provide them to associated client businesses. As early as September 2015, IRS management was aware of the risk associated with the unauthorized release of taxpayer information via the IVES Program. However, management took little action to address these risks, and when actions were ultimately taken, they were not always effective. For example, **********1**********
**********1**********
**********1**********
**********1**********
**********1**********
**********1**********
*******1*******.

On September 30, 2015, IRS Executives were briefed on this incident and discussions ensued to identify actions that would be taken to reduce the risk of unauthorized disclosure of taxpayer information via the IVES. These actions included the IRS adding ****1**** to their dynamic selection list[31] and notifying its Criminal Investigation function. However, management's overall position with regard to the unauthorized release of this tax data was that the IRS did not release the tax information so there were no actions its Privacy, Governmental Liaison, and Disclosure function staff needed to take. We disagree. Management's untimely actions to address poor authentication controls directly contributed to this disclosure. Figure 7 shows a timeline of the subsequent actions taken by IRS management to address this breach.

[31] A list of taxpayers impacted by a data breach which is used to identify potentially fraudulent tax returns resulting from the breach.

Figure 7: Timeline of IRS Actions Taken to Address IVES Breach

Date	Action Taken
10/7/2015	A meeting was held to discuss treatment of the tax accounts involved in breach (*i.e.*, identity theft markers, sending letters). The IRS also acknowledged the need to create a formalized process for IVES participants to alert the IRS of similar concerns as well as the need to establish a protocol for remedy when an incident occurs.
12/22/2015	The IRS notified IVES participants via e-mail that a dedicated e-mail account[32] was established for reporting suspicious activity or concerns about a potential loss of taxpayer data due to any unauthorized access to systems.
4/4/2016	A meeting was held to discuss additional actions that needed to be taken to strengthen the IVES program, including: Improved procedures. More rigorous application process. Quarterly meetings with IVES participants. Cross-training of employees to assist when volumes increase.
6/23/2016	IVES certification process was implemented.

Source: TIGTA's analysis of IRS IVES data.

As noted in Figure 7, in December 2015, the IRS established an e-mail box for IVES participants to report suspicious activity. The IRS provided us with eight suspicious activity e-mails that were received from IVES participants between December 2015 and December 2016. Highlights from some of the e-mails include:

- **********1 and 5**********
  **********1 and 5**********
  **********1 and 5**********
  **********1 and 5**********
  **********1 and 5**********
  1 and 5.
- **********1 and 5**********
  **********1 and 5**********
  **********1 and 5**********
  **********1 and 5**********

[32] wi.ives.participant.assistance@irs.gov.

**********1 and 5**********
1 and 5.

- **********1 and 5**********
**********1 and 5**********
**********1 and 5**********. The IRS's procedures for a rejected tax transcript request includes sending a letter to the taxpayer, along with a copy of the Form 4506-T. **********1 and 5**********
**********1 and 5**********
**********1 and 5**********
**********1 and 5**********
**********1 and 5**********.

- **********1**********
**********1**********
**********1**********
**********1**********
**********1**********
**********1**********.

It should be noted that our analysis of the e-mails submitted by IVES users was limited to what the IRS provided. We were unable to independently identify the volume of e-mails sent to the suspicious activity e-mail account. When we requested access to this e-mail account, IRS management indicated that once e-mails are received they are forwarded to an IVES analyst for review and then deleted from the suspicious activity e-mail account. As such, we were unable to independently identify the exact volume of reported suspicious activity to the IRS since the inception of the mailbox in December 2015. On May 10, 2017, we notified the IRS of our concerns with these practices. In response, IRS management stated that as of May 16, 2017, e-mails received reporting suspicious IVES activity are no longer being moved or deleted from the mailbox.

The examples provided clearly show that there were indications that additional safeguards needed to be put in place to prevent the potential unauthorized release of taxpayer information through the IVES program. IRS management was aware of the suspicious activity as early as September 2015, but took no action to reduce risks until June 2016 when they implemented new certification requirements for IVES participants that still does not ensure that a legitimate taxpayer in fact authorizes the release of their tax transcripts to an IVES participant or their associated clients.

