TREASURY INSPECTOR GENERAL FOR TAX ADMINISTRATION

Filing Season 2016: Implementation of New Data Elements

September 21, 2016

Reference Number: 2016-20-062

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

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

1-800-366-4484

By Web:

www.treasury.gov/tigta/

Or Write:

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

Information you provide is confidential and you may remain anonymous.

FILING SEASON 2016: IMPLEMENTATION OF NEW DATA ELEMENTS

Highlights

Final Report issued on September 21, 2016

Highlights of Reference Number: 2016-20-062 to the Internal Revenue Service Commissioner for the Wage and Investment Division.

IMPACT ON TAXPAYERS

Tax-related identity thefts adversely affect the ability of taxpayers to file their tax returns and timely receive their tax refunds and can impose financial and emotional hardships on the victims. Therefore, continued improvements and advancements in identification of identity theft when tax returns are processed and before fraudulent tax refunds are issued must be a priority for the IRS.

WHY TIGTA DID THE AUDIT

The overall audit objective was to review the implementation of new tax return-related data elements based on the 2015 Security Summit, *Protecting Taxpayers from Identity Theft Tax Refund Fraud*.

WHAT TIGTA FOUND

The IRS tested 23 new Federal tax return-related data elements in accordance with the Internal Revenue Manual procedures. All 23 data elements were implemented into the IRS's Return Review Program system, although only three were used systemically to filter returns and help identify potential identity theft tax refund fraud during the 2016 Filing Season. As of March 25, 2016, the IRS identified approximately $4.1 billion in suspected identity theft tax refund fraud, of which $72 million (21,000 tax returns) is attributable to the three new data elements. Additionally, the IRS attributed the prevention of 24,000 taxpayer returns from being incorrectly selected as potential identity theft tax refund fraud returns to one of the three data elements.

For the remaining 20 new data elements, there was insufficient historical data to create business rules that would enable systemic usage during the 2016 Filing Season. The Applications Development division intends to determine their potential use in future filing seasons.

The IRS indicated that the data elements should remain confidential and be kept a secret from the public. TIGTA agrees with the IRS's position and believes the data elements should be protected from public exposure.

However, TIGTA's search of the IRS's public website identified schemas that included several of the new data elements. The IRS was notified of this finding and responded by removing the schemas containing the data elements. Further, TIGTA identified two additional documents on the IRS's public website containing information related to the data elements; one of the documents included specific information about one of the new data elements.

WHAT TIGTA RECOMMENDED

TIGTA recommended that the Commissioner, Wage and Investment Division, permanently remove the data elements from public access to ensure that inappropriate use cannot occur, conduct a thorough inspection of its public websites and publications to determine if other data element information is available to the public and ensure that it is removed, and implement a secure process to provide the data elements to valid parties who have a need to access them.

The IRS agreed with one recommendation and plans to implement a secure process to provide the data elements to valid parties. The IRS partially agreed with two recommendations and removed the schema information from its website. TIGTA maintains that data element exposure on the IRS public website and in publications increases the risk of fraud, and stands by the recommendation to remove data element information from the IRS's public website and in publications to minimize potential misuse.

TREASURY INSPECTOR GENERAL
FOR TAX ADMINISTRATION

DEPARTMENT OF THE TREASURY

WASHINGTON, D.C. 20220

September 21, 2016

MEMORANDUM FOR COMMISSIONER, WAGE AND INVESTMENT DIVISION

FROM: Michael E. McKenney
Deputy Inspector General for Audit

SUBJECT: Final Audit Report – Filing Season 2016: Implementation of New Data Elements (Audit # 201520029)

This report presents the results of our review of the Internal Revenue Service's (IRS) implementation of new tax return-related data elements based on the 2015 Security Summit, *Protecting Taxpayers from Identity Theft Tax Refund Fraud*. This review is included in our Fiscal Year 2016 Annual Audit Plan and addresses the major management challenge of Improving Tax Systems and Online Services.

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

Copies of this report are also being sent the IRS mangers affected by the report recommendations. If you have any questions, please contact me or Danny Verneuille, Acting Assistant Inspector General for Audit (Security and Information Technology Services).

