TREASURY INSPECTOR GENERAL FOR TAX ADMINISTRATION

Electronic Authentication Security Controls Have Improved, but Continued Progress Is Needed to Ensure the Protection of Public-Facing Applications

April 19, 2019

Reference Number: 2019-20-017

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

Redaction Legend:
2 = Law Enforcement Techniques/ Procedures and Guidelines for Law Enforcement Investigations or Prosecutions

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.

ELECTRONIC AUTHENTICATION SECURITY CONTROLS HAVE IMPROVED, BUT CONTINUED PROGRESS IS NEEDED TO ENSURE THE PROTECTION OF PUBLIC-FACING APPLICATIONS

Highlights

Final Report issued on April 19, 2019

Highlights of Reference Number: 2019-20-017 to the Commissioner of Internal Revenue**.**

IMPACT ON TAXPAYERS

The IRS has developed Internet-accessible, public-facing applications to interact with taxpayers for various tax administrative purposes. Because these applications collect, process, and store large amounts of taxpayer data, the IRS has become a target of criminals and identity thieves. Strong electronic authentication controls are needed to prevent identity thieves from succeeding at impersonating taxpayers and gaining improper access to tax records.

WHY TIGTA DID THE AUDIT

This audit was initiated to evaluate whether the IRS has properly implemented secure electronic authentication controls in accordance with Federal standards for public access to IRS online systems.

WHAT TIGTA FOUND

The IRS is making progress at improving electronic authentication controls on its public-facing applications. The IRS established the Electronic Authentication Risk Assessment Compliance Initiative, an ongoing effort to help secure the IRS's public-facing applications. In addition, the IRS continues to take steps to mitigate risks related to using the Short Messaging Service as part of the authentication process.

The IRS performed an analysis of its 52 public-facing applications. As of April 2018, it secured 14 high-risk and eight moderate-risk applications at their assessed (or at a higher) electronic authentication levels of assurance based on the older National Institute of Standards and Technology (NIST) Special Publication 800-63-2, *Electronic Authentication Guideline*. Conversely, 26 (50 percent) applications were not at the assessed electronic authentication level of assurance and not in compliance with the old Federal standards. The remaining four applications were either offline or retired. The IRS is accepting the risks associated with one-half of its public-facing applications not meeting the necessary level of assurance, and TIGTA found that the IRS's rationale for maintaining them at the current level was reasonable based on the IRS's transaction analysis and compensating controls to mitigate risks.

Lastly, the IRS is not yet compliant with new NIST guidelines for public-facing applications, issued in June 2017. The OMB requires compliance with these guidelines within one year of publication. The IRS initiated efforts to develop its Digital Identity Risk Assessment process to meet the new guidelines and started piloting its new processes with one of its high-risk public-facing applications.

WHAT TIGTA RECOMMENDED

TIGTA recommended that the Chief Information Officer ensure that public-facing legacy applications are complying with NIST Special Publication 800-63-3, *Digital Identity Guidelines*, and that an implementation plan includes specific timelines for accomplishing full compliance for legacy applications.

The IRS partially agreed with this recommendation and plans to ensure that public-facing legacy applications are aligned with NIST Special Publication 800-63-3 through its Digital Identity Risk Assessment process. TIGTA concurs in part with the IRS's approach to addressing our recommendation but is concerned that the IRS did not include an implementation plan. Moreover, TIGTA is concerned that the completion date proposed by the IRS will leave it noncompliant with the NIST guidelines until February 2023.

TREASURY INSPECTOR GENERAL
FOR TAX ADMINISTRATION

DEPARTMENT OF THE TREASURY

WASHINGTON, D.C. 20220

April 19, 2019

MEMORANDUM FOR COMMISSIONER OF INTERNAL REVENUE

FROM: Michael E. McKenney
Deputy Inspector General for Audit

SUBJECT: Final Audit Report – Electronic Authentication Security Controls Have Improved, but Continued Progress Is Needed to Ensure the Protection of Public-Facing Applications (Audit # 201820005)

This report presents the results of our review to evaluate the effectiveness of electronic authentication controls over public access to online systems. This audit is included in our Fiscal Year 2019 Annual Audit Plan and addresses the major management challenge of Security Over Taxpayer Data and Protection of Internal Revenue Service Resources.

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

Copies of this report are also being sent to the Internal Revenue Service managers affected by the report recommendation. If you have any questions, please contact me or Danny R. Verneuille, Assistant Inspector General for Audit (Security and Information Technology Services).

Table of Contents

Abbreviations

DIRA	Digital Identity Risk Assessment
E-Authentication	Electronic Authentication
eRA	Electronic Authentication Risk Assessment
FISMA	Federal Information Security Modernization Act
IP PIN	Identity Protection Personal Identification Number
IRS	Internal Revenue Service
NIST	National Institute of Standards and Technology
OMB	Office of Management and Budget
SP	Special Publication
TIGTA	Treasury Inspector General for Tax Administration

Background

The mission of the Internal Revenue Service (IRS) is to "provide America's taxpayers top quality service by helping them understand and meet their tax responsibilities and by applying the tax law with integrity and fairness to all." To achieve its mission, the IRS has developed Internet-accessible, public-facing applications to interact with taxpayers for various tax administrative purposes. For example, the Get Transcript[1] application allows taxpayers to obtain copies of their tax return transcripts. These applications collect, process, and store large amounts of Personally Identifiable Information and tax return data. Because this information is considered extremely valuable, the IRS has become a target of criminals and identity thieves. As such, the IRS must ensure that its applications are secure against threats on the Internet. Of particular concern is how the IRS ensures that only authorized taxpayers can access their information on these public-facing applications. Strong electronic authentication (hereafter referred to as e-authentication) controls are needed to prevent identity thieves from succeeding at impersonating taxpayers and gaining improper access to tax records.

