



*Electronic Authentication Process Controls  
Have Been Improved, but Have Not Yet  
Been Fully Implemented*

**February 5, 2018**

**Reference Number: 2018-20-007**

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

**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](mailto: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/](http://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.



## HIGHLIGHTS

### **ELECTRONIC AUTHENTICATION PROCESS CONTROLS HAVE BEEN IMPROVED, BUT HAVE NOT YET BEEN FULLY IMPLEMENTED**

## Highlights

**Final Report issued on February 5, 2018**

Highlights of Reference Number: 2018-20-007 to the Internal Revenue Service Chief Information Officer.

### **IMPACT ON TAXPAYERS**

As part of its Future State initiative, the IRS continues to enhance its existing online applications and self-help tools by increasing the amount of tax information and services available to taxpayers on IRS.gov. These online applications may process and store Personally Identifiable Information and tax return data for millions of taxpayers. Because this information is considered extremely valuable, the IRS has become a target of cyber criminals and identity thieves. Proper 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 in accordance with Federal standards for public access to IRS online systems and effectively resolved identified control weaknesses.

### **WHAT TIGTA FOUND**

The IRS has made progress in improving its electronic authentication controls. It deployed a more rigorous electronic authentication process that provides two-factor authentication via a security code sent to text-enabled mobile phones. It completed or updated electronic authentication risk assessments for 28 of its online applications to determine appropriate levels of authentication assurance, and enhanced its network monitoring and audit log analysis capabilities.

However, the network monitoring tools that the IRS purchased to improve the prevention and detection of automated attacks were not fully implemented due to issues related to resources, incompatibility, and higher priorities. In addition, controls to prevent a fraudulent user from improperly creating profiles were not fully implemented. Further, the IRS is not fulfilling requirements for monitoring audit logs for suspicious activity due to inadequate processes for generating and reviewing audit log reports as well as not ensuring reports are useful for investigating and responding to suspicious activities.

### **WHAT TIGTA RECOMMENDED**

TIGTA recommended that the IRS Chief Information Officer: 1) prepare a plan of action and milestones to ensure that remaining issues preventing full implementation of the two network monitoring tools are addressed; 2) establish a process to adequately test and subsequently monitor enhancements made to application controls until it can be confirmed that the controls are effective; 3) ensure that electronic authentication audit logs capture adequate data to allow for tracking and analysis of user activity; and 4) ensure that IRS policy is met in regards to audit log report generation and review, and reports are useful for investigation and response to suspicious activities.

The IRS agreed with our recommendations. The IRS plans to develop a plan of action and milestones to ensure that remaining issues preventing full implementation of the two network monitoring tools are addressed; ensure that the amount of time in the eAuthentication Test Plan is expanded so anomalies are captured and resolved; modify the eAuthentication audit log process to capture adequate data for all user transactions; and continue implementing the capability to generate reports from the eAuthentication audit logs, which will enable on-demand audit review, analysis, and after-the-fact investigations.



TREASURY INSPECTOR GENERAL  
FOR TAX ADMINISTRATION

DEPARTMENT OF THE TREASURY  
WASHINGTON, D.C. 20220

February 5, 2018

**MEMORANDUM FOR CHIEF INFORMATION OFFICER**

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

**SUBJECT:** Final Audit Report – Electronic Authentication Process Controls  
Have Been Improved, but Have Not Yet Been Fully Implemented  
(Audit # 201720004)

This report presents the results of our review to evaluate whether the Internal Revenue Service (IRS) has properly implemented secure electronic authentication in accordance with Federal standards for public access to IRS online systems and effectively resolved identified control weaknesses. This audit is included in the Treasury Inspector General for Tax Administration's Fiscal Year 2018 Annual Audit Plan and addresses the major management challenge of Security Over Taxpayer Data and Protection of IRS Resources.

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

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



---

*Electronic Authentication Process Controls Have Been Improved, but Have Not Yet Been Fully Implemented*

---

## *Table of Contents*

<a href="#">Background</a> .....	Page 1
<a href="#">Results of Review</a> .....	Page 5
<a href="#">Progress Has Been Made in Improving Controls for Secure Access Electronic Authentication</a> .....	Page 5
<a href="#">Network Monitoring Tools Purchased to Improve the Prevention and Detection of Automated Attacks Were Not Fully Implemented</a> .....	Page 7
<a href="#">Recommendation 1:</a> .....	Page 8
<a href="#">Electronic Authentication Control Enhancements to Improve the Prevention of Improper Profile Creation and Unauthorized Access to Tax Data Were Not Fully Effective</a> .....	Page 9
<a href="#">Recommendations 2 and 3:</a> .....	Page 11
<a href="#">Requirements for Monitoring Audit Logs for Suspicious Activity Were Not Being Fulfilled</a> .....	Page 11
<a href="#">Recommendation 4:</a> .....	Page 14
 <b>Appendices</b>	
<a href="#">Appendix I – Detailed Objective, Scope, and Methodology</a> .....	Page 15
<a href="#">Appendix II – Major Contributors to This Report</a> .....	Page 17
<a href="#">Appendix III – Report Distribution List</a> .....	Page 18
<a href="#">Appendix IV – List of Online Applications With Reassessed Electronic Authentication Risk Assessments</a> .....	Page 19
<a href="#">Appendix V – Management’s Response to the Draft Report</a> .....	Page 23



*Electronic Authentication Process Controls Have Been Improved, but Have Not Yet Been Fully Implemented*

---

## *Abbreviations*

eRA	Electronic Authentication Risk Assessment
ID	Identification
IRS	Internal Revenue Service
NIST	National Institute of Standards and Technology
PIN	Personal Identification Number
TIGTA	Treasury Inspector General for Tax Administration
TIN	Taxpayer Identification Number
UUID	Universally Unique UserID



---

*Electronic Authentication Process Controls Have Been Improved, but Have Not Yet Been Fully Implemented*

---

## *Background*

As part of its Future State initiative, the Internal Revenue Service (IRS) continues to enhance its existing online applications and self-help tools by increasing the amount of tax information and services available to taxpayers on IRS.gov. These online applications may process and store Personally Identifiable Information and tax return data for millions of taxpayers. Because this information is considered extremely valuable, the IRS has become a target of cyber criminals and identity thieves. As cybersecurity threats against the Federal Government continue to grow, protecting the confidentiality of taxpayer information continues to be a top concern for the IRS.