Table of Contents

Abbreviations

IDT	Identity Theft
IRM	Internal Revenue Manual
IRS	Internal Revenue Service
RRP	Return Review Program
SSN	Social Security Number

Background

Identity thieves access electronic systems unlawfully[1] and steal Personally Identifiable Information, such as names, Social Security Numbers (SSN), or other identifying information from limitless sources, to commit fraud or other crimes. One such crime, known as identity theft (IDT) tax refund fraud, occurs when someone uses a legitimate taxpayer's identity to file a fraudulent tax return and claim a refund. The identity thief will use a stolen SSN to file a forged tax return and attempt to get a fraudulent refund early in the filing season[2] before the victim sends his or her tax return to the Internal Revenue Service (IRS) to be processed.

While the IRS has made progress in its prevention, detection, and resolution of IDT tax refund fraud, more work remains to fight IDT. New Federal tax return-related data elements were created for the 2016 Filing Season to help authenticate the taxpayer and detect IDT tax refund fraud.

Refund fraud is one of the biggest challenges facing the IRS and is described as one of the IRS's "Dirty Dozen" tax scams.[3] In an April 2015 audit report,[4] the Treasury Inspector General for Tax Administration estimated undetected potentially fraudulent refunds to be approximately $11 billion between Tax Years 2010 and 2012. IDT tax refund fraud has an immediate and negative impact on taxpayers whose personal information is used to commit these crimes, as it adversely affects their ability to file tax returns and timely receive tax refunds. This can impose financial and emotional hardships on the affected taxpayers. Tax-related IDT places an enormous burden on the tax system and ultimately erodes public confidence in our tax system. The IRS must protect taxpayers' dollars to maintain public trust.

IRS's efforts to combat identify theft tax refund fraud

In recent years, the IRS has adopted strategies designed to combat IDT tax refund fraud. Those strategies focused on prevention, detection, and resolution for victims of IDT tax refund fraud. Figure 1 reflects some of the strategies the IRS has implemented:

[1] Systems can be accessed by hackers/outsiders that break in to the network and gain access to systems and data; alternatively employees/insiders with valid credentials can log on legitimately but use the system for illegal purposes.
[2] See Appendix V for a glossary of terms.
[3] The "Dirty Dozen" list is compiled annually by the IRS and lists a variety of common scams taxpayers may encounter any time during the year.
[4] See Appendix IV for the prior Treasury Inspector General for Tax Administration audit reports.

Figure 1: IDT Tax Refund Fraud Strategies the IRS Uses

IRS Fraud Strategies	Results of the Fraud Strategies Used
Added systemic filters and multiple layers of authentication.	The IRS implemented several IDT filters to improve its ability to detect false tax returns at the time of processing and to prevent fraudulent refunds from being issued. As of September 2014, 114 filters detected 832,412 tax returns, preventing the issuance of approximately $5.5 billion in fraudulent tax refunds. Also, the IRS continues to expand the number of Identity Protection Personal Identification Numbers issued to victims. For the 2014 Processing Year, the IRS issued more than 1.2 million notices to taxpayers.
Took steps to prevent the fraudulent use of deceased persons' identity information.	The IRS is able to lock tax accounts of deceased individuals, thus preventing the fraudulent use of their identity information. This tool has locked more than 26 million accounts between January 2011 and September 2014.
Improved the use of the prisoner databases.	In 2012, the IRS stopped more than 137,000 fraudulent tax returns filed by prisoners which prevented $936 million in refunds from being issued. To accomplish this, the IRS compiles a list of prisoners received from the Federal Bureau of Prisons and State Departments of Corrections.
Established the External Leads Program to thwart attempts by identity thieves to defraud the Government.	The IRS works cooperatively with financial institutions, Government, law enforcement agencies, and others to identify and recover questionable tax refunds. Through the External Leads Program, the IRS is alerted of suspicious transactions. The IRS investigates the taxpayers involved and, if fraudulent activity is verified, recovers the erroneous funds. In 2013, through this program the IRS recovered more than $576 million.
Protected taxpayers' identities through the SSN Elimination and Reduction Program.	Through the SSN Elimination and Reduction Program, the IRS removed SSNs or reduced the use of them within its systems, forms, notices, and letters in which use is not necessary. As of January 2015, the IRS estimates that it has masked or eliminated SSNs on 267 different taxpayer correspondences.