IVES certification processes were ineffective in addressing risks associated with the unauthorized release of tax transcripts to IVES clients

On June 23, 2016, e-mail communications were sent to IVES participants detailing new certification requirements they were to follow to verify and validate the identity of their clients for whom they requested tax transcripts. Each participant was required to complete the following self-attestation statements by the date specified in order to receive tax transcripts:

- ***Certification #1*** – Effective June 23, 2016, IVES participants were required to certify that they have policies and procedures in place to validate the identities of a *new clients'* President, Chief Executive Officer, or other officer who can legally bind the client. In addition, participants must certify the *new client* has procedures and policies in place to validate the identities of all individuals authorized to submit and retrieve IRS tax transcripts on behalf of a taxpayer. This certification must be completed prior to submitting any tax transcript requests for new clients.
- ***Certification #2*** – Effective July 15, 2016, IVES participants must certify that *existing clients'* identities have been verified, unique usernames and passwords for each authorized individual have been provided, tax transcripts are delivered only to authorized individuals and validated destinations, evidence of verifications of identities is retained for a minimum of five years, and any suspected fraudulent activity is reported to the e-mail address designated by the IRS. In addition, participants must certify they will submit tax transcript requests for *existing clients* only when the participant has re-verified the identity of the corporate officers and verified that the client has policies and procedures to validate the identities of all individuals authorized to submit and retrieve tax transcripts. IRS management extended the deadline to September 15, 2016, and disabled participants that failed to meet the requirements by that date.
- ***Certification #3*** – Effective August 7, 2016, IVES participants must certify *all new and existing clients* by ensuring accounts are locked after three failed attempts to log in, ensuring the e-mail address of each client is verified, and providing documentation of the implementation of these security controls.

These certifications are self-attestations and required no supporting documentation be provided to the IRS to allow for independent verification that an IVES participant is in fact complying with these requirements. For example, if a participant attested they verified the identity of all 50 of their clients, the IRS would have **********2********** **********2********** **********2**********.

Management did not ensure successful implementation of IVES certification requirements

Our comparison of a list of 3,301 IVES participants from the IRS's Information Technology organization to a list of 1,733 IVES participants that were sent an e-mail notification of the new certification requirements on June 23, 2016, identified 1,568 (47.5 percent) IVES participants that were not even notified by the IRS of the new certification requirements previously discussed. This occurred because the IRS's records for notifying IVES participants were incomplete and the IRS did not reconcile those records with the actual IVES participant list to ensure that all participants were accounted for prior to issuing the letters. Although 212 of the IVES participants certified without being notified, further analysis found that 1,356 (86.5 percent) of the 1,568 had not certified by the required deadline of September 15, 2016.

In addition to management not ensuring all IVES participants were notified, the IRS did not properly disable the TDS access for two IVES participants that did not complete the required certifications. These IVES participants requested and received a total of 10 tax transcripts. As of September 24, 2016, we found that of the 1,733 IVES participants that were notified, 1,412 (81 percent) did not complete the certification by September 15, 2016, and were disabled. When we brought our concerns to IRS management's attention, the IRS agreed that the 1,356 users we identified that were not notified and did not complete the required certification were inappropriately excluded from the notification process. The IRS also stated that although the applicant's status was not considered as a factor in the notification of the new certification requirements sent to the IVES participants, it was important to note that 691 of the 1,356 were not in an active status as of June 24, 2016, and were consequently not required to be notified. This response contradicts IRS's previous statement to us that ***all*** IVES participants, regardless of their status, would be notified of the new requirements.

Processes to evaluate compliance with the new certification requirements were not timely implemented and do not address all participants

The June 2016 IVES certification procedures stated that all IVES users needed to maintain a list of all authorized users submitting and retrieving IRS tax transcripts on behalf of clients. When we asked the IRS in July 2016 how it planned to ensure compliance with this requirement and the other certification procedures, management indicated that they had not yet developed processes for ensuring IVES user compliance. We followed up with management in March 2017 and again asked about plans for ensuring that IVES participants complied with the new requirements. IRS management indicated they were developing a compliance review process. In May 2017, the IRS provided the final Compliance Review Letters that were approved by Chief Counsel, and subsequently sent letters to a judgmental sample of 70 IVES participants with a response date of 30 days later. As of August 4, 2017, the IRS had received 62 responses and found 29 to be in compliance. For the remaining responses, the IRS is still evaluating each response to determine if the IVES user is in compliance with program requirements.