***The purpose of electronic authentication is to prevent unauthorized access to tax information and fraudulent transactions.***

Electronic authentication is the process of establishing confidence in user identities (*i.e.*, the person is who they say they are) that are electronically accessing an information system. In January 2014, the IRS deployed an electronic authentication solution (hereafter referred to as eAuthentication) as its enterprise identity management and authentication infrastructure to authenticate the identity of public users when they request access to an online application. The IRS designed eAuthentication to provide various levels of assurance when confirming the identity of the person requesting access (*i.e.*, identity proofing) depending on the sensitivity of the data being shared. Its purpose is to prevent taxpayer impersonations and account takeovers by identity thieves.

Three of the IRS's online applications, Get Transcript,<sup>1</sup> Identity Protection Personal Identification Number (PIN),<sup>2</sup> and Online Payment Agreements, authenticated users through eAuthentication. Two of these applications, Get Transcript and Identity Protection PIN, were compromised during Fiscal Years 2015 and 2016. In addition, the Electronic Filing PIN tool on IRS.gov was also compromised.<sup>3</sup>

- **Get Transcript Breach** – In May 2015, the IRS discovered that criminals had launched a coordinated attack on its eAuthentication 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. The

---

<sup>1</sup> The Get Transcript online application provides the ability to view, print, or download an individual's tax records using eAuthentication.

<sup>2</sup> An Identity Protection PIN is a six-digit number assigned to taxpayers who have been victims of identity theft and fraudulent tax refunds. The Identity Protection PIN helps the IRS verify the taxpayer's identity when filing tax returns.

<sup>3</sup> The Electronic Filing PIN tool, at the time of the compromise, did not authenticate users through eAuthentication.



---

## *Electronic Authentication Process Controls Have Been Improved, but Have Not Yet Been Fully Implemented*

---

Treasury Inspector General for Tax Administration's (TIGTA) review of the audit logs estimated there were a total of 724,000 potential unauthorized accesses to taxpayer accounts through the Get Transcript application. The IRS identified that approximately 252,400 potentially fraudulent tax returns were filed related to this incident. The IRS stated that it stopped approximately \$1.55 billion in refunds on 189,400 of these returns; however, the IRS did not stop \$490 million in refunds from being issued on the remaining 63,000 returns. A subsequent TIGTA audit report<sup>4</sup> presented an analysis of the IRS's eAuthentication audit logs that found criminals were using automated attacks to authenticate and obtain copies of tax returns as early as July 2014.

- **Identity Protection PIN Breach** – In January 2016, TIGTA issued two e-mail alerts to the IRS, stating concerns regarding the fraudulent use of the Identity Protection PIN application and recommending that the IRS take it offline until a stronger level of electronic authentication was implemented. The IRS had also noted instances in which taxpayers tried to file their tax return with an Identity Protection 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 Identity Protection PIN application offline.

A subsequent TIGTA audit report<sup>5</sup> presented an analysis of Tax Year 2015 tax returns that were filed with an Identity Protection PIN obtained from the online application. That report identified that, of the 100,463 tax returns filed with an Identity Protection PIN, 23,991 (24 percent) of them with refunds claimed totaling \$26 million were potentially fraudulent.

- **Electronic Filing PIN Breach** – In January 2016, an orchestrated bot attack<sup>6</sup> exploited the IRS Electronic Filing PIN tool on IRS.gov. The Electronic Filing PIN tool is an application that was created to provide taxpayers with a special PIN number that would allow them to electronically file a Federal tax return. Using personal data and Social Security Numbers obtained from sources outside of the IRS, identity thieves used automated malware<sup>7</sup> to generate Electronic Filing PINs. The IRS discovered the attack during the testing of a new tool purchased to detect automated attack activity following the Get Transcript incident.

The IRS estimates the exploitation resulted in the issuance of over 100,000 Electronic Filing PINs that were used to file tax returns claiming over \$100 million dollars in

---

<sup>4</sup> TIGTA, Ref. No. 2016-20-082, *Improvements Are Needed to Strengthen Electronic Authentication Process Controls* (Sept. 2016).

<sup>5</sup> 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).

<sup>6</sup> A software application that runs automated tasks over the Internet, that may be used for beneficial purposes or for attacks.

<sup>7</sup> A program that is inserted into a system, usually covertly, with the intent of compromising the confidentiality, integrity, or availability of the computer's data, applications, or operating system.





---

*Electronic Authentication Process Controls Have Been Improved, but Have Not Yet Been Fully Implemented*

---

fraudulent refunds. As a result of this exploitation, the IRS announced on June 23, 2016, that it had disabled the Electronic Filing PIN tool.

Subsequent to the Get Transcript incident, TIGTA reported<sup>8</sup> that the authentication methods used for the IRS's online applications did not comply with the National Institute of Standards and Technology (NIST) requirements. The electronic authentication processes used to authenticate users of the Get Transcript and Identity Protection PIN applications provided only single-factor authentication<sup>9</sup> despite the NIST standards requiring multifactor authentication<sup>10</sup> for higher risk applications. In addition, the single-factor process used by the IRS to authenticate users did not meet NIST standards for single-factor authentication. As a result, unscrupulous individuals gained unauthorized access to tax account information. Further, TIGTA reported that the IRS's network monitoring tools were not sufficient to detect automated attacks and that the eAuthentication audit logs were not being adequately monitored to detect fraudulent activity.

\*\*\*\*\*2\*\*\*\*\*  
\*\*\*\*\*2\*\*\*\*\*  
\*\*\*\*\*2\*\*\*\*\*. The IRS also acknowledged that it lacked the ability to detect and prevent automated attacks and to adequately monitor system access anomalies. To correct these deficiencies, the IRS planned numerous corrective actions, including:

- Improving security protections at the IRS.gov portal.
- Strengthening authentication requirements.
- Building cyber analytics capabilities.
- Enhancing monitoring to include Get Transcript and protected applications.
- Revisiting electronic authentication risk assessments (eRA) and the overall eRA process.<sup>11</sup>
- Bringing in outside expertise to assess capabilities and test deployment readiness.