Source: Prior Treasury Inspector General for Tax Administration audit reports.

Fighting IDT tax refund fraud is an ongoing challenge as identity thieves are adaptable and constantly change their tactics to circumvent controls. While the IRS has made progress in its prevention, detection, and resolution of IDT tax refund fraud, more work remains to fight IDT. Therefore, the IRS must place priority on continued improvements and advancements in the identification of IDT when tax returns are processed and before fraudulent tax refunds are issued.

2015 Security Summit: Protecting Taxpayers from Identity Theft Tax Refund Fraud

As noted in the June 2015 report, *Protecting Taxpayers from Identity Theft Tax Refund Fraud*, a Security Summit was held between the IRS, private tax industries, and State departments of revenue. The IRS Commissioner called on leaders of public and private sectors to work together to combat the emerging threats of IDT tax refund fraud. The summit worked to identify new

steps to validate taxpayer and tax return information, increase information sharing between industry and Governments, and standardize sharing of suspected identity fraud information and analytics from the tax industry to identify fraud schemes and indicators of fraud patterns.

Three specialized working groups were derived from the Security Summit. The Information Sharing working group was tasked with sharing information that would collectively improve the ability to detect and prevent IDT tax refund fraud. The Strategic Threat Assessment and Response working group was tasked with developing proactive initiatives to fight IDT tax refund fraud. The Authentication working group was responsible for strengthening authentication practices and created 23 new Federal tax return-related data elements to help validate taxpayers. The data elements are needed to help authenticate the taxpayer and detect IDT tax refund fraud at the time of electronic filing in support of revenue protection and fraud prevention strategies. The Authentication working group collaborated to ensure that the data elements would be implemented timely. The group met regularly from April 2015 through March 2016 to discuss data element creation, testing, and implementation. IRS senior management and executives were regularly updated on challenges and successes of data element progress. The group continues to have regular discussions about ways to protect taxpayers from IDT tax refund fraud.

This review was performed at the Applications Development division office at the New Carrollton Federal Building in Lanham, Maryland, and the Wage and Investment Division office at the Brookhaven Campus in Holtsville, New York, during the period January through April 2016. We conducted this performance audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objective. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objective. Detailed information on our audit objective, scope, and methodology is presented in Appendix I. Major contributors to the report are listed in Appendix II.

Results of Review

Twenty-Three New Data Elements Were Tested and Implemented for the 2016 Filing Season

Internal Revenue Manual (IRM) Section 2.127.1, *Software Testing Standards and Procedures, Information Technology Test Policy*, states that projects must have test artifacts or work products, such as test plans, test scripts, test cases, test reports, and measurements documented and maintained in an approved repository. IRM Section 2.127.2, *Software Testing Standards and Procedures, Information Technology Software Testing Process and Procedures*, identifies four phases of information technology software testing in which test artifacts are developed. Figure 2 describes these four phases.

Figure 2: Information Technology Software Testing Phases

Phase	Definition	End Product
Perform Planning	Ensures that the requirements, Unified Work Request, test environments, and test plans are defined.	Test plans are complete.
Perform Preparation	Uses the test plans, the Unified Work Request, and the Requirements Traceability Verification Matrix to complete the Development Phase for the test cases and test scripts.	Test plans are finalized; test cases and test scripts are complete.
Execute and Document Test	Uses the test cases and test scripts and executes the tests based on these documents, which develop the test status reports.	Test case disposition is complete.
Closeout Test	Outlines the activities required to close out the test.	End of Test Report with signatures.

Source: IRM Section 2.127.2, dated March 2015.

Implementation of the data elements was noted in the June 2015 report, *Protecting Taxpayers from Identity Theft Tax Refund Fraud*, which stated that the Security Summit parties intended to have IDT tax refund fraud detection and prevention solutions, including programming modifications (*e.g.*, data element implementation), ready for the 2016 Filing Season and beyond.