E-authentication is the process of establishing confidence in user identities electronically presented to an information system. E-authentication presents a technical challenge when it involves the remote authentication of individual people over an open network, such as the Internet, for the purpose of electronic government and commerce. The IRS Information Technology Cybersecurity organization is responsible for protecting taxpayer information and the IRS's electronic systems, services, and data from internal and external cybersecurity-related threats.

There are significant examples of the security threats associated with the IRS's public-facing applications. The Treasury Inspector General for Tax Administration (TIGTA) previously reported[2] that two of the IRS's public-facing applications, Get Transcript and Identity Protection Personal Identification Number (IP PIN), were compromised during Fiscal Years 2015 and 2016.

- **Get Transcript Incident** – In May 2015, the IRS discovered that criminals had launched a coordinated attack on its e-authentication portal and used taxpayer personal identification information obtained from sources outside the IRS to impersonate legitimate taxpayers and gain unauthorized access to tax information in the Get Transcript application. TIGTA estimated 724,000 potential unauthorized accesses to

[1] See Appendix VIII for a glossary of terms.
[2] TIGTA, Ref. No. 2016-20-082, *Improvements Are Needed to Strengthen Electronic Authentication Process Controls* (Sept. 2016) and TIGTA, Ref. No. 2017-40-026, *Inconsistent Processes and Procedures Result in Many Victims of Identity Theft Not Receiving Identity Protection Personal Identification Numbers* (Mar. 2017).

taxpayer accounts through the Get Transcript application, which resulted in 252,400 potentially fraudulent tax returns filed related to this incident.

- **IP PIN Incident** – In January 2016, TIGTA issued two e-mail alerts to the IRS stating concerns regarding the fraudulent use of the IP PIN application and recommending that the IRS take it offline until a stronger level of e-authentication was implemented. The IRS had also noted instances in which taxpayers tried to file their tax return with an IP PIN only to find out that identity thieves had already filed a fraudulent tax return. On March 7, 2016, two months after the e-mail alerts, the IRS took the IP PIN application offline. TIGTA identified that, of the 100,463 tax returns filed with an IP PIN for Tax Year 2015, 23,991 (24 percent) of the tax returns with refunds claimed totaling $26 million were potentially fraudulent.

In addition, in September 2017, the credit reporting and monitoring company Equifax announced that hackers gained access to its systems, potentially exposing the personal information of 145.5 million U.S. consumers. While this incident was not directly aimed at the IRS, the IRS was affected because it had a contract with Equifax to provide identity authentication services for IRS online systems. Additionally, the compromise of personal information for that many individuals meant that information, which was once considered private, is now public and cannot be trusted as a means to remotely authenticate an individual's identity.

In February 2018, TIGTA reported[3] that the IRS has made progress to improve its e-authentication controls. The IRS deployed a more rigorous e-authentication process that provides two-factor authentication via a security code sent to text-enabled mobile phones. It completed or updated e-authentication risk assessments for 28 of its public-facing applications to determine appropriate levels of authentication assurance and enhanced its network monitoring and audit log analysis capabilities.

This review was performed in the Information Technology organization at the New Carrollton Federal Building in Lanham, Maryland; in the Cybersecurity and Application Development offices in Dallas, Texas; and with information obtained from the Cybersecurity Contractor Security Assessments function during the period of February through July 2018. 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 objectives. 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.

[3] TIGTA, Ref. No. 2018-20-007, *Electronic Authentication Process Controls Have Been Improved, but Have Not Yet Been Fully Implemented* (Feb. 2018).

Results of Review

Secure Access Electronic Authentication Controls Are Improved

The IRS continues to take steps to mitigate risks that relate to e-authentication of its public-facing applications. In May 2017, the IRS began the Electronic Authentication Risk Assessment (eRA) Compliance Initiative. The initiative is an ongoing effort to help secure the IRS's public-facing applications. As part of this effort, an eRA Compliance Initiative Team comprised of executives from across the IRS performed an analysis on every IRS public-facing application to determine the security risks and impact of the application if a breach was to occur and the technical and business impact of integrating the application with e-authentication. After the IRS performed the analysis of its public-facing applications, it prioritized addressing the issues on applications with high security risks. The IRS has completed this process for all 52 public-facing applications (compared to 28 completed during our prior review).[4]

In June 2018, the IRS was in the process of creating the Applications Development, Identity, and Access Management office to provide direction for all application developmental activities for external identity proofing, authentication, and authorization. It will also provide technical integration and coordination of other public-facing applications in support of the Information Technology organization's secure data access activities both within the IRS and with other Government agencies. This office will work across the Information Technology organization and in alignment with the business operating divisions to identify digital identity and authentication needs across the IRS by:

- Enabling adherence to Federal security standards such as those of the National Institute of Standards and Technology (NIST).
- Supporting the development and delivery of new and existing public-facing applications.
- Collaborating across Federal agencies to implement Federal security initiatives.
- Coordinating and collaborating on cybersecurity and internal identity and access management activities with stakeholders.