This review was performed in the IRS Information Technology organization at the New Carrollton Federal Building in Lanham, Maryland, in the Offices of Cybersecurity and Applications Development; at Accenture's office in Hyattsville, Maryland; and with information obtained from the Office of Online Services, Identity Assurance Office during the period of

---

<sup>8</sup> TIGTA, Ref. No. 2016-40-007, *Improved Tax Return Filing and Tax Account Access Authentication Processes and Procedures Are Needed* (Nov. 2015).

<sup>9</sup> A characteristic of an authentication system or a token that uses one of the three authentication factors to achieve authentication – something you know, something you have, or something you are.

<sup>10</sup> A characteristic of an authentication system or a token that uses two or more authentication factors to achieve authentication.

<sup>11</sup> The process of identifying the risks to system security and determining the probability of occurrence, the resulting impact, and additional safeguards that would mitigate this impact.



*Electronic Authentication Process Controls Have Been Improved, but Have Not Yet Been Fully Implemented*

---

November 2016 through July 2017. We conducted this performance audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objective. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objective. Detailed information on our audit objective, scope, and methodology is presented in Appendix I. Major contributors to the report are listed in Appendix II.



*Electronic Authentication Process Controls Have Been Improved, but Have Not Yet Been Fully Implemented*

*Results of Review*

**Progress Has Been Made in Improving Controls for Secure Access Electronic Authentication**

The IRS has taken a number of steps to provide for more secure authentication and improve network monitoring controls and audit log analysis. Following the discovery of unauthorized access to the Get Transcript application in May 2015, the IRS redesigned its electronic authentication process to provide multifactor remote authentication techniques for its online applications that contain sensitive information. In addition, the IRS completed or reassessed its online applications to determine, or update where necessary, the appropriate level of assurance at which to authenticate its users. The IRS enhanced its network monitoring controls at the IRS.gov portal that were needed to help identify and block malicious activity. \*\*\*\*\*2\*\*\*\*\*  
\*\*\*\*\*2\*\*\*\*\*  
\*\*\*\*\*2\*\*\*\*\*  
\*\*\*\*\*2\*\*\*\*\*.

**The IRS deployed a more rigorous electronic authentication process**

In June 2016, the IRS deployed a more rigorous electronic authentication process that provides identity and authentication services at the NIST Special Publication 800-63-2, *Electronic Authentication Guideline*, assurance levels (Levels 1 through 3). In particular, the IRS improved its authentication processes to achieve compliance with the NIST Level 3 standard.<sup>12</sup> The NIST Level 3 assurance level requires two-factor authentication to create a user profile. Two-factor authentication requires additional credentials beyond username and password for gaining access to the application. The IRS’s new Level 3 authentication involves verification using financial information and having a text-enabled mobile phone associated with the profile. Users must receive a security code text to complete the identity validation process and when returning to access their profiles. The security code is sent to the mobile phone of record (something the user possesses) to verify account access authorization. Users without a text-enabled phone are issued a mailed activation code to the address of record. Upon receipt, the users can complete the identity validation process.

The IRS calls its new means to authenticate and authorize online users as “Secure Access eAuthentication,” which it describes as a rigorous identity verification process that helps protect

---

<sup>12</sup> While this report was being drafted, the NIST released the final version of NIST Special Publication 800-63-3, *Digital Identity Guidelines*, in June 2017. The new guidance replaced NIST Special Publication 800-63-2. During the course of our review, the IRS indicated it would work to ensure it is compliant with the new guidance once issued. We plan to review the IRS’s implementation of the new guidance in a subsequent audit.



---

## *Electronic Authentication Process Controls Have Been Improved, but Have Not Yet Been Fully Implemented*

---

taxpayer data and IRS systems from automated cyberattacks. Before accessing certain IRS online self-help tools, users must first register through Secure Access eAuthentication and authenticate their identities. Thereafter, each time registered users return to the tool, they must enter both their credentials (username and password) plus a security code sent via mobile phone text. This enhanced eAuthentication solution is currently used for five online applications<sup>13</sup> at the appropriate level of assurance to authenticate users.

### **The IRS completed or reassessed the electronic authentication risk assessments for its online applications**

The IRS wants its online applications to use the appropriate level of assurance to conduct identity proofing that is required to protect the sensitivity of the data being shared with the taxpayer. To determine the appropriate level of authentication assurance required by the NIST (Levels 1 through 3), the IRS implemented an eRA process, in accordance with the Office of Management and Budget's Memorandum 04-04, *E-Authentication Guidance for Federal Agencies*, and NIST Special Publication 800-63-2 guidance, that it completes for each new online application or when there is a change made to an application. The IRS indicated that it will renew all eRAs annually to ensure that the identified assurance level remains consistent with the application's online risk profile and any applicable policies. The IRS Cybersecurity organization has responsibility for the eRA process and tracks the initial completion and annual renewals of the eRAs. The IRS has recently completed or updated eRAs for 28<sup>14</sup> of its online applications. For example, the IRS raised the risk assessment level of the Get Transcript online application from moderate to high to more accurately reflect the risk demonstrated during the previous unauthorized accesses.

### **The IRS enhanced its network monitoring and audit log analysis capabilities**

The IRS enhanced its network monitoring controls at the IRS.gov portal that were needed to help identify and block malicious activity. This involved implementing various applications to provide enhanced analysis and monitoring capabilities.

In addition, the IRS enhanced its capabilities to aggregate and correlate system audit logs across different systems. The IRS is able to stream the eAuthentication log data to its Cybersecurity Data Warehouse and hired a contractor to analyze anomalous log activity as part of its Cyber Fraud Analytics group. The scope of the work performed by the contractor includes using advanced analytic techniques to prevent and detect fraudulent activity in IRS online applications. The contractor has been tasked with conducting complex analytics on large transactional data sets to identify anomalous patterns in activity and building and refining predictive models to

---

<sup>13</sup> The five online applications which use eAuthentication at an appropriate level of authentication assurance are Get Transcript, Identity Protection PIN, Online Payment Agreement Individual Master File, Online Account – View Payment Status and History, and Taxpayer Digital Communications.