We reviewed documentation from the four test phases and determined the IRS tested the 23 new data elements in accordance with IRM procedures. The Wage and Investment Division

developed a Unified Work Request to document the need for the data elements for the 2016 Filing Season. It was used to create a schema for the data elements. This schema was placed in a table within the Requirements Traceability Verification Matrix. From the schema table, the Systems Acceptability Testing group within the IRS's Information Technology organization developed the test cases, test scripts, and test execution documents to use when conducting the tests on the data elements schema. Five tests were conducted on the data elements schema. Of the five tests conducted, two initially failed because of an issue with the data file. Once the issue was corrected, the two tests were performed again and passed.

The Applications Development division within the IRS's Information Technology organization was responsible for implementing the 23 data elements into the Return Review Program (RRP).[5] IRS management informed us that it typically evaluates new data elements for one year to determine if they could be used systemically. For the 2016 Filing Season, Applications Development personnel evaluated whether there was sufficient data for the data elements to be useful. After completing their review, Applications Development personnel determined that business rules could be created for three of the data elements that enabled them to be used systemically during the 2016 Filing Season. However, there was insufficient historical data to create business rules for the remaining 20 data elements. The Applications Development division intends to determine their potential use in future filing seasons. During our on-site visits, Applications Development division personnel executed the business rules to demonstrate how these three data elements are systemically used and demonstrated that the remaining 20 data elements had also been implemented into the RRP.

As of March 25, 2016, the IRS identified approximately $4.1 billion in suspected IDT tax refund fraud, of which $72 million (21,000 tax returns) was attributable to the three new data elements used systemically in the RRP. Additionally, the IRS attributed the prevention of 24,000 taxpayer returns from being incorrectly selected as potential IDT tax refund fraud returns to one of the three data elements.[6]

Public Access to the Data Elements Allows for Potential Misuse

National Institute of Standards and Technology Special Publication 800-53, *Security and Privacy Controls for Federal Information Systems and Organizations*,[7] states that the general public is not authorized access to nonpublic information. This includes Sensitive But Unclassified information, which IRM Section 10.8.1, *Information Technology Security, Policy and Guidance*

[5] The RRP uses a series of "filters" to identify suspected fraud and route any return that fits the filters' definition to the proper treatment stream. A filter is made up of logic that defines a return as suspected fraud. This logic references RRP business rules, model scores, and/or return clustering (grouping returns with common, suspicious characteristics).
[6] Dollar values and number of taxpayer returns represent suspected amounts only. The IRS will confirm actual amounts through analysis, with results available in June and August 2016.
[7] National Institute of Standards and Technology Special Publication 800-53 (Revision 4) p. 191 (April 2013).

defines as any information which, if misused, may adversely affect the conduct of Federal programs, including IRS operations. It further states that Sensitive But Unclassified information shall not be posted to internal or external IRS websites.

The June 2015 report, *Protecting Taxpayers from Identity Theft Tax Refund Fraud*, states that to provide extensive details of the new data elements [to the public] would give a "roadmap" to identity thieves and weaken their effectiveness to protect taxpayers from IDT tax refund fraud. *Standards for Internal Control in Federal Government*[8] instructs that internal control deficiencies should be corrected timely.

At the Council for Electronic Revenue Communication Advancement meeting in October 2015, the IRS indicated that the data elements should remain confidential and be kept a secret from the public. In multiple public articles, the IRS has remained silent about details of the data elements and indicated that making this information public would inform identity thieves of its specific plans/strategy. We agree with the IRS's position and believe the data elements should be protected from public exposure.

Our search of the IRS's public website (www.IRS.gov) identified schemas that included several of the new data elements. The audit team notified the IRS of its finding and recommended the IRS immediately remove the schemas with the data elements from its website. The audit team also recommended the IRS ensure that any future communication does not specifically identify the data elements. The IRS posted the data elements to its website on September 11, 2015, and removed them on March 14, 2016. The link on the website that initially led to the data elements has been replaced with a link to an IRS e-mail address where the schemas with the data elements must be requested. The information on the website indicates that the data elements will be available only to valid parties (*e.g.*, software developers, transmitters, or State users). The IRS has written procedures to validate the requestor and ensure that data element information can be provided to valid requestors.