Recommendations

The Commissioner, Wage and Investment Division, should:

Recommendation 5**:** Suspend the IVES Program until processes and procedures are put in place to ensure that a legitimate taxpayer signed a Form 4506-T authorizing the release of their tax transcript to IVES participants and their clients. This could include notifying taxpayers of the release of their tax information or mailing tax transcripts to the taxpayer's address of record for them to provide to the requestor.

> ***Management's Response:*** The IRS disagreed with this recommendation. IRS management responded that the IVES program supports the nationwide loan and mortgage industry and the taxpayers who rely on the services they provide. IRS management also implemented certification requirements to ensure that IVES participants are authenticated prior to being granted access to the TDS and being accepted into the IVES program.
>
> ***Office of Audit Comment:*** Management's response does not address our concern that processes or procedures are needed (*e.g.*, sending a notification) to ensure that a legitimate taxpayer authorized the release of his or her tax transcript to an IVES participant and its clients. Further, although the IRS has implemented a process that requires IVES participants to certify to the IRS that they verified the identity of all of their clients, the certification is a self-attestation and no supporting documentation is required to be submitted to the IRS for review.

If the IVES Program is not suspended, the Commissioner, Wage and Investment Division, should:

Recommendation 6: Notify the 1,356 IVES participants who were not notified (and did not independently certify) of the need to certify and disable those participants that do not certify as required.

> ***Management's Response:*** The IRS disagreed with this recommendation. However, IRS management disabled the accounts. IRS management stated that e-mail addresses provided by these participants are no longer valid and it is likely they are no longer in business. The certification process requires all IVES participants to revalidate the identity of their clients and ensure that there are proper procedures in place to authenticate individuals requesting transcripts. All IVES participants who did not certify were disabled by September 2017. Any disabled users needing access are required to contact the IRS to revalidate. Had any of these participants attempted to submit Form 4506-T, they would have been unsuccessful, prompting contact with the IRS.
>
> ***Office of Audit Comment:*** Management indicated they have disabled the 1,356 IVES participant accounts and stated that the e-mail addresses provided by these IVES participants are no longer valid and it is likely the participants are no longer in business.

Management also stated that had any of these IVES participants attempted to submit a tax transcript request, the request would have been unsuccessful and the IVES participant would have had to contact the IRS to learn about the new certification requirements. The IRS should have had a process, other than relying solely upon an e-mail address, to contact the IVES participants that it had previously acknowledged were excluded from the notification process.

Recommendation 7**:** Require IVES participants to provide the IRS with a list of their clients. In addition, develop a field in the online request system that requires the IVES user, at the time tax transcripts are requested, to enter identifying information for the client that is requesting the tax transcript.

Management's Response: The IRS disagreed with this recommendation. IRS management responded that the IVES participants cannot submit requests online. Requests are submitted via facsimile and when processed are sent electronically to a Secure Object Repository mailbox. Participants need to log in to e-Services to retrieve the requested information. Additionally, the IRS has initiated a compliance review process to ensure that participants are adhering to participant requirements and client certifications.

Office of Audit Comment: IVES certification procedures require IVES participants to maintain a list of clients requesting and receiving IRS tax transcripts on behalf of taxpayers. As such, IVES participants should already have lists of their clients that the IRS can request. The IRS's receipt of these lists, along with the implementation of a process by which IVES participants enter client identifying information, could enable the IRS to verify and monitor the specific clients for whom the tax transcript information is ultimately provided. Finally, the IRS cites its initiation of a compliance review process as a control to ensure IVES participants adhere to program and client certification requirements. It should be noted that as of May 2017, the IRS had sent letters to a judgmental sample of only 70 of the 693 IVES participants.

Recommendation 8: Implement a compliance strategy to ensure that IVES participants comply with the certification and program participation requirements.

Management's Response: The IRS agreed with this recommendation. IRS management implemented a compliance review process to ensure that IVES participants comply with their certification requirements. IRS management further developed procedures for the compliance reviews and will continue to assess the need for additional controls. The IRS plans to evaluate the procedures over the course of the next year and determine if adjustments to the strategy are required.

Actions to Reduce **********2**********

In June 2016 **********2**********
**********2**********
**********2**********
**********2**********. Figure 8 provides an example of the unnecessary level of detail the IRS provides.

Figure 8: **********2**********

****
****
****
****
****
****
****
********** 2 **********
****
****
****
****
****

Source: **********2**********.

**********2**********
**********2**********
**********2**********
**********2**********
2. The IRS responded that it was addressing this issue with all of the *******2******* products by working on implementing programing that will partly **********2********** **********2********** including **********2**********
**********2**********
**********2**********.