<sup>14</sup> See Appendix IV for a list of the 28 online applications.



---

*Electronic Authentication Process Controls Have Been Improved, but Have Not Yet Been Fully Implemented*

---

classify or identify anomalous transactions. The total contract cost from April 2017 to April 2018 is \$6.7 million.

The Cyber Fraud Analytics group developed a tool that searches the log data for suspicious activities and potentially fraudulent behavior. \*\*\*\*\*2\*\*\*\*\*

\*\*\*\*\*2\*\*\*\*\*<sup>15</sup>,

\*\*\*\*\*2\*\*\*\*\*. Using this tool, the Cyber Fraud Analytics group identified fraudulent activity in which fraudsters improperly used data stolen from sources outside of the IRS to successfully perpetrate a small number of targeted attacks.

While the IRS took action to enhance controls and security, more work is needed to fully implement the security improvements the IRS indicated were completed since the Get Transcript breach in May 2015. Specifically, additional work is needed in the following areas:

- Fully implement network monitoring tools to improve prevention and detection of automated attacks on online applications.
- Ensure that eAuthentication controls are in place to effectively improve the prevention of improper profile creation and unauthorized access to tax data.
- Ensure that eAuthentication audit log review, analysis, and reporting processes provide useful information to support investigation and response to suspicious activities.

**Network Monitoring Tools Purchased to Improve the Prevention and Detection of Automated Attacks Were Not Fully Implemented**

IRS policy<sup>16</sup> states that automated tools shall be employed to support near real-time analysis of events in support of attack detection, that IRS information systems shall continuously monitor inbound and outbound communications traffic for unusual or unauthorized activities or conditions, and that the systems should alert appropriate IRS personnel when indications of compromise or potential compromise occur.

TIGTA previously reported<sup>17</sup> that the IRS's network monitoring tools were not sufficient to detect automated attacks. In its response to the recommendation for this finding, the IRS stated it had completed this action, as "reflected by the acquisition of specified security centric contractor services and technology tools managed by the IRS Integrated Enterprise Portal contractor." The IRS has made progress towards implementing network monitoring controls, and the enhanced network monitoring controls that are currently in place provide a significant improvement in the

---

<sup>15</sup> A nine-digit number assigned to taxpayers for identification purposes. Depending upon the nature of the taxpayer, the TIN is an Employer Identification Number, a Social Security Number, or an Individual Taxpayer Identification Number.

<sup>16</sup> Internal Revenue Manual 10.8.1, *Information Technology (IT) Security, Policy and Guidance* (July 2015).

<sup>17</sup> TIGTA, Ref. No. 2016-20-082, *Improvements Are Needed to Strengthen Electronic Authentication Process Controls* (Sept. 2016).



*Electronic Authentication Process Controls Have Been Improved, but Have Not Yet Been Fully Implemented*

IRS’s ability to detect and prevent attacks compared to its prior posture. The IRS has implemented the enhanced controls it planned related to network traffic, such as network activity rate controls, increased detection via perimeter controls, and filtering of suspicious Internet Protocol addresses. However, the IRS has not fully completed implementation of other controls specific to analyzing network activity in real-time and identifying automated attacks.

\*\*\*\*\*2\*\*\*\*\*.

- \*\*\*\*\*2\*\*\*\*\* , 18  
 \*\*\*\*\*2\*\*\*\*\* , 19  
 \*\*\*\*\*2\*\*\*\*\* , 20 \*\*\*\*\*.

- \*\*\*\*\*2\*\*\*\*\*  
 \*\*\*\*\*2\*\*\*\*\*  
 \*\*\*\*\*2\*\*\*\*\*.

\*\*\*\*\*2\*\*\*\*\*  
 \*\*\*\*\*2\*\*\*\*\*  
 \*\*\*\*\*2\*\*\*\*\*  
 \*\*\*\*\*2\*\*\*\*\*.

While the IRS is receiving weekly status reports from the contractor implementing these security improvements, a more formalized process for identifying needed tasks, establishing milestones, and detailing required resources would be beneficial. For example, creating a plan of action and milestones, which includes these items, would ensure proper tracking and management visibility of the remaining issues that need to be addressed. Thus, a plan of action and milestones would allow management to determine and direct the resources needed to address the issues timely. If automated attacks are not prevented, more taxpayer records could be compromised and revenue lost to identity theft refund fraud.

**Recommendation**

**Recommendation 1:** The Chief Information Officer should prepare a plan of action and milestones to ensure that remaining issues preventing full implementation of the two network monitoring tools are addressed.

<sup>18</sup> Identifies online activities or requests that are potentially bot-like and collects additional information that is used to validate false positives or legitimate scripting users, but no action is taken.

<sup>19</sup> The security tools are intended to provide protection for many other applications besides eAuthentication. For example, see applications listed in Appendix IV.

<sup>20</sup> Executes automated mitigation action when an online activity or request is identified as bot-like, such as redirecting it to an application error page or other nonsensitive page that does not collect data.



*Electronic Authentication Process Controls Have Been Improved, but Have Not Yet Been Fully Implemented*

**Management’s Response:** The IRS agreed with this recommendation. The IRS will develop a plan of action and milestones to ensure that remaining issues preventing full implementation of the two network monitoring tools are addressed.

**Electronic Authentication Control Enhancements to Improve the Prevention of Improper Profile Creation and Unauthorized Access to Tax Data Were Not Fully Effective**

IRS policy<sup>21</sup> states the IRS information systems shall uniquely identify and authenticate non-IRS users, and that electronic authentication shall be used in accordance with Office of Management and Budget’s Memorandum 04-04 and the E-Government Act of 2002, Section 208.<sup>22</sup>

Following the Get Transcript breach, the IRS took actions to correct the control deficiencies within eAuthentication that allowed the previous fraudulent activities related to creating user profiles and accessing tax records. For example, the IRS indicated by June 7, 2016, it had completed a number of eAuthentication improvements to implement stronger authentication, including preventing a fraudulent user from creating new profiles using TINs that already had previously established eAuthentication profiles. This ability previously allowed cyber criminals to gain access to the tax data of multiple taxpayers. However, not all control enhancements were fully effective. While the IRS stated that it had completed implementation of these controls, our  
\*\*\*\*\*2\*\*\*\*\*  
\*\*\*\*\*2\*\*\*\*\*.