In addition, the IRS has taken steps to mitigate risks related to using the Short Messaging Service as part of the authentication process. Evolving threat vectors have rendered the use of the Short Messaging Service as a less secure means to authenticate individuals. Smartphones, which are typically used to receive verifying texts during the authentication process, are prone to theft and

[4] TIGTA, Ref. No. 2018-20-007, *Electronic Authentication Process Controls Have Been Improved, but Have Not Yet Been Fully Implemented* (Feb. 2018).

undetected redirection of text messages. In December 2017, the IRS launched an authentication module within its IRS2Go mobile application. The IRS2Go mobile application provides an alternative means for users to authenticate rather than using Short Messaging Service. Next to providing users a security token, use of an authentication application provides the best available means of authentication.

Following the Equifax breach in September 2017, the IRS considered the potential impact on its public-facing applications and ensured that risk assessments were conducted and appropriate corrective actions were taken. The IRS Information Technology organization collaborated with the TIGTA Office of Investigations and IRS Criminal Investigation to form a Security Review Team. The Security Review Team held several conversations with Equifax and conducted an initial on-site inspection at its headquarters, confirming that IRS data were not compromised and the services provided by Equifax under the contract were not affected. However, the IRS did identify additional high-risk vulnerabilities related to Equifax's data security. The IRS suspended the Equifax contract in October 2017 and replaced Equifax with Experian. The IRS then conducted two security reviews of Experian systems, identified control weaknesses, and requested corrective actions. Of the 19 findings identified, we noted that six moderate-risk issues still require corrective action. The IRS plans to conduct a follow-up review in Fiscal Year 2019.

While the IRS has made progress to improve e-authentication for its public-facing applications, the IRS is in the middle of transitioning between meeting the older Federal Government standards on e-authentication to the newer Federal Government standards on digital identities.

High-Risk, Public-Facing Applications Have Secure Electronic Authentication Based on Older Standards, but Electronic Authentication Risk Assessments Were Not Timely Updated on All Applications

Office of Management and Budget (OMB) Memorandum M-04-04, E-*Authentication Guidance for Federal Agencies*,[5] establishes criteria for determining the risk-based level of authentication assurance required for specific electronic applications and transactions. The guidance requires agencies to review new and existing electronic transactions to ensure that authentication processes provide the appropriate level of assurance and defines four levels of assurance,[6] including the required level of authentication assurance in terms of the likely consequences of an authentication error. As the consequences of an authentication error become more serious, the required level of assurance increases. The guidance also states that agencies should select technologies that meet the corresponding technical requirements.

[5] OMB, OMB M-04-04, *E-Authentication Guidance for Federal Agencies* (Dec. 2003).
[6] See Appendix IV for e-authentication level of assurance requirements.

NIST Special Publication (SP) 800-63-2,[7] published in August 2013, provided technical guidelines to supplement OMB M-04-04. The OMB requires agencies to periodically reassess the information system to ensure that the identity authentication requirements continue to be valid because of technology changes or changes to the agency's business processes. It recommends this be performed as part of the annual information security assessment requirements.

The IRS eRA Guide includes the written procedures for conducting eRAs consistent with this guidance. It requires the eRA panel to conduct a review of all eRA results annually during the Annual Security Control Assessment and a full eRA whenever changes have been made to the transaction or every two years if no changes are made.

The eRA Guide requires completion of the OMB M-04-04 eRA Transaction Worksheet before beginning the assessment of the transaction. The purpose of the worksheet is to focus the assessor on the parts of the transaction that could have the greatest negative impact. To simplify the assessment, the IRS created six tables that narrow the criteria depending on the type of transaction. These tables are calibrated to the technical definitions in OMB and NIST guidance. The table used by the eRA panel for assessing the impact and probability of the transaction should be included in the eRA. The eRA Guide requires that assessors score within prescribed scoring ranges unless there is a compelling reason for another score. Assessors may score the probability higher than prescribed ranges, but the guidance requires that assessors add an explanation or statement of the conditions that warrant the higher rating. Overall, assessors are required to reconcile their assessments so that the process promotes consistency.

High-risk applications had secure e-authentication, and applications not operating at the recommended level of assurance had mitigation plans

As of April 2018, the IRS had 52 public-facing applications. After performing an analysis of these applications, the IRS secured 14 high-risk[8] and eight moderate-risk applications at their assessed (or at a higher) e-authentication levels of assurance.[9] Conversely, 26 (50 percent) applications[10] were not at the assessed e-authentication level of assurance and thus not in compliance with NIST SP 800-63-2. The remaining four applications were either offline or retired.