The IRS has previously stated that, "in an era of increasing cybercrimes, the IRS must strengthen the security around our online tools, including e-Services, to protect taxpayers." According to the timeline of activities provided to us by the IRS on December 15, 2016, the IRS planned to submit the programming requests for **********2********** by the end of May 2017, meaning these changes will likely not become effective until sometime in Calendar Year 2018. On June 19, 2017, we followed up with the IRS on its actions to ***2*** **********2*********. IRS management responded on June 26, 2017, that a meeting was scheduled with its Information Technology organization staff for July 6, 2017, to coordinate and discuss the programming request requirements.

Since we brought our concerns to the IRS's attention over one year ago, the IRS has been engaging with various stakeholders about their needs, and working with its Information Technology organization staff to identify programming requirements. IRS management agrees that **********2**********
**********2**********. However, management stated that it is taking longer to implement a solution because its Information Technology organization staff is dedicated to higher priority work, such as implementing Secure Access for e-Services. Further, **********2********** will need to be implemented to fulfill stakeholder needs, resulting in more complex work for its Information Technology organization staff. However, the fact remains that the continued delay **********2**********
**********2**********.

Recommendation

Recommendation 9: The Commissioner, Wage and Investment Division, should ***2*** **********2********** as an additional safeguard to protect taxpayer information.

> ***Management's Response:*** The IRS agreed with this recommendation. In May 2016, IRS management initiated a project to **********2**********
> ********2******** and took the necessary actions to implement the programming changes. A Unified Work Request was submitted on August 31, 2017, outlining the preliminary programming requirements needed.

Appendix I

Detailed Objective, Scope, and Methodology

The overall objective of this review was to assess the IRS's controls for verifying and validating transcript requests through the TDS. To accomplish our objective, we:

I. Determined how the IRS authenticates users requesting transcript information, for each of the transcript request methods, and if there is a risk associated with potential unauthorized disclosure of tax transcript information.

II. Identified and reviewed the methods and controls used by the IRS to authenticate taxpayers and evaluated the IRS's plans to strengthen access to e-Services.

   A. Determined if the IRS effectively performed the required risk assessments to determine the proper e-Authentication procedures.

   B. Evaluated the current processes the IRS uses to authenticate taxpayers' identities before providing access to IRS services. We evaluated the new processes and procedures, effective October 2016, for authenticating new and existing e-Services users.

   C. Interviewed IRS management to determine if the IRS made an informed and effective decision to delay the new authentication procedures.

   D. Identified the e-Services users that failed to complete the interim authentication requirements and quantified the impact on tax administration by determining the number of transcripts fulfilled for those users.

III. Determined if the IRS has effective processes and procedures to ensure that only authorized participants of the IVES services are requesting and receiving tax transcript information.

   A. Determined if the IRS is effectively authenticating the identity of third parties during the registration process to use the IVES service including verifying information provided on the IVES application.

   B. Determined if the IRS is effectively verifying that a valid Form 4506-T, *Request for Transcript of Tax Return*, is submitted when fulfilling transcript requests for the IVES program.

   C. Determined the effectiveness of the IVES certification requirements that went into effect on July 15, 2016, by evaluating whether the IRS is ensuring compliance with the certification requirements.

D. Identified the IVES participants that did not complete all required recertifications and quantified the impact on tax administration by determining the number of transcripts fulfilled for those participants.

E. Selected a sample of IVES participants that successfully completed the required recertifications and reviewed supporting certification documents to ensure that the IRS made a correct determination that the participant recertified.

F. Determined if the IRS has effective processes in place to review IVES participants' procedures that ensure the identity of their customers.

G. Reviewed the e-mails sent to the IRS to report suspicious IVES activity and determined if the IRS took appropriate actions.

IV. Evaluated the **********2********** ********** 2********** ********** 2********.

V. Determined the effectiveness of ******* 2********** **********2**********, procedures for processing **********2********** ***2*** and identifying fraudulent activity.

A. Determined if the new ****2**** procedures, effective July 1, 2016, are effective and evaluated IRS's decision to keep them temporary or make them permanent.

B. Reviewed the ****2***** that were received on or after June 10, 2016, to determine if the IRS properly processed or rejected the **********2**********.