**Controls did not always prevent improper creation of profiles**

The IRS stated that it implemented a control enhancement in July 2015 to enforce a one TIN to  
\*\*\*\*\*2\*\*\*\*\*<sup>23</sup>  
\*\*\*\*\*2\*\*\*\*\*  
\*\*\*\*\*2\*\*\*\*\*  
\*\*\*\*\*2\*\*\*\*\*  
\*\*\*\*\*2\*\*\*\*\*  
\*\*\*\*\*2\*\*\*\*\*  
\*\*\*\*\*2\*\*\*\*\*  
\*\*\*\*\*2\*\*\*\*\*.

We reported this information to the IRS on March 28, 2017. The IRS officials responded that they were aware of the deficiency, and subsequently indicated that they had corrected it on May 14, 2017. However, we are concerned about the IRS’s ability to test and monitor enhanced

<sup>21</sup> Internal Revenue Manual 10.8.1 *Information Technology (IT) Security, Policy and Guidance* (July 2015).

<sup>22</sup> Public Law 107-347, 44 U.S.C. Chapter 36.

<sup>23</sup> \*\*\*\*\*2\*\*\*\*\*  
\*\*\*\*\*2\*\*\*\*\*.



*Electronic Authentication Process Controls Have Been Improved, but Have Not Yet Been Fully Implemented*

application controls based on the amount of time it took to discover and correct this deficiency.

\*\*\*\*\*2\*\*\*\*\*  
\*\*\*\*\*2\*\*\*\*\*

However, it took almost two years for the IRS to discover and address the deficiency in the control's effectiveness.

While the IRS indicated it had completed actions to correct this deficiency, it did not adequately test or monitor the audit logs to determine whether the controls were fully effective at preventing the unauthorized activities.

**Audit log limitations could have contributed to difficulties in ensuring controls were effective**

Based on our review and analysis of the eAuthentication audit logs, we believe limitations with the log data may have contributed to the IRS's difficulty in ensuring controls were effective. The eAuthentication audit logs contain key data, but much of it is combined into one field such that, to make it usable for analysis, would require extra time and effort to extract the key elements. TIGTA had to perform this work of extracting key elements prior to running the tests that determined that IRS's enhanced controls were not fully effective, and it took a significant amount of time and resources.

\*\*\*\*\*2\*\*\*\*\*  
\*\*\*\*\*2\*\*\*\*\*  
\*\*\*\*\*2\*\*\*\*\*  
\*\*\*\*\*2\*\*\*\*\*  
\*\*\*\*\*2\*\*\*\*\*  
\*\*\*\*\*2\*\*\*\*\*  
\*\*\*\*\*2\*\*\*\*\*  
\*\*\*\*\*2\*\*\*\*\*  
\*\*\*\*\*2\*\*\*\*\*  
\*\*\*\*\*2\*\*\*\*\*

\*\*\*\*\*2\*\*\*\*\*  
\*\*\*\*\*2\*\*\*\*\*  
\*\*\*\*\*2\*\*\*\*\*. Without adequate and readily usable audit logs or other means to sufficiently test and monitor controls, the IRS may not discover control deficiencies in a timely manner. If controls are not effective in stopping unauthorized activities, more taxpayer records could be compromised and revenue lost to identity theft refund fraud.





---

*Electronic Authentication Process Controls Have Been Improved, but Have Not Yet Been Fully Implemented*

---

## **Recommendations**

The Chief Information Officer should:

**Recommendation 2:** Establish a process to adequately test and subsequently monitor enhancements made to application controls until it can be confirmed that the controls are effective.

**Management's Response:** The IRS agreed with this recommendation. While the IRS has processes in place to confirm that all corrections to application controls are tested and verified in lower environments, the IRS will ensure the amount of time in the eAuthentication Test Plan is expanded to ensure that any anomalies are captured and resolved.

**Recommendation 3:** Ensure that the eAuthentication audit log captures \*\*\*\*\*2\*\*\*\*\* in a separate field for all user transactions to allow for tracking and analysis of user activity.

**Management's Response:** The IRS agreed with this recommendation. Information Technology staff will modify the eAuthentication audit log process to capture \*\*\*2\*\*\* \*\*2\*\* in a separate field for all user transactions. This modification will be assessed and prioritized along with all other eAuthentication work in the product backlog.

## **Requirements for Monitoring Audit Logs for Suspicious Activity Were Not Being Fulfilled**

NIST Special Publication 800-53 (Revision 4),<sup>24</sup> audit requirement 6, states that organizations need to regularly review and analyze audit records for indications of inappropriate or unusual activity, investigate suspicious activity or suspected violations, report findings to appropriate officials, and take necessary actions.

IRS policy<sup>25</sup> states that the IRS shall employ automated mechanisms to integrate audit review, analysis, and reporting processes to support organizational processes for investigation and response to suspicious activities. IRS information systems shall also provide the ability to summarize voluminous audit log information into a more meaningful format and report generation capability that supports on-demand audit review, analysis, and reporting requirements and after-the-fact investigations of incidents.

---

<sup>24</sup> NIST Special Publication 800-53 (Revision 4), *Security and Privacy Controls for Federal Information Systems and Organizations* (Apr. 2013).

<sup>25</sup> Internal Revenue Manual 10.8.1, *Information Technology (IT) Security, Policy and Guidance* (July 2015).



---

*Electronic Authentication Process Controls Have Been Improved, but Have Not Yet Been Fully Implemented*

---

In addition, IRS policy<sup>26</sup> requires that auditable events be reviewed and updated at a minimum of every two years. NIST guidance<sup>27</sup> also describes the need for periodically reassessing which events are captured. Specifically, it states, “Over time, the events that organizations believe should be audited may change. Reviewing and updating the set of audited events periodically is necessary to ensure that the current set is still necessary and sufficient.”