After notifying the IRS of the finding on the IRS's public website, we identified two additional documents on the public website containing information related to the data elements. One of the documents was a publication with specific information about one of the new data elements. However, the IRS did not intend to include on its website information about the data elements in its publication.

The IRS indicated that prior to posting the data elements to its website on September 11, 2015, discussions were held to determine how to make the schemas available to software developers. The e-File Services division within the IRS's Wage and Investment Division publish schemas necessary for filing tax returns on its public website because software developers must have access to the schemas to develop their tax preparation software. Because the IRS has always provided public access to all of its schemas and believed a workable solution to provide secure

[8] Government Accountability Office, GAO-14-704G, *Standards for Internal Control in the Federal Government* p. 26 (September 2014).

access could not be implemented in time for the 2016 Filing Season, the IRS decided to accept the business risk and make public the schemas that included the data elements. Although the IRS recognized the need to provide secure access to the data elements, it stated the removal of the data elements on March 14, 2016, from the public website is temporary and subsequent discussions will determine possible implications of their removal.

While the IRS acknowledged that the data elements may be located via Internet searches, the IRS believes they are concealed and difficult to find. The IRS admitted that knowledge of the existence of the data elements might be helpful to fraudsters but did not believe the data elements by themselves increased the risk of fraud. The IRS also noted that providing secure access to its trusted partners is not the ultimate solution because the IRS has no control over the schemas once they are shared externally.

Providing schemas and publications that contain the data elements used by the IRS to detect IDT tax refund fraud to the general public is contrary to the IRS's stated intention that data elements should remain confidential. The data element information is Sensitive But Unclassified information designed to help prevent IDT tax refund fraud. Making data element information public could allow criminals to use the public information to thwart the IRS's intended use of the data elements and allow identity thieves to circumvent implemented safeguards. While the IRS has also noted the importance of safeguarding the data elements, secure access was not provided timely. Timely protection of the data elements by the IRS helps prevent improper use.

Recommendations

The Commissioner, Wage and Investment Division, should:

Recommendation 1: Permanently remove the data elements from public access to ensure that inappropriate use cannot occur.

> ***Management's Response:*** The IRS partially agreed with this recommendation. The IRS already removed schema information related to the authentication data elements from its public website (IRS.gov) on March 14, 2016, and is currently implementing a new secure distribution process for authentication data element information starting in Filing Season 2017. However, the IRS does not believe that this recommendation, as written, can be fully implemented as it does not retain control over the schemas once they are shared externally.
>
> ***Office of Audit Comment:*** The corrective actions described by the IRS appear responsive to the recommendation.

Recommendation 2: Conduct a thorough inspection of its public websites and publications to determine if other data element information is available to the public and ensure that it is removed.

Management's Response: The IRS partially agreed with this recommendation. The IRS took action in March 2016 to remove the Modernized e-File schema that contains the data definition of elements designed to combat fraud and identity theft. Removing all data element references from public websites and publications puts burden on the IRS and industry partners who need access to reference material that may or may not contain references to data elements. Furthermore, it is not the reference to the authentication elements that is the highest security concern. Instead, it is the detailed technical information describing how this data will be used to combat fraud, which is closely guarded. Consequently, the IRS will proceed with its current approach of determining the appropriateness of data element information available for public access within the context of a risk-based decision framework.

Office of Audit Comment: We maintain that data element exposure on the IRS public website and in publications increases the risk of fraud. We believe the corrective actions to remove data element information from the IRS's public website and publications need to be taken to minimize potential misuse.

Recommendation 3: Implement a secure process to provide the data elements to valid parties (*e.g.*, software developers, transmitters, and State users) who have a need to access them.

Management's Response: The IRS agreed with this recommendation. The IRS is implementing a secure process to provide the authentication data elements to valid parties who have a need to access them. Beginning in August 2016, the schema and business rule packages will be delivered to software providers through a Secure Object Repository and Registered User Portal. Also, because the IRS understands the importance of distributing this information to the software community in a timely manner, the IRS is currently leveraging a manual process through the Modernized e-File mailbox until the automated solution is available.