C. Evaluated Accounts Management function procedures while contacting corporations to determine if improvements need to be made. In addition, we assessed whether sending letters to corporations is a more effective communication method.

Data validation methodology

During this review, we relied on IRS's Individual Master File[1] data for Tax Years[2] 2013 through 2016 stored on TIGTA's Data Center Warehouse,[3] TDS audit logs, and an analysis of data extracted from the IRS's e-Services Revalidation Project SharePoint site. To assess the reliability of computer-processed data, programmers within TIGTA's Data Center Warehouse validated the data files we extracted while we ensured that each data extract contained the specific data elements we requested and that the data elements were accurate. In addition, we performed extensive validation, when available, of the IRS's information on the e-Services Revalidation Project SharePoint site. For example, we reviewed random samples of each file

[1] The IRS database that maintains transactions or records of individual tax accounts.
[2] A 12-month accounting period for keeping records on income and expenses used as the basis for calculating the annual taxes due. For most individual taxpayers, the tax year is synonymous with the calendar year.
[3] A TIGTA repository of IRS data.

and verified that the data in the files were the same as the data captured in the IRS's Integrated Data Retrieval System[4] and/or the Employee User Portal[5] Maintain Registration application. As a result of our testing, we determined that the data were sufficiently reliable for purposes of this report.

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: 1) processes and procedures used to provide tax transcripts of tax returns and tax information to taxpayers and tax professionals with authorizations on file with the IRS; 2) processes and procedures to identify and disable/revoke IVES participants and TDS e-Services users that did not meet certification and authentication requirements; and 3) processes and procedures to ensure that *****2***** were properly processed and fraudulent claims were identified and prevented from being issued. We evaluated these controls by reviewing policies and procedures, interviewing employees and management, and analyzing data.

[4] IRS computer system capable of retrieving or updating stored information. It works in conjunction with a taxpayer's account records.

[5] A web hosting infrastructure located on the IRS intranet which supports an intranet portal that allows IRS employees to access business applications and data such as e-Services.

Appendix II

Major Contributors to This Report

Russell P. Martin, Assistant Inspector General for Audit (Returns Processing and Account Services)
Diana M. Tengesdal, Director
Roy E. Thompson, Audit Manager
Stephen A. Elix, Lead Auditor
Ryan N. Hadlock, Auditor
Heidi C. Turbyfill, Auditor
Alberto Garza, Manager (Data Analytics)

Appendix III

Report Distribution List

Commissioner
Office of the Commissioner – Attn: Chief of Staff
Deputy Commissioner for Services and Enforcement
Chief Information Officer
Director, Customer Account Services, Wage and Investment Division
Director, Office of Audit Coordination

Appendix IV

Outcome Measures

This appendix presents detailed information on the measurable impact that our recommended corrective actions will have on tax administration. These benefits will be incorporated into our Semiannual Report to Congress.

Type and Value of Outcome Measure:

- Taxpayer Privacy and Security – Potential; 17,792 taxpayer accounts (see page 4).

Methodology Used to Measure the Reported Benefit:

We obtained two lists of e-Services users that requested tax transcripts or updated their e-Services user account between October 2015 and November 2016 from the IRS's e-Services Revalidation Project SharePoint site. The IRS's Electronic Products and Services Support function filtered these lists for e-Services users of the TDS only and the IRS sent letters to these users the first two weeks of December 2016 notifying them of the new e-authentication requirements. We compared these lists to tax transcript request logs from October 1, 2015, to March 31, 2017, to identify e-Services TDS users that were not included and, therefore, not notified of the new requirements.

Our analysis identified e-Services TDS users that were not notified of the new interim authentication requirements. Management did not ensure that notification letters were in fact sent to all users. As a result, 1,507 of the 4,022 users continued to request a total of 96,639 tax transcripts without being required to re-authenticate in compliance with the interim requirements and, consequently, tax account information for 17,792 taxpayers was disclosed without proper authorization. IRS management could not explain why the 4,022 were excluded from receiving notification of the new authentication requirements and indicated that they would ensure that these users would be issued letters.

Type and Value of Outcome Measure:

- Revenue Protection – Actual; $49,944,732 (see page 9).