The IRS is accepting the risks associated with applications not at the assessed e-authentication level of assurance. We found that the IRS's rationale for maintaining them at the current identity

[7] NIST, NIST SP 800-63-2, *Electronic Authentication Guideline* (Aug. 2013).
[8] See Appendix V for a list of applications secured at level of assurance 3 that provide high confidence in the validity of an individual's identity.
[9] TIGTA assigned high- and moderate-risk levels to the applications based on our evaluation of the IRS's implemented e-authentication level of assurances.
[10] See Appendix VI for a list of the 26 public-facing applications that are not at the assessed e-authentication level of assurance.

proofing and authentication method was reasonable based on our review of their risk acceptance documents, which included transaction analysis and current or proposed compensating controls to mitigate risks for these applications.

The IRS completes mitigation plans to assess the risks of applications not operating at the assessed level of assurance. Specifically, the IRS identified and evaluated the risks associated with applications that are not at the assessed level of authentication assurance in order to implement appropriate mitigation controls.[11] **********2********** **********2********** **********2********** **********2**********.[12] *******2******** **********2********** *****2*****.

E-authentication risk assessments were not timely updated, and over one-half did not meet requirements in IRS guidance

The IRS eRA Annual Review process does not ensure that eRAs are updated timely and have followed all the necessary steps required by IRS guidelines. Specifically, the IRS did not timely update the eRAs for four public-facing applications: **********2********** **********2**********2**********. The IRS should have conducted a full eRA assessment on these applications *********2********** to determine the effect of any changes to e-authentication.

This occurred because the Cybersecurity Certification Program Office managed the biennial update of the eRAs based on a "Federal Information Security Modernization Act (FISMA) Year," which typically runs from July 1 to June 30. The guidance TIGTA reviewed does not explicitly state a FISMA year as part of the biennial requirement. In the cases of the four public-facing applications previously discussed, the eRA reviews were completed after June 30, 2015. Because the IRS reviewed applications in FISMA Year 2016, it believed these eRAs were already on schedule for reassessment in FISMA Year 2018. Further, the IRS indicated that these transactions were each reviewed during the annual review of all transactions with no noted changes or new risks to the transactions that would otherwise have required

[11] TIGTA did not evaluate whether the IRS implemented the mitigation controls for applications that did not meet the assessed levels of assurance, nor did we test the effectiveness of any mitigation controls.

[12] **********2********** **********2********** **********2********** **********2**********.

conducting a new eRA. Because the IRS used a FISMA year, rather than a calendar year, the four public-facing applications had review dates that exceeded two years. The Cybersecurity organization has adjusted the practice for the eRAs and is now using calendar years to determine when a reassessment is due. Prior to the end of our audit fieldwork, the IRS provided TIGTA with documents showing that it agreed with our findings and updated the eRAs of the four public-facing applications that were not timely completed. The IRS also provided us with an updated eRA guidance document that now requires a full eRA every three calendar years if no changes are made to the application.

In addition, we evaluated the eRAs of all 52 public-facing applications and found that the eRAs generally complied with NIST SP 800-63-2 and OMB M-04-04 guidelines. However, we found that the eRAs did not always meet the IRS eRA guidance. Specifically, we found one or more issues on 27 (51 percent) of 52 eRAs that included:

- Pre-Assessment Worksheets were not consistently completed. For example, the IRS did not always include mitigation options.
- Meeting minutes were not included with the eRA or the minutes that were included lacked the necessary details for risk-related decisions.
- A business owner's vote was not captured in the eRA report for the e-authentication level of assurance.

These conditions occurred because the controls in place were not adequate. Controls that require management oversight of the eRAs provide assurance that the eRAs are in accordance with the IRS eRA guidance. Without a review process to ensure the full implementation of existing controls and timely updates to the eRAs, the IRS increases the risk that taxpayer records could be compromised and revenue lost due to identity theft.

Public-Facing Applications Are Not Compliant With New Guideline Requirements

In June 2017, NIST SP 800-63-3, *Digital Identity Guidelines*, was published, superseding NIST SP 800-63-2. This new guidance substantially overhauled the guidance under NIST SP 800-63-2, including the elimination of the level of assurance model previously used by Federal agencies and described in OMB M-04-04, instead requiring agencies to individually select levels corresponding to each function being performed.[13]

For legacy systems, the OMB expected agencies to meet the requirements and comply with NIST standards and guidelines within one year of their respective publication dates unless

[13] See Appendix VII for more information on the specific changes to NIST SP 800-63 guidance.

otherwise directed by the OMB.[14] The one-year compliance date for revisions to NIST publications applies only to new or updated material in the publications.

The IRS has not fully implemented NIST SP 800-63-3 requirements on its 52 public-facing applications. While the IRS is currently developing its compliance plan, it is past the one-year mark of implementing NIST SP 800-63-3 requirements as currently required by the OMB.

In August 2017, the IRS indicated that it provided training on the new NIST SP 800-63-3 guidelines. In addition, it conducted the initial workshop with NIST guidelines for key stakeholders. In November 2017, the IRS began planning the Digital Identity Risk Assessment (DIRA) process to address NIST SP 800-63-3 requirements. The DIRA process is a redesign of the IRS's current eRA process. The DIRA process uses a data-driven approach to identity assurance risk determinations and related implementation tailoring of remote identity proofing and authentication requirements for IRS public-facing applications.