Appendix I

Detailed Objective, Scope, and Methodology

Our overall objective was to review the implementation of new tax return-related data elements based on the 2015 Security Summit, *Protecting Taxpayers from Identity Theft Tax Refund Fraud.* To accomplish our objective, we:

I. Evaluated the planning efforts related to the new data elements implemented.

A. Obtained and reviewed documentation to determine what goals or expectations were established for the data elements implemented.

B. Obtained and reviewed documentation to determine how the data elements implementation process was communicated from inception to implementation.

C. Reviewed Wage and Investment Division and Information Technology organization planning documentation, including status reports, to determine how the progress of the data elements implemented was monitored and managed.

II. Evaluated the data element testing and implementation.

A. Obtained and reviewed documentation that all new data elements were implemented into the RRP.

B. Reviewed requirements testing guidance Section 2.127.2, *Software Testing Standards and Procedures, Information Technology Software Testing Process and Procedures,* of the IRM to ensure that controls/procedures were followed.

C. Reviewed requirements testing documentation of test schedules, tests conducted, and test results to ensure adequate testing.

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: documentation related to the goals or expectations established for data elements, communication of data elements, and how the progress of data elements implemented were monitored and managed; and the policies and procedures for planning, testing, and implementing the new data elements. We evaluated these controls by interviewing Wage and Investment Division and Application Development division management and identifying tests and tracing documentation of the new data elements as they moved through the four test phases to implementation into the RRP system.

Appendix II

Major Contributors to This Report

Danny Verneuille, Acting Assistant Inspector General for Audit (Security and Information Technology Services)
Myron Gulley, Acting Director
Michael Mohrman, Acting Audit Manager
Chanda Stratton, Lead Auditor
Chinita Coates, Auditor

Appendix III

Report Distribution List

Commissioner
Office of the Commissioner – Attn: Chief of Staff
Deputy Commissioner for Operations Support
Deputy Commissioner for Services and Enforcement
Chief Information Officer
Associate Chief Information Officer, Applications Development
Associate Chief Information Officer, Enterprise Services
Director, Customer Account Services
Director, Office of Audit Coordination

Appendix IV

Prior Treasury Inspector General for Tax Administration Audit Reports on Identity Theft Tax Refund Fraud

Reference No. (Date)	Report Title and Page Number
2014-40-057 (Aug. 2014)	*The External Leads Program Results in the Recovery of Erroneously Issued Tax Refunds; However, Improvements Are Needed to Ensure That Leads Are Timely Verified (pp. 2, 6)*
2014-40-086 (Sept. 2014)	*Identity Protection Personal Identification Numbers Are Not Provided to All Eligible Taxpayers (p. 6)*
2014-40-091 (Sept. 2014)	*Prisoner Tax Refund Fraud: Delays Continue in Completing Agreements to Share Information With Prisons, and Reports to Congress Are Not Timely or Complete (pp. 6-7)*
2015-40-024 (Mar. 2015)	*Victims of Identity Theft Continue to Experience Delays and Errors in Receiving Refunds (p. 9)*
2015-40-026 (Apr. 2015)	*Efforts Are Resulting in the Improved Identification of Fraudulent Tax Returns Involving Identity Theft (pp. 9-10, 13)*
2015-40-063 (July 2015)	*Limited Progress Has Been Made to Eliminate the Unnecessary Use of Social Security Numbers in Taxpayer Correspondence (p. 11)*

Appendix V

Glossary of Terms

Term	Definition
Artifact	The tangible result (output) of an activity or task performed by a project during the life cycle.
Data Element	The smallest named item of data that conveys meaningful information or condenses a lengthy description into a short code.
End of Test Report	A requirement for all testing. The purpose of the End of Test Report is to provide a standard artifact to summarize the complete test effort for the test type(s). The Report also allows the test managers an opportunity to mitigate risks that may cause delays to project implementation.
Filing Season	The period from January through mid-April when most individual income tax returns are filed.
Identity Theft Tax Refund Fraud	A tax-related IDT occurs when someone uses a stolen SSN to file a tax return claiming a fraudulent refund.
Processing Year	The calendar year in which the tax return or document is processed by the IRS.
Requirements	Describes a condition or capability to which a system must conform, either derived directly from user needs, or stated in a contract, standard, specification, or other formally imposed document. A desired feature, property, or behavior of a system.
Requirements Traceability Verification Matrix	A tool that documents requirements and establishes the traceability relationships between the requirements to be tested and their associated test cases and test results.
Return Review Program	A system the IRS uses to identify potentially fraudulent electronically filed tax returns. It enhances the IRS's capabilities to detect, resolve, and prevent criminal and civil noncompliance, and reduces issuance of fraudulent tax refunds.