Methodology Used to Measure the Reported Benefit:

On June 1, 2016, we were notified of a potential refund fraud scheme affecting corporate taxpayers whereby the tax information needed to perpetrate this scheme was obtained ***5*** **********5**********. **2** June 9, 2016, we notified IRS management of concerns with the processing of **********2**********

**********2**********, requests. In response, the IRS immediately suspended processing of these refund requests until it could put additional safeguards in place. As of June 30, 2017, the IRS's Criminal Investigation function confirmed fraud on 17 refund requests and stopped or recovered refunds totaling $49,944,732.

Type and Value of Outcome Measure:

- Revenue Protection – Actual; $1,113,817,570 (see page 9).

Methodology Used to Measure the Reported Benefit:

On June 1, 2016, we were notified of a potential refund fraud scheme affecting corporate taxpayers whereby the tax information needed to perpetrate this scheme was obtained from the TDS or a phone call to the IRS on behalf of the corporation. On June 9, 2016, we notified IRS management of concerns with the processing of *****2***** requests. In response, the IRS immediately suspended processing of these refund requests until it could put additional safeguards in place. As of June 30, 2017, 349 *****2***** with refund requests totaling $1,113,817,570 were rejected[1] and held from processing. Of the 349 *****2***** rejected, 15 refund requests totaling $19,844,327 were held from processing because they had indicators of fraud and are under further review by the IRS's Criminal Investigation function.

Type and Value of Outcome Measure:

- Reliability of Information – Potential; 1,356 IVES participants (see page 17).

Methodology Used to Measure the Reported Benefit:

We obtained a list of 3,301 IVES participants from the IRS's Information Technology organization and compared it to a list of 1,733 IVES participants that received the e-mail notification of the new certification requirements on June 23, 2016. We found that 1,568 (47.5 percent) of the 3,301 participants were not notified by the IRS of the new certification requirements. This occurred because the IRS's records for notifying IVES participants were incomplete and the IRS did not reconcile those records with the actual IVES participant list to ensure that all participants were accounted for prior to issuing the letters. Although 212 of the IVES participants certified without being notified, further analysis found that the remaining 1,356 (86.5 percent) of the 1,568 had not certified by the required deadline of September 15, 2016. When we brought our concerns to IRS management's attention, the IRS stated that 691 of the 1,356 that were not notified were not in active status as of June 24, 2016. As such, they were not required to be notified. However, this is contrary to what the IRS

[1] Reasons for rejection included: returns had indicators of fraud, tax return already filed, form filed too late, duplicate form filed, unable to contact taxpayer, and unable to verify amounts reported on *****2*****.

previously stated that ***all*** IVES participants, regardless of their status, would be notified of the new requirements.

Appendix V

Management's Response to the Draft Report

DEPARTMENT OF THE TREASURY
INTERNAL REVENUE SERVICE
ATLANTA, GA 30308

COMMISSIONER
WAGE AND INVESTMENT DIVISION

DEC 2 9 2017

MEMORANDUM FOR MICHAEL E. MCKENNEY
DEPUTY INSPECTOR GENERAL FOR AUDIT

FROM: Kenneth C. Corbin
Commissioner, Wage and Investment Division

SUBJECT: Draft Audit Report – Transcript Delivery System Authentication and Authorization Processes Do Not Adequately Protect Against Unauthorized Release of Tax Information (Audit # 201640032)

Thank you for the opportunity to review and comment on the subject draft report. Protecting the tax information and personally identifiable information (PII) of taxpayers, and ensuring only those who have been authorized to receive it, are top priorities for the IRS. The e-Services suite of web-based applications was initially launched in 2003 to provide tax professionals, financial institutions, State taxing authorities, and government entities with the ability to conduct business with the IRS electronically. The Transcript Delivery System (TDS), one component of e-Services, was launched in 2005 to permit authorized external third-parties to view and obtain the tax information of individual and business taxpayers. In the twelve years subsequent to the TDS launch, advances in information system technologies that have revolutionized the way taxpayers and third-parties interact with the IRS have also contributed to dramatic increases in attempted fraud through identity theft, deception, impersonation, and other cyber-crime activities used to aid and abet unscrupulous individuals attempting to defeat our internal controls.

Recognizing that controls and processes needed to be improved and strengthened, the IRS embarked on a strategy in 2016, to place the e-Services applications behind a multi-factor authentication process, Secure Access Authentication (SAA). The IRS deployed the e-Services Convergence, which included placing the TDS application, behind the protection of secure access protocols on December 10, 2017. The SAA provides Level of Assurance (LOA) 3 protection, as defined by the National Institute of Standards and Technology Special Publication 800-63. Given that TDS now resides behind the SAA process, separate notification to the 4,022 users identified in the report as not having received notification of the interim procedures is not necessary. All e-Services users, including the 4,022 identified are required to reauthenticate at the LOA 3 standard.