Further, IRS policy<sup>28</sup> describes the Security Specialist’s role to include reviewing all types of audit logs and observing system activity at least weekly. In addition, the Cybersecurity Operations Standard Operating Procedures roles and responsibilities include reviewing audit logs and observing system activity to detect potential security incidents.

TIGTA previously reported<sup>29</sup> that the Security Operations organization was not monitoring or analyzing system audit logs for eAuthentication in compliance with IRS policy or the eAuthentication Audit Plan. \*\*\*\*\*2\*\*\*\*\*  
\*\*\*\*\*2\*\*\*\*\*  
\*\*\*\*\*2\*\*\*\*\*. These occurrences over the specified thresholds should then be reviewed to determine if action is necessary based on the underlying data. We reported that, if the IRS had been adequately monitoring the audit trails, the automated attacks and improper accesses could have been identified and stopped much sooner.

During this review, Security Operations organization management informed us that, in order to meet IRS policy and eAuthentication Audit Plan requirements, it has utilized contractor and IRS resources to process the audit log data and generate the unusual activity reports specified in the eAuthentication Audit Plan.

**The unusual activity reports were not reviewed**

Although the Security Operations organization generated and e-mailed reports of exceeded thresholds to the application owner and indicated that a response was required, the application owner did not review the reports or provide a response. The Security Operations organization did not follow up on why a response was not provided, indicating to us that the report generation and review process was still being developed. Our review of the unusual activity reports that were generated through the contractor identified that key data were still left combined into one field and, therefore, these reports were not readily useful for review, analysis, or after-the-fact investigations of user activity. This lack of usefulness may have contributed to the application owner’s failure to review them.

---

<sup>26</sup> Internal Revenue Manual 10.8.1, *Information Technology (IT) Security, Policy and Guidance* (July 2015).  
<sup>27</sup> NIST Special Publication 800-53 (Revision 4), *Security and Privacy Controls for Federal Information Systems and Organizations* (Apr. 2013).  
<sup>28</sup> Internal Revenue Manual 10.8.2, *Information Technology (IT) Security, IT Security Roles and Responsibilities* (Sept. 2016).  
<sup>29</sup> TIGTA, Ref. No. 2016-20-082, *Improvements Are Needed to Strengthen Electronic Authentication Process Controls* (Sept. 2016).



---

*Electronic Authentication Process Controls Have Been Improved, but Have Not Yet Been Fully Implemented*

---

In June 2017, the application owner assigned staff to begin reviewing the reports e-mailed by the Security Operations organization. However, a reviewer indicated that instructions were needed on what to do with the suspicious activity once identified. \*\*\*\*\*2\*\*\*\*\*  
\*\*\*\*\*2\*\*\*\*\*  
\*\*\*\*\*2\*\*\*\*\*.

The lack of the capability to generate reports from the eAuthentication audit logs that readily support on-demand audit review, analysis, and after-the-fact investigations of incidents reduces the IRS's ability to discover and address malicious activity and to determine the effectiveness of eAuthentication controls in a timely manner. In addition, not reviewing the unusual activity reports or conducting adequate and timely follow up on the identified suspicious activities could lead to taxpayer records being compromised.

**Criteria to generate certain reports was not reviewed or updated**

As mentioned previously, IRS policy requires auditable events to be reviewed and updated at a minimum of every two years. However, the IRS could not demonstrate this was done in the case of certain auditable events in the eAuthentication Audit Plan as required. It is the responsibility of various parties, including the Security Operations organization, eAuthentication's owner, and the program management office, among others, to meet and review this information. Failure to do so could result in criteria being obsolete, which would limit the effectiveness of the reports being generated.

Our analysis of approximately two months of daily unusual activity reports showed that some specific threshold amounts were not exceeded at all or by very minor amounts, while others were exceeded by very large amounts. This discrepancy indicates that the individual thresholds may be either too low or too high, and therefore, need to be reviewed to ensure their usefulness. The usefulness of the generated reports is in question given the potentially outdated thresholds and the lack of a readily available means to review the underlying data.

\*\*\*\*\*2\*\*\*\*\*  
\*\*\*\*\*2\*\*\*\*\*. The IRS indicated that it had implemented new controls to block excessive attempts in Calendar Year 2014 and further strengthened them in Calendar Year 2016. However, instances of excessive activity still appear on the unusual activity reports. This could indicate that some controls are not working as intended or that event thresholds are inappropriate and outdated. This further reinforces the need to review the unusual activity reports and ensure that the thresholds that trigger report generation are appropriate and kept up to date.

Without periodically reassessing which events are captured and keeping the event thresholds that trigger report generation current, the reports being produced may lose their usefulness. If the reports being produced have limited usefulness, the IRS will not be able to effectively investigate and respond to suspicious activities.



*Electronic Authentication Process Controls Have Been Improved, but Have Not Yet Been Fully Implemented*

---

***Recommendation***

**Recommendation 4:** The Chief Information Officer should ensure that IRS policy is met in regards to audit log report generation and review, that actionable events and threshold triggers are kept current, and reports are useful for investigation and response to suspicious activities.

**Management's Response:** The IRS agreed with this recommendation. Cybersecurity staff will continue to implement the capability to generate reports from the eAuthentication audit logs, which enables on-demand audit review, analysis, and after-the-fact investigations. Additionally, Cybersecurity staff will continue to implement process changes to ensure that actionable events, threshold triggers, and reports are kept current.