IRS management indicated that, since February 2018, they have provided monthly updates to executives and briefings to the eRA Compliance Oversight Team on the new DIRA process. In June 2018, the IRS completed a DIRA assessment tool to collect the parameters of a transaction and calculate the xAL[15] and levels of assurance. As of July 2018, the IRS indicated that it was fully staffed and moving aggressively to complete the DIRA process and started a pilot using the DIRA assessment tool on **********2**********. A second pilot was planned in August 2018 to take another application through the DIRA process. The IRS then planned to begin applying the DIRA process to the remaining applications in September 2018.

In addition, the IRS stated that it believes the OMB is in the process of issuing new guidance.[16] Based on the draft version, the new guidance will provide implementation instructions for NIST SP 800-63-3 and will officially rescind OMB M-04-04. The current OMB M-04-04 requirements do not properly align with the newer NIST SP 800-63-3 standards. NIST SP 800-63-3 does not recognize the four levels of assurance previously used by Federal agencies described in OMB M-04-04. The draft version does not provide a time frame to which Federal agencies will be required to meet this new guidance. Without full implementation of NIST SP 800-63-3, the IRS increases the risk of using inappropriate authentication controls, which could allow unauthorized access and activities, compromised taxpayer records, and revenue lost due to identity theft refund fraud.

[14] OMB Circular No. A-130, *Managing Federal Information as a Strategic Resource* (July 2016).
[15] When described generically or bundled, NIST SP 800-63-3 guidelines refer to Identity Assurance Level, Authenticator Assurance Level, and Federation Assurance Level as xAL. AL = Assurance Level.
[16] The OMB sought public comments on its proposed Memorandum, *Strengthening the Cybersecurity of Federal Agencies through Improved Identity, Credential, and Access Management*, in April 2018.

Recommendation

Recommendation 1***:*** The Chief Information Officer should ensure that public-facing legacy applications are complying with NIST SP 800-63-3 and that an implementation plan includes specific timelines for accomplishing full compliance of legacy applications.

Management's Response: The IRS partially agreed with this recommendation. The IRS Information Technology organization will ensure that public-facing legacy applications are aligned with NIST SP 800-63-3 through the IRS's DIRA process. The DIRA process is a data-driven approach to comprehensively assess IRS public-facing application risk. In accordance with NIST SP 800-63-3, the IRS may determine alternatives to NIST-recommended guidance. As part of the DIRA process, the IRS will document both the justification for any departure from normative requirements and detail the compensating control(s) employed**.**

Office of Audit Comment: TIGTA concurs in part with the IRS's approach to addressing our recommendation. The IRS's response is incomplete in that it did not address our request for an implementation plan with specific timelines on how it will address all public-facing applications. The IRS should create such a plan to ensure that it stays on track in addressing the requirements from NIST SP 800-63-3. We are also concerned with the long timeframe that the IRS proposes to complete the recommendation because, based on that timeframe, the IRS will not be compliant with NIST guidelines until February 2023. We will follow up with the IRS in regard to these concerns.

Appendix I

Detailed Objective, Scope, and Methodology

Our overall objective was to evaluate the effectiveness of e-authentication controls over public access to online systems. To accomplish our objective, we:

I. Determined whether the IRS's risk assessment processes for online systems are in accordance with NIST standards.[1]

- A. Confirmed/identified all IRS online systems.
- B. Obtained the most recent risk assessments for all online systems.
- C. Identified and documented NIST standards for risk assessments of online systems similar to IRS online systems.
- D. Compared IRS risk assessment processes/procedures to NIST criteria and documented exceptions.
- E. For any exceptions identified, consulted with the IRS and obtained additional documentation to identify the causes.

II. Determined the current status of the IRS's efforts to bring all online applications to their appropriate levels of authentication assurance.

- A. Based on a review of IRS risk assessments, documented the current level of authentication assurance for each system.
- B. Identified systems with insufficient levels of assurance.
- C. Consulted with responsible IRS parties to identify the current status of IRS efforts to bring systems with insufficient levels of assurance into compliance.
- D. For any exceptions identified, consulted with the IRS and obtained additional documentation to identify the causes.
- E. Determined the feasibility and reasonableness of the IRS's plans to bring all of its online applications to the appropriate levels of authentication assurance.

[1] See Appendix VIII for a glossary of terms.

III. Determined whether the IRS's multifactor authentication process as it relates to text messaging, while meeting NIST requirements, provides sufficient identity validation assurance.

A. Consulted with the IRS to confirm whether or not text messaging remains an element of its e-authentication process.

B. Researched available information on the risks associated with incorporating text messaging into authentication processes.

C. Determined the prevalence of this issue and whether mitigating controls exist to address this weakness.

IV. Determined whether the IRS considered how the Equifax breach may have affected its e-authentication processes and controls.

A. Consulted with the IRS to determine whether the risks related to the Equifax breach have been considered.

B. Obtained and reviewed any documentation demonstrating IRS consideration and actions related to the Equifax breach's impact on e-authentication, including any revised risk assessments on its online applications.