Term	Definition
Schema	An Extensible Markup Language document that specifies the data elements, structure, and rules for each form, schedule, document, and attachment.
Sensitive But Unclassified	Any information that requires protection due to the risk and magnitude of loss or harm to the IRS or the privacy to which individuals are entitled under the Privacy Act, which could result from inadvertent or deliberate disclosure, alteration, or destruction.
System Acceptability Test	The process of testing a system or program to ensure that it meets the original objectives outlined by the user in the requirement analysis document.
Tax Year	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.
Test Plan	A standard artifact to summarize the complete test effort for the test type. It allows test managers an opportunity to mitigate risks that may cause delays to project implementation.
Unified Work Request	A formal notification to an information technology supplier organization(s) that a requestor organization has a business need for information technology products or services.

Appendix VI

Management's Response to the Draft Report

DEPARTMENT OF THE TREASURY
INTERNAL REVENUE SERVICE
ATLANTA, GA 30308

COMMISSIONER
WAGE AND INVESTMENT DIVISION

AUG 2 4 2016

MEMORANDUM FOR MICHAEL E. MCKENNEY
DEPUTY INSPECTOR GENERAL FOR AUDIT

FROM: Debra Holland
Commissioner, Wage and Investment Division

SUBJECT: Draft Audit Report – Filing Season 2016: Implementation of New Data Elements (Audit # 201520029)

Thank you for the opportunity to review and comment on the subject draft report. We appreciate your acknowledgment of our efforts in the prevention, detection, and resolution of identity theft (IDT) refund fraud. In recognition of escalating challenges and the need to act quickly to prepare for the next tax filing season, the IRS Commissioner called on leaders in the public and private sectors to come together and work collaboratively to protect taxpayers from IDT refund fraud. On March 19, 2015, the IRS convened an unprecedented Security Summit meeting with IRS officials, the chief executive officers of the leading tax preparation firms, software developers, payroll and tax financial product processors, and state tax administrators to discuss common challenges and ways to leverage our collective resources and efforts. The Summit participants agreed to commit their leadership and resources to work together to combat this growing problem, and to that end, the group agreed to form a public-private partnership committed to protecting the nation's taxpayers and the tax system from IDT refund fraud.

The Security Summit represents not only a ground-breaking partnership, but also an unprecedented collaboration of the private and public sector working together on multiple fronts with a unified goal of protecting taxpayers and the tax ecosystem from IDT refund fraud. Having marked its first year, the Security Summit partnership has yielded several accomplishments, including a real and substantial impact on curbing IDT refund fraud. Specifically, accomplishments realized through the Security Summits include:

- Software providers shared approximately 20 data elements from tax returns with the IRS and the states that could identify possible fraud.

- New protocols were established for all individual tax software customers to update their security credentials to a minimum eight-digit password and establish security questions.
- Industry partners performed regular reviews to identify possible identity theft schemes and report them to the IRS and state partners to be informed of emerging schemes.

Some of the tangible operational benefits from the Security Summit efforts include:

- From January through April 2016, the IRS stopped $1.1 billion in fraudulent refunds claimed by identity thieves on more than 171,000 tax returns, compared to $754 million in fraudulent refunds claimed on 141,000 returns for the same period in 2015. Better data from returns and information about schemes resulted in better internal processing filters that identify fraudulent tax returns.
- Due to leads reported by industry partners from January through May 8, 2016, the IRS suspended approximately 36,000 suspicious returns, claiming $148 million in refunds, for further review. This was more than twice the number of returns stopped for the same period in 2015.
- The number of refunds issued that were detected by banks and financial institutions as potentially fraudulent dropped by 66 percent from 2015 to 2016. This validated that having better data available led to better detection capabilities.