---

*Electronic Authentication Process Controls Have Been Improved, but Have Not Yet Been Fully Implemented*

---

## **Appendix I**

### *Detailed Objective, Scope, and Methodology*

Our overall objective was to evaluate whether the IRS has properly implemented secure electronic authentication in accordance with Federal standards for public access to IRS online systems and effectively resolved identified control weaknesses. To accomplish our objective, we:

- I. Determined whether the IRS has implemented secure authentication for remote access to IRS information in compliance with Federal standards.
  - A. Determined the IRS's progress in implementing NIST-compliant eAuthentication for its online tools and applications IRS-wide.
  - B. Determined whether the IRS is using adequate risk assessment procedures that result in the proper identity and authentication assurance levels for its online tools and applications.
- II. Determined whether the IRS has effectively strengthened its network monitoring controls to ensure quick detection of malicious activity and fraudulent transactions occurring over the network.
  - A. Evaluated the IRS's deployment of infrastructure (*i.e.*, the Cyber Analytics initiative) to enhance network monitoring and analytic capabilities along with the new group of employees who can analyze large volumes of data across the IRS and track end-to-end access and usage of online applications.
  - B. Evaluated the IRS's enhancements at the Integrated Enterprise Portal level related to network monitoring.
- III. Determined whether the IRS has effectively strengthened controls in the Secure Access eAuthentication to correct weaknesses that allowed the previous fraudulent activity and unauthorized accesses.
  - A. Determined whether the IRS has established appropriate monitoring parameters in the eAuthentication Audit Plan and has implemented regular review and analysis of the audit records.
  - B. Determined whether the IRS has corrected code deficiencies within the Secure Access eAuthentication that allowed previous fraudulent activity and unauthorized access.
- IV. Determined whether the IRS has effectively implemented corrective actions for recommendations (contained in TIGTA, Ref. No. 2016-20-082, *Improvements Are*



## *Electronic Authentication Process Controls Have Been Improved, but Have Not Yet Been Fully Implemented*

---

*Needed to Strengthen Electronic Authentication Process Controls* (Sept. 2016) to improve controls for preventing unauthorized access to IRS online data sources.

### **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 (IT) Security, Policy and Guidance* (July 2015), and other IRS procedures related to network monitoring, authentication and authorization controls, and audit log analysis and review. We evaluated these controls by interviewing IRS management and staff, reviewing relevant NIST and IRS documentation, and reviewing relevant supporting documentation and application audit logs.



*Electronic Authentication Process Controls Have Been Improved, but Have Not Yet Been Fully Implemented*

---

**Appendix II**

*Major Contributors to This Report*

Danny R. Verneuille, Assistant Inspector General for Audit (Security and Information Technology Services)  
Kent Sagara, Director  
Jody Kitazono, Audit Manager  
Midori Ohno, Lead Auditor  
Steven Stephens, Senior Auditor  
Linda Cieslak, Information Technology Specialist  
Alberto Garza, Manager, Applied Research and Technology



*Electronic Authentication Process Controls Have Been Improved, but Have Not Yet Been Fully Implemented*

---

**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  
Deputy Chief Information Officer for Operations  
Associate Chief Information Officer, Applications Development  
Associate Chief Information Officer, Cybersecurity  
Associate Chief Information Officer, Enterprise Operations  
Director, Enterprise Technology Implementation  
Director, Office of Online Services  
Director, Office of Audit Coordination





*Electronic Authentication Process Controls Have Been Improved, but Have Not Yet Been Fully Implemented*

**Appendix IV**

*List of Online Applications With Reassessed Electronic Authentication Risk Assessments*

	<b>ONLINE APPLICATIONS</b>	<b>DESCRIPTION</b>
1	Affordable Care Act Information Returns	Allows insurance companies, self-insured, large businesses, and businesses that provide health insurance to their employees to electronically file information returns.
2	Certified Professional Employer Organizations	Supports Certified Professional Employer Organizations and 501(c)4 exempt organizations in data collection, identity verification, payment, application processing, and communication related to each registration process.
3	Continuing Education Provider Registration and Tracking System	Tracks continuing education hours earned by tax return preparers.
4	ePostcard	Used for online submission of IRS Form 990-N, <i>Electronic Notice (e-Postcard) for Tax-Exempt Organizations Not Required to File Form 990 or Form 990EZ</i> , for annual filings for small tax-exempt organizations reporting \$50,000 or less.
5	eServices e-File	Allows a third party to apply online to become an electronic filer and allows internal users to input paper applications.
6	eServices Secure Object Repository Transcript Delivery System	Allows users to request transcripts through the Transcript Delivery System that are delivered to the user's individual secure object repository mailbox.
7	eServices External Services Authorization Management	Allows tax filers of Affordable Care Act related tax forms to register for and receive a transmission control code to be used as an authorization identifier for the submissions of tax filer data.



*Electronic Authentication Process Controls Have Been Improved, but Have Not Yet Been Fully Implemented*

	<b>ONLINE APPLICATIONS</b>	<b>DESCRIPTION</b>
8	eServices Secure Object Repository TIN Matching	Allows matching of TINs against IRS records for eServices users with results delivered to the user's individual secure object repository mailbox.
9	Excise Files Information Retrieval System – Excise Summary Terminal Activity Reporting System	Provides an online process for fuel terminal operators and carriers to file information returns.
10	Federal Student Aid – Datashare	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.
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	Foreign Accounts Tax Compliance Act	Provides an online means for financial institutions to submit registration data and agreement forms in order to engage in withholding and reporting activities under the Foreign Accounts Tax Compliance Act.
14	Get Transcript	Allows taxpayers to view and download their tax return information online.
15	IDVerify	Allows taxpayers, who have received a letter from the IRS indicating it has stopped their return due to indications of identity theft, a means to verify their identities.
16	Identity Protection PIN	Enables at-risk taxpayers the opportunity to obtain an Identity Protection PIN online, which is a six-digit number assigned to taxpayers that have been victims of identity theft and which allows their tax returns to be processed without delay.



*Electronic Authentication Process Controls Have Been Improved, but Have Not Yet Been Fully Implemented*

	<b>ONLINE APPLICATIONS</b>	<b>DESCRIPTION</b>
17	Integrated Customer Communications Environment – Modernized Internet Employer Identification Number	Assists taxpayers, businesses, and their representatives to complete the application for an Employer Identification Number using an interactive system, which asks questions tailored to the type of entity the taxpayer is establishing.
18	IRS Direct Pay	Provides a means to make an electronic payment directly to the IRS from a checking or savings account with an electronic confirmation.
19	Modernized e-File Internet Filing Application Production Transmitter	Provides a means to electronically file corporate, exempt organization, individual, partnership, and excise tax returns through the Internet.
20	Online Account – View Payment Status/History	Allows an online capability to display taxpayer payment information.
21	Online Payment Agreement – Business Master File and Power of Attorney	Allows a qualified taxpayer or authorized representative (Power of Attorney) to apply for or modify a previously established installment agreement if the business is unable to pay the liability on time.
22	Online Payment Agreement – Individual Master File	Allows an individual taxpayer the opportunity to apply for or modify a current installment agreement if the individual is unable to pay the liability on time.
23	Order a Transcript (via postal mail)	An interactive web application on IRS.gov for transcript requests that mirrors the telephone applications and sends transcripts to taxpayers via U.S. mail based on the address of record on the Master File. <sup>1</sup>
24	Political Organization Filing and Disclosure and 527 Political Action Committee	Enables political organizations to register and submit forms online.