C. For any exceptions identified, consulted with the IRS and obtained additional documentation to identify the causes.

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: Internal Revenue Manual 10.8.1, *Information Technology Security, Policy and Guidance* (July 2015), and other IRS procedures related to risk assessments, authentication, and authorization controls. We evaluated these controls by interviewing IRS management and staff, reviewing relevant NIST and IRS documentation, and reviewing relevant supporting documentation.

Appendix II

Major Contributors to This Report

Danny R. Verneuille, Assistant Inspector General for Audit (Security and Information Technology Services)
Kent Sagara, Director
Jason McKnight, Acting Audit Manager
Ryan Perry, Acting Audit Manager
Bret Hunter, Lead Auditor
Esther Wilson, Senior Auditor

Appendix III

Report Distribution List

Deputy Commissioner for Operations Support
Deputy Commissioner for Services and Enforcement
Chief Information Officer
Deputy Chief Information Officer for Operations
Associate Chief Information Officer, Cybersecurity
Associate Chief Information Officer, Enterprise Operations
Associate Chief Information Officer, Enterprise Services
Director, Office of Event Driven Architecture
Director, Office of Audit Coordination

Appendix IV

E-Authentication Levels of Assurance Requirements
(Prior to June 2017)

Level of Assurance	Requirements	Level of Confidence
Level 1	No identity proofing is required.	Provides little or no confidence in the validity of an individual's identity.
Level 2	Requires basic identity proofing data, a valid current Government identification number, and a valid financial or utility account number. 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 SP 800-63-2, Electronic Authentication Guideline, and OMB M-04-04, E-Authentication Guidance for Federal Agencies.

Appendix V

Applications Secured at Level of Assurance 3

	Applications Secured at Level of Assurance 3
1	Automated Enrollment
2	eServices Electronic Services Authorization Management 3.1
3	eServices Personal Identification Number Management
4	eServices Taxpayer Identification Number Matching
5	eServices Transcript Delivery System
6	Get Transcript Online
7	Identity Protection Personal Identification Number
8	Modernized e-File Internet Filing Application Assurance Test System Transmitter
9	Modernized e-File Internet Filing Application Production Transmitter
10	Online Account (Balance Due and View Payment Status/History)
11	Secure Object Repository Delivery
12	Taxpayer Digital Communications – Small Business/Self-Employed
13	Taxpayer Digital Communications – Taxpayer Advocate Services
14	Taxpayer Protection Program IDVerify

Source: IRS eRA Compliance Application Disposition List, as of April 5, 2018.

Appendix VI

Public-Facing Applications Not at the Assessed Level of Assurance

	Public-Facing Applications	Description
1	94x On-Line Personal Identification Number Registration	Allows users to obtain a Personal Identification Number to use for electronically signing Forms 94x.
2	Certified Professional Employer Organizations – Professional Employer Organizations	Allows aspiring professional employer organizations to apply for certification online.
3	Certified Professional Employer Organizations – 501(c)(4)	Supports Certified Professional Employer Organizations and Internal Revenue Code Section 501(c)(4) exempt organizations in data collection, identity verification, payment, application processing, and communication related to each registration process.
4	Continuing Education Provider Application and Tool System Administrative	Allows accredited continuing education providers to register with the IRS as a continuing education provider and to track continuing education information.
5	Continuing Education Provider Application and Tool System Principal	Allows accredited continuing education providers to register with the IRS as a continuing education provider and to track continuing education information. This system is used for principal points of contact.
6	ePostcard	Used for online submission of IRS Form 990-N, *Electronic Notice (e-Postcard) for Tax-Exempt Organizations Not Required to File Form 990 or Form 990EZ*, for annual filings for small tax-exempt organizations reporting $50,000 or less.
7	Excise Files Information Retrieval System – Excise Summary Terminal Activity Reporting System (State Government)	Provides an online process for fuel terminal operators and bulk carriers to file information returns. Allows users to upload data, change passwords, download data, and check for errors (State Government entities only).
8	Excise Files Information Retrieval System – Excise Summary Terminal Activity Reporting System (Terminal Operator)	Provides an online process for fuel terminal operators and bulk carriers to file information returns. Allows users to upload data, change passwords, download data, and check for errors (terminal entities only).

	Public-Facing Applications	Description
9	Federal Student Aid Datashare Free Application for Federal Student Aid on the Web	Provides an online means for applicants to retrieve individual Federal tax return information from the IRS while on the Department of Education's website completing the Free Application for Federal Student Aid form. This specific version of the application provides a response to the users request for Federal income tax information via the Department of Education's Federal student aid online application.
10	Federal Student Aid – Datashare Income Driven Repayment	Provides an online means for applicants to retrieve individual Federal tax return information from the IRS while on the Department of Education's website completing the Free Application for Federal Student Aid form. This specific version of the application provides a response to the users request for Federal income tax information via the Department of Education's income-driven repayment plan online calculator.
11	Filing Information Returns Electronically	Used by external trading partners to transmit tax documents to report certain types of payments made as part of their trade or business.
12	First-Time Home Buyer Credit Account Lookup	Allows users to look up the balance of the First-Time Homebuyer Credit, the amount paid back to date, the total amount of the credit received, and annual installment repayment amount.
13	Get Transcript by Mail	Allows taxpayers to request a tax return transcript or a tax account transcript to be mailed to their address of record.
14	IRS Direct Pay (Look up a Payment)	Allows a taxpayer to look up an electronic payment made by IRS Direct Pay, to review the status of the payment, and if available, to cancel or modify the payment.
15	IRS Direct Pay (Make a Payment)	Provides a secure service for taxpayers to pay their taxes for Form 1040, *U.S. Individual Income Tax Return*, series estimated taxes or other associated forms directly from their checking or savings accounts at no cost to the taxpayer.
16	Modernized Internet Employer Identification Number	Allows users to determine whether they need an Employer Identification Number and to apply for an Employer Identification Number.
17	Section 527 Political Action Committee/Political Organization and Filing Disclosure	Enables political organizations to register and submit forms online.