Technological challenges and procedural concerns raised by stakeholders delayed implementation of the strategy. Due to the delay, the IRS implemented interim procedures to mitigate the risks associated with not having the e-Services applications protected by the SAA. These mitigating processes included using systemic monitoring protections such as a Bot Manager that performed ongoing analyses of activity at the server level to detect anomalous activity. Additionally, active e-Services users with access to the TDS application were required to revalidate their accounts. Approximately 90,000 users revalidated and approximately 55,000 other users had their access revoked for failure to revalidate.

Further, the ability to access and use the TDS is granted either through an e-File application or through an Income Verification Express Services (IVES) application. The e-File Application process has suitability checks, including a tax compliance check and either a criminal background check or professional credential checks. Also, the account holder must either file a minimum of five tax returns or be an individual eligible to practice before the IRS, including attorneys, certified public accountants, enrolled agents, enrolled actuaries, and enrolled retirement plan agents. The IVES application process also requires tax compliance checks and IVES certification, meaning all users listed on the application must be registered for e-Services basic identity proofing by providing their name, address, date of birth, and adjusted gross income, and completing the registration process by providing a confirmation code sent to the address of record.

We recognize the concerns the Treasury Inspector General for Tax Administration has regarding the IRS' ability to validate the authenticity of third-party requests for tax information, but we believe the interim risk-mitigation procedures that were put in place, along with placing TDS behind secure access, are effective at balancing the protection of sensitive tax information and PII with the legitimate needs of third-party service providers whom taxpayers have authorized to receive their information.

Attached are our comments and proposed actions to your recommendations. If you have any questions, please contact me, or a member of your staff may contact James P. Clifford, Director, Customer Account Services, Wage and Investment Division, at 470-639-3504.

Attachment

Attachment

Recommendations

The Commissioner, Wage and Investment Division, should:

RECOMMENDATION 1
Send notification letters of interim authentication requirements to the 4,022 e-Services TDS users not notified and revoke access privileges for any users that do not complete the interim authentication requirements.

CORRECTIVE ACTION
We disagree with the recommendation to send notification letters to the 4,022 e-Services Transcript Delivery System (TDS) users who were not initially notified of the interim authentication requirements. Level of Assurance 3 standards for the TDS application were deployed on December 10, 2017. All TDS users, including the 4,022 who did not receive interim authentication notification letters are required to reauthenticate.

IMPLEMENTATION DATE
N/A

RESPONSIBLE OFFICIAL
N/A

CORRECTIVE ACTION MONITORING PLAN
N/A

RECOMMENDATION 2
Implement multifactor authentication for e-Services, which includes the TDS application, to comply with Federal Government Information Security Standards.

CORRECTIVE ACTION
We agree with this recommendation. Multi-factor authentication was implemented for the TDS application on December 10, 2017.

IMPLEMENTATION DATE
Implemented

RESPONSIBLE OFFICIAL
Deputy Director Online Services and IRS Identity Assurance Executive, Office of Online Services.

CORRECTIVE ACTION MONITORING PLAN
N/A

RECOMMENDATION 3
Implement processes and procedures to ensure that legitimate taxpayers authorize the release of their tax transcripts. In addition, discontinue offering tax transcripts via those processes in which the IRS cannot confirm whether legitimate taxpayers authorized the release of their tax transcripts.

CORRECTIVE ACTION
We agree with this recommendation. New certification requirements for Income Verification Express Service (IVES) participants were established on June 30, 2016 which required more rigorous steps for IVES participants to verify the legitimacy of clients and individuals requesting transcripts. The E-Services suite of applications is now protected by Secure Access Authentication so all IVES participants are behind a two-factor authentication process. We will continue to evaluate the effectiveness of our process and determine where improvements can be made.

IMPLEMENTATION DATE
December 15, 2018

RESPONSIBLE OFFICIAL
Director, Submission Processing, Customer Account Services, Wage and Investment Division

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

RECOMMENDATION 4
Implement processes and procedures that prevent the use of data scraping programs to request tax transcripts.