<sup>1</sup> The IRS database that stores various types of taxpayer account information. This database includes individual, business, and employee plans and exempt organizations data.



*Electronic Authentication Process Controls Have Been Improved, but Have Not Yet Been Fully Implemented*

	<b>ONLINE APPLICATIONS</b>	<b>DESCRIPTION</b>
25	Tax Professional Preparer/Tax Identification Number	Provides online registration and renewal, user fee collection, and issuance of unique identifying numbers for all paid tax preparers.
26	Taxpayer Digital Communications – Small Business and Self-Employed	Enables taxpayers to communicate with IRS employees on small business and self-employment issues over the Internet through several communication channels: secure messaging, text chat, voice chat, video meetings, and co-browsing.
27	Where's My Amended Return	Provides automated access to the processing status of taxpayers' Form 1040X, <i>Amended U.S. Individual Income Tax Return</i> , for the current year and up to three prior years.
28	Where's My Refund	Provides automated access to the processing status of tax refunds for taxpayers who filed a Form 1040, <i>U.S. Individual Income Tax Return</i> , and are eligible to receive a refund.



*Electronic Authentication Process Controls Have Been Improved, but Have Not Yet Been Fully Implemented*

**Appendix V**

*Management's Response to the Draft Report*



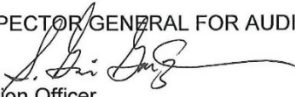
CHIEF INFORMATION OFFICER

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

DEC 13 2017

MEMORANDUM FOR DEPUTY INSPECTOR GENERAL FOR AUDIT

FROM:

S. Gina Garza   
Chief Information Officer

SUBJECT:

Draft Audit Report – Electronic Authentication Process Controls Have Been Improved, but Have Not Yet Been Fully Implemented (Audit # 201720004) (e-trak # 2018-97621)

Thank you for the opportunity to review your draft audit report and meet with the audit team to discuss earlier report observations. We are pleased that your report acknowledged IRS has taken actions to improve security over taxpayer data and follow updated security standards for electronic authentication (eAuthentication) process controls.

The IRS is committed to continuously improving the identification proofing process and capabilities and maintaining required levels of assurance as directed by National Institute of Standards and Technology (NIST) and the Office of Management and Budget (OMB). This is critical to help maintain the integrity, confidentiality and availability of taxpayer data. The attachment lists our detailed planned corrective actions to implement the audit report's recommendations.

The IRS values your continued support and the assistance your organization provides. If you have any questions, please contact me at (202) 317-5000 or a member of your staff may contact Carmelita White, Senior Manager of Program Oversight Coordination, at (240) 613-2191.

Attachment



---

*Electronic Authentication Process Controls Have Been Improved, but Have Not Yet Been Fully Implemented*

---

Attachment

Draft Audit Report - Electronic Authentication Process Controls Have Been Improved, but Have Not Yet Been Fully Implemented (Audit# 201720004) (e-trak # 2018-97621)

**Recommendation 1:** The Chief Information Officer should prepare a plan of action and milestones to ensure that remaining issues preventing full implementation of the two network monitoring tools are addressed.

**CORRECTIVE ACTION:** The IRS agrees with this recommendation. The IRS will develop a Plan of Action and Milestones (POAM) to ensure that remaining issues preventing full implementation of the two network monitoring tools are addressed.

**IMPLEMENTATION DATE:** March 15, 2018

**RESPONSIBLE OFFICIAL(S):** 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.

**RECOMMENDATION 2:** The Chief Information Officer should establish a process to adequately test and subsequently monitor corrections made to application controls until it can be confirmed that the corrections were effective.

**CORRECTIVE ACTION:** The IRS agrees with this recommendation. While the IRS has processes in place to confirm that all corrections to application controls are tested and verified in lower environments the IRS will ensure the amount of time in the eAuthentication Test Plan is expanded to ensure any anomalies are captured and resolved.

**IMPLEMENTATION DATE:** March 15, 2018

**RESPONSIBLE OFFICIAL(S):** Associate Chief Information Officer, Application 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.

**RECOMMENDATION 3:** The Chief Information Officer should ensure that the eAuthentication audit log captures \*\*\*\*\*2\*\*\*\*\* in a separate field for all user transactions to allow for tracking and analysis of user activity.



---

*Electronic Authentication Process Controls Have Been Improved, but Have Not Yet Been Fully Implemented*

---

Attachment

Draft Audit Report - Electronic Authentication Process Controls Have Been Improved, but Have Not Yet Been Fully Implemented (Audit# 201720004) (e-trak # 2018-97621)

**CORRECTIVE ACTION:** The IRS agrees with this recommendation. Information Technology will modify the eAuthentication audit log process to capture \*\*\*\*\*2\*\*\*\*\* in a separate field for all user transactions. This modification will be assessed and prioritized along with all other eAuthentication work in the product backlog.

**IMPLEMENTATION DATE:** March 15, 2018

**RESPONSIBLE OFFICIAL(S):** 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.

**RECOMMENDATION 4:** The Chief Information Officer should ensure that IRS policy is met in regards to audit log report generation and review, that actionable events and threshold triggers are kept current, and reports are useful for investigation and response to suspicious activities.

**CORRECTIVE ACTION:** The IRS agrees with this recommendation. Cybersecurity will continue to implement the capability to generate reports from the eAuthentication audit logs, which enables on-demand audit review, analysis, and after-the-fact investigations. Additionally, Cybersecurity will continue to implement process changes to ensure that actionable events, threshold triggers and reports are kept current.

**IMPLEMENTATION DATE:** October 15, 2018

**RESPONSIBLE OFFICIAL(S):** Associate Chief Information Officer, Cybersecurity

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