	Public-Facing Applications	Description
18	Taxpayer Digital Communications – Large Business and International	Secure mailbox that allows the exchange of messages between the IRS and business taxpayers.
19	The Foreign Account Tax Compliance Act – Qualified Intermediary	Enables entities to enter into an agreement with the IRS to become a qualified intermediary, withholding foreign partnership, or withholding foreign trust.
20	The Foreign Account Tax Compliance Act Financial Institution – Registration	Allows users to register themselves online as a participating foreign entity.
21	The Foreign Account Tax Compliance Act International Data Exchange System – Form 8966, *FATCA Report*, Download	Allows data to be downloaded from the IRS by Host Country Tax Authorities recipients. FATCA = Foreign Account Tax Compliance Act.
22	The Foreign Account Tax Compliance Act International Data Exchange System – Form 8966 Upload	Allows authorized users to upload Foreign Account Tax Compliance Act data for secure exchange.
23	The Tax Professional Preparer Tax Identification Number System	Allows tax professionals to apply for or renew their Preparer Tax Identification Number.
24	Where's My Amended Return	Allows users to view the status of their amended return.
25	Where's My Refund	Allows taxpayers to check on the status of their current year refund.
26	Where's My Refund – Trace	Allows a taxpayer to track their refund as it moves through the refund process and the postal mail.

Source: TIGTA analysis of the IRS eRA Compliance Application Disposition List, IRS Risk Acceptance Form and Tool documents, and various eRA documents.

Appendix VII

Changes to National Institute of Standards and Technology Special Publication 800-63

NIST SP 800-63-2[1] provided technical guidelines to Federal agencies for the implementation of e-authentication solutions for its systems.[2] It supplemented OMB M-04-04,[3] which defines the four levels of assurance in terms of the consequences of authentication errors and misuse of credentials. Appendix IV presents those four levels of assurance.

Since the last revision of NIST SP 800-63-2 in August 2013, the NIST recognized the need to update its guidance to implement and manage digital identities because digital identity components have evolved substantially. To better align with market-driven business models and innovation, the new revision replaces levels of assurance with ordinals for individual parts of the digital identity flow, providing implementers with more flexibility in their design and operations.

- **Identity Assurance Level:** the identity proofing process and the binding between one or more authenticators and the records pertaining to a specific subscriber.
- **Authenticator Assurance Level:** the authentication process, including how additional factors and authentication mechanisms can impact risk mitigation.
- **Federation Assurance Level:** the assertion used in a federated environment to communicate authentication and attribute information to a relying party.

Within the Identity Assurance processes, the NIST provides further guidance on three varying levels of assertions depending on an agency's risk profile and potential harm caused by an attacker making a successful false claim of identity. Within the Authenticator Assurance processes, the NIST provides further guidance on three different levels of confidence based on the desired effectiveness of the solution.

Rather than being a single, monolithic guideline, NIST SP 800-63-3[4] has been separated in multiple parts, each representing a distinct component of digital identity services. This way, organizations can choose the document that applies to the digital identity services they want to offer. NIST SP 800-63 is now a suite of four documents:

[1] NIST, NIST SP 800-63-2, *Electronic Authentication Guideline* (Aug. 2013).
[2] See Appendix VIII for a glossary of terms.
[3] OMB, OMB M-04-04, *E-Authentication Guidance for Federal Agencies* (Dec. 2003).
[4] NIST, NIST SP 800-63-3, *Digital Identity Guidelines (*June 2017).

- SP 800-63-3, *Digital Identity Guidelines.*
- SP 800-63A, *Enrollment and Identity Proofing.*
- SP 800-63B, *Authentication and Lifecycle Management.*
- SP 800-63C, *Federation and Assertions*.[5]

[5] Information Technology Laboratory, *Understanding the Major Update to NIST SP 800-63: Digital Identity Guidelines* (Aug. 2017).