The Security Summit is actively engaged in its initiatives and preparations for the 2017 filing season and beyond. And, at the request of our Security Summit partners, we have taken steps to ensure that the Security Summit will be an ongoing collaboration; namely, by modifying the charter to our Electronic Tax Administration Advisory Council to encompass the Security Summit work and provide a permanent vehicle for the partnership and collaboration to continue in our joint battle against IDT refund fraud.

We agree that IRS processes and procedures used to identify IDT should not be made public. The IRS publishes schemas necessary for filing tax returns on IRS.gov because software developers use these schemas to develop their tax preparation software. New data elements, resulting from the Security Summit, were added to the schemas to assist in fraud detection. While it was preferable to provide some form of secure access to the schemas, a workable solution could not be implemented in time for the 2016 filing season. The IRS made an informed decision to accept the business risk of making the schemas public but not to include any information about the elements in Modernized e-File publications, to provide them as much protection as possible. While knowledge about the existence of data elements in the header schemas might be helpful to fraudsters, those data elements by themselves do not necessarily increase the risk of

fraud. The IRS removed the schema information from IRS.gov in March 2016, shortly after the audit team brought their concern to our attention.

Attached are our comments to your recommendations. If you have any questions, please contact me, or a member of your staff may contact Ken Corbin, Director, Return Integrity and Compliance Services, Wage and Investment Division, at (470) 639-3450.

Attachment

Attachment

Recommendations

The Commissioner, Wage and Investment Division, should:

RECOMMENDATION 1
Permanently remove the data elements from public access to ensure that inappropriate use cannot occur.

CORRECTIVE ACTION
We partially agree with this recommendation. The IRS already removed schema information related to the Authentication data elements from its public website (IRS.gov) on March 14, 2016, and is currently implementing a new secure distribution process for authentication data element information starting in Filing Season 2017. However, the IRS does not believe that this Recommendation, as written, can be fully implemented as we do not retain control over the schemas once they are shared externally. We have previously informed the Treasury Inspector General for Tax Administration of our concerns with the feasibility of implementing this recommendation.

IMPLEMENTATION DATE
N/A

RESPONSIBLE OFFICIAL
N/A

CORRECTIVE ACTION MONITORING PLAN
N/A

RECOMMENDATION 2
Conduct a thorough inspection of its public websites and publications to determine if other data element information is available to the public and ensure that it is removed.

CORRECTIVE ACTION
We partially agree with this recommendation. The IRS took action in March 2016, to remove the Modernized e-File (MeF) schema that contains the data definition of elements designed to combat fraud and identify theft. Removing all data element references from public websites and publications puts burden on the IRS and industry partners who need access to reference material that may or may not contain references to data elements. Furthermore, it is not the reference to the authentication elements that is the highest security concern. Instead, it is the detailed technical information describing how this data will be used to combat fraud, which is closely guarded. Consequently, we will proceed with our current approach of determining the appropriateness of data element information available for public access within the context of a risk-based decision framework.

IMPLEMENTATION DATE
N/A

RESPONSIBLE OFFICIAL
N/A

CORRECTIVE ACTION MONITORING PLAN
N/A

RECOMMENDATION 3
Implement a secure process to provide the data elements to valid parties (*e.g.*, software developers, transmitters, and State users) who have a need to access them.

CORRECTIVE ACTION
We agree with this recommendation. The IRS is implementing a secure process to provide the authentication data elements to valid parties who have a need to access them. Beginning in August 2016, the schema and business rule packages will be delivered to software providers through a Secure Object Repository and Registered User Portal. Also, since the IRS understands the importance of distributing this information to the software community in a timely manner, the IRS is currently leveraging a manual process through the MeF mailbox until the automated solution is available.

IMPLEMENTATION DATE
Implemented

RESPONSIBLE OFFICIAL
Director, Return Integrity and Compliance Services, Wage and Investment Division

CORRECTIVE ACTION MONITORING PLAN
N/A