CORRECTIVE ACTION
We disagree with this recommendation. Neither the Treasury Inspector General for Tax Administration nor the IRS' analysis has identified illegitimate transcript requests associated with the use of data scraping programs. The TDS application uses protective analytics that monitors system activity to detect anomalous activity. We have seen no evidence of increased fraud risk involving this retrieval technique, and preventing the use of the technique would adversely affect IVES participants and the taxpayers they represent without a compelling reason for doing so.

IMPLEMENTATION DATE
N/A

RESPONSIBLE OFFICIAL
N/A

CORRECTIVE ACTION MONITORING PLAN
N/A

RECOMMENDATION 5
Suspend the IVES Program until processes and procedures are put in place to ensure that a legitimate taxpayer signed a Form 4506-T authorizing the release of their tax transcript to IVES participants and their clients. This could include notifying taxpayers of the release of their tax information or mailing tax transcripts to the taxpayer's address of record for them to provide to the requestor.

CORRECTIVE ACTION
We disagree with this recommendation. The IVES program supports the nationwide loan and mortgage industry and the taxpayers who rely on the services they provide. We have implemented certification requirements to ensure IVES participants are authenticated prior to being granted access to the TDS and being accepted into the IVES program.

IMPLEMENTATION DATE
N/A

RESPONSIBLE OFFICIAL
N/A

CORRECTIVE ACTION MONITORING PLAN
N/A

If the IVES Program in not suspended, the Commissioner, Wage and Investment Division, should:

RECOMMENDATION 6
Notify the 1,356 IVES participants who were not notified (and did not independently certify) of the need to certify and disable those participants that do not certify as required.

CORRECTIVE ACTION
We disagree with the recommendation to notify the 1,356 participants; however, those accounts have been disabled. E-mail addresses provided by these participants are no longer valid and it is likely they are no longer in business. The certification process requires all IVES participants to re-validate the identity of their clients and ensure that there are proper procedures in place to authenticate individuals requesting transcripts. All IVES participants who did not certify were disabled by September 2017. Any disabled users needing access are required to contact us to revalidate. Had any of these participants attempted to submit Form 4506-T, *Request for Transcript of Tax Return*, they would have been unsuccessful, prompting contact with the IRS.

IMPLEMENTATION DATE
Implemented

RESPONSIBLE OFFICIAL
Director, Submission Processing, Customer Account Services, Wage and Investment Division

CORRECTIVE ACTION MONITORING PLAN
N/A

RECOMMENDATION 7
Require IVES participants to provide the IRS with a list of their clients. In addition, develop a field in the online request system that requires the IVES user, at the time tax transcripts are requested, to enter identifying information for the client that is requesting the tax transcript.

CORRECTIVE ACTION
We disagree with this recommendation. The IVES participants cannot submit requests online. Requests are submitted via facsimile and, when processed, are sent electronically to a Secure Object Repository mailbox. Participants need to log in to e-Services to retrieve the requested information. Additionally, the IRS has initiated a compliance review process to ensure participants are adhering to participant requirements and client certifications.

IMPLEMENTATION DATE
N/A

RESPONSIBLE OFFICIAL
N/A

CORRECTIVE ACTION MONITORING PLAN
N/A

RECOMMENDATION 8
Implement a compliance strategy to ensure that IVES participants comply with the certification and program participation requirements.

CORRECTIVE ACTION
We agree with this recommendation. The IRS implemented a compliance review process to ensure that IVES participants comply with our certification requirements. We further developed procedures for the compliance reviews and will continue to assess the need for additional controls. We will evaluate the procedures over the course of the next year and determine if adjustments to the strategy are required.

IMPLEMENTATION DATE
October 15, 2018

RESPONSIBLE OFFICIAL
Director, Submission Processing, Customer Account Services, Wage and Investment Division.

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

RECOMMENDATION 9
The Commissioner, Wage and Investment Division, should **********2********** **********2********** as an additional safeguard to protect taxpayer information.

CORRECTIVE ACTION
We agree with this recommendation. In May 2016, we initiated a project to *****2****** **********2********** and have taken the necessary actions to implement the programming changes. Unified Work Request 203857 was submitted on August 31, 2017, outlining the preliminary programming requirements needed. However, due to limited resources and competing priorities that could affect completion of the work, the IRS cannot provide an implementation date for the programming.

IMPLEMENTATION DATE
N/A

RESPONSIBLE OFFICIAL
Director, Submission Processing, Customer Account Services, Wage and Investment Division.

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