Appendix VIII

Glossary of Terms

Term	Definition
Annual Security Control Assessment	A formal, annual evaluation of a system against a defined set of controls.
Breach	Any incident that results in unauthorized access of data, applications, services, networks, or devices by bypassing their underlying security mechanisms.
Cybersecurity	A function within the IRS Information Technology organization responsible for ensuring compliance with Federal statutory, legislative, and regulatory requirements governing confidentiality, integrity, and availability of IRS electronic systems, services, and data.
Experian	One of the major credit reporting agencies and provides a number of services for consumers and businesses through their online system.
Federal Information Security Modernization Act	A statute that requires agencies to assess risks to information systems and provide information security protections commensurate with the risks. The FISMA also requires that agencies integrate information security into their capital planning and enterprise architecture processes, conduct annual information systems security reviews of all programs and systems, and report the results of those reviews to the OMB.
Fiscal Year	A 12-consecutive-month period ending on the last day of any month. The Federal Government's fiscal year begins on October 1 and ends on September 30.
Get Transcript	Public-facing application that provides the ability to view, print, or download an individual's tax records using e-authentication.
Identity Proofing	Process that establishes that a subject is who they claim to be.
Identity Protection Personal Identification Number	A six-digit number assigned to eligible taxpayers that helps prevent the misuse of their Social Security Number on fraudulent Federal income tax returns.

Term	Definition
Legacy Systems	A mainframe or minicomputer information system that has been in existence for a long period of time.
National Institute for Standards and Technology	Part of the U.S. Department of Commerce. It develops management, administrative, technical, and physical standards and guidelines for the cost-effective security and privacy of "other than national security"–related information in Federal information systems.
Office of Management and Budget	The largest component of the Executive Office of the President. The management side oversees and coordinates Federal procurement policy, performance and personnel management, information technology, and financial management. In this capacity, it oversees agency management of programs and resources to achieve legislative goals and administration policy.
************2*********** **********2*************	*************************2*************************** *************************2*************************** *************************2*************************** *************************2*************************** *************************2*************************** *********2*********.
Personally Identifiable Information	Information that can be used to distinguish or trace an individual's identity (name, Social Security Number, biometric records, *etc.*), alone or when combined with other personal or identifying information that is linked or linkable to a specific individual (date and place of birth, mother's maiden name, *etc.*).
Portal	A point of entry to a network system that includes a search engine or a collection of links to other sites, usually arranged by topic. It provides the infrastructure that allows users (including IRS employees and taxpayers) to have web-based access to IRS information.

Term	Definition
Risk Assessment	The process of determining risks; that is, determining the extent to which an entity is threatened by potential adverse circumstances or events. Risk assessment for information system–related security risks includes assessment of the susceptibility to adverse impacts through information, (*e.g.*, consideration of the dependence on information, the vulnerabilities in mission and business processes), the effectiveness of risk mitigations, and the assessment of the threat environment with regard to causing such impacts.
Secure Access	A process used to verify users prior to gaining access to online systems.
Security Token	A small hardware device that the owner carries to authorize access to a network service.
Short Messaging Service	A technology for sending short text messages between mobile phones.
Tax Year	The year for which taxpayers file their Federal income tax returns.

Appendix IX

Management's Response to the Draft Report

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

CHIEF INFORMATION OFFICER

FEB 28 2019

MEMORANDUM FOR DEPUTY INSPECTOR GENERAL FOR AUDIT

FROM: S. Gina Garza
Chief Information Officer

SUBJECT: Draft Audit Report Electronic Authentication Security Controls Have Improved, but Continued Progress Is Needed to Ensure Protection Over Public-Facing Applications (audit #201820005) (e-trak # 2019-08558)

Thank you for the opportunity to review your draft audit report and to discuss the observations with the audit team. The IRS is committed to continuously improving our authentication procedures in line with guidelines from the Office of Management and Budget (OMB) and National Institute of Standards and Technology (NIST), which apply to all federal agencies implementing digital identity services.

Over the last several years, we have focused on strengthening our online identity proofing and authentication processes, and we have made significant progress. We are encouraged the report recognizes that the IRS's rationale for maintaining the current identity proofing and authentication methods is reasonable based on this independent review. Our goal is to ensure we use adequate security controls, and where necessary, implement strong mitigations and compensating controls to strengthen the overall security of online services. For example, we are using the new Digital Identity Risk Assessment (DIRA) process as a foundational requirement moving forward.

The IRS will continue strengthening our electronic authentication security controls to provide secure access for taxpayers. The continued support and guidance your team provides is very valuable to us in this regard.

If you have any questions, please contact me at (202) 317-5000 or a member of your staff may contact Carmelita White at (240) 613-2191.

Attachment

Attachment

Draft Audit Report Electronic Authentication Security Controls Have Improved, but Continued Process Is Needed To Ensure Protection Over Public-Facing Applications (Audit # 201820005)

RECOMMENDATION #1: The Chief Information Officer should ensure that public-facing legacy applications are complying with NIST SP 800-63-3 and that an implementation plan includes specific timelines for accomplishing full compliance of legacy applications.

CORRECTIVE ACTION #1: The IRS partially agrees with this recommendation. IRS IT will ensure public-facing legacy applications are aligned with NIST SP 800-63-3 through the IRS's Digital Identity Risk Assessment (DIRA) process. The DIRA process is a data-driven approach to comprehensively assess IRS public-facing application risk. In accordance with NIST SP 800-63-3, the IRS may determine alternatives to the NIST-recommended guidance. As part of the DIRA process, the IRS will document both the justification for any departure from normative requirements and detail the compensating control(s) employed.

IMPLEMENTATION DATE: February 15, 2023

RESPONSIBLE OFFICIALS: Associate Chief Information Officer, Applications Development

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