TREASURY INSPECTOR GENERAL FOR TAX ADMINISTRATION

Improvements Are Needed to Strengthen Electronic Authentication Process Controls

September 7, 2016

Reference Number: 2016-20-082

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

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

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.

IMPROVEMENTS ARE NEEDED TO STRENGTHEN ELECTRONIC AUTHENTICATION PROCESS CONTROLS

Highlights

Final Report issued on September 7, 2016

Highlights of Reference Number: 2016-20-082 to the Internal Revenue Service Chief Information Officer.

IMPACT ON TAXPAYERS

The risk of unauthorized access to tax accounts will continue to grow as the IRS focuses its efforts on delivering online tools to taxpayers. The IRS estimated that unauthorized accesses may have occurred on an estimated 724,000 taxpayer accounts as a result of fraudulent activity on its online Get Transcript application. The consequences of unauthorized accesses include expanding the taxpayers' preexisting identity theft issues and potential delays in tax return processing while identity theft issues are resolved.

WHY TIGTA DID THE AUDIT

In May 2015, the IRS discovered that fraudsters, using personal information stolen from third parties, had been able to perpetrate an attack on the online Get Transcript application by successfully authenticating via the eAuthentication process. The overall objective of this review was to evaluate the appropriateness of the IRS's response to the Get Transcript incident and the effectiveness of the proposed solution to address the authentication weakness which allowed the incident to occur.

WHAT TIGTA FOUND

The IRS has undertaken a number of steps to improve systems and provide for more secure authentication, including strengthening application and network controls. However, additional actions could further improve security over the eAuthentication process.

Due to poor communication between the IRS and its contractor, the IRS did not have complete knowledge of what was being screened at the Integrated Enterprise Portal, and thus it was unaware of the weaknesses related to detecting automated attacks or which tools it might need to address them. The IRS did not clearly specify which parties, including IRS divisions and contractors, were responsible to detect and prevent such automated attacks.

At the time of the Get Transcript incident, audit log reports were not being adequately monitored. For example, in July 2014, one user attempted to authenticate 902 times within one 24-hour period, which far exceeded the unusual activity trigger. Additionally, the IRS did not have a routine way to correlate audit log information across different repositories. During the audit period, the IRS was able to produce the required reports, but they were just lists of transactions and did not contain summary information that could be used to identify trends. Additionally, some useful transaction information was not captured in eAuthentication audit logs. The IRS also did not provide responsible staff with the tools and training needed to monitor and analyze large amounts of audit log data.

WHAT TIGTA RECOMMENDED

TIGTA recommended that the Chief Information Officer: 1) clarify IRS and contractor responsibilities related to preventing automated attacks; 2) monitor results of controls being put in place to prevent/detect automated attacks; 3) ensure that management implements IRS policy to monitor audit trails; 4) provide security specialists with adequate tools and training; 5) implement enhancements to audit log analysis; 6) compile periodic summary data of eAuthentication volume and unusual activity trigger event transactions; and 7) ensure that audit trails indicate which target application the user intended to access after authenticating.

The IRS agreed with our recommendations. The IRS stated that it has completed four of the seven recommendations. In addition, the IRS plans to provide security specialists with training, produce monthly reports for unusual activity, and ensure that audit trails indicate the target application.

TREASURY INSPECTOR GENERAL
FOR TAX ADMINISTRATION

DEPARTMENT OF THE TREASURY

WASHINGTON, D.C. 20220

September 7, 2016

MEMORANDUM FOR CHIEF INFORMATION OFFICER

FROM: Michael E. McKenney
Deputy Inspector General for Audit

SUBJECT: Final Audit Report – Improvements Are Needed to Strengthen Electronic Authentication Process Controls (Audit # 201520006)

This report presents the results of our review of the Internal Revenue Service's (IRS) response to the Get Transcript incident. The overall objective of this review was to evaluate the appropriateness of the IRS's response to the Get Transcript incident and the effectiveness of the proposed solution to address the authentication weakness which allowed the incident to occur. This audit is included in our Fiscal Year 2016 Annual Audit Plan and addresses the major management challenge of Security for Taxpayer Data and IRS Employees.

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

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 Verneuille, Acting Assistant Inspector General for Audit (Security and Information Technology Services).

Table of Contents

Appendices

Abbreviations

CSIRC	Computer Security Incident Response Center
ID	Identification
IRM	Internal Revenue Manual
IRS	Internal Revenue Service
NIST	National Institute of Standards and Technology
PIN	Personal Identification Number
SAAS	Security Audit and Analysis System
SP	Special Publication
SSN	Social Security Number
TIGTA	Treasury Inspector General for Tax Administration

Background

Taxpayers continue to prefer electronic products and services that enable them to interact and communicate with the Internal Revenue Service (IRS). As such, the IRS has ongoing plans to expand the information and tools available online to assist taxpayers. The IRS's goal is to provide taxpayers with dynamic online account access that includes viewing their recent payments, making minor changes and adjustments to their accounts in real-time, and corresponding digitally with the IRS to respond to notices or complete required forms. Federal regulation also mandates development of such online services. The IRS Restructuring and Reform Act of 1998[1] requires the IRS to allow taxpayers to access tax account information online. Other Federal mandates[2] provide guidance related to implementing electronic access to Government information.

When taxpayers seek to access tax returns or other personal information from the IRS, they are required to authenticate their identities. Authentication in a face-to-face setting, such as when a taxpayer visits a Taxpayer Assistance Center, is straight-forward. A picture identification (ID) is compared with the taxpayer's face. However, online authentication is more difficult because of the lack of physical verification. Electronic authentication is the process of establishing confidence in user identities electronically prior to any transaction with an information system.[3] Electronic authentication also poses a technical challenge when this process involves the remote authentication of individuals over an open network, such as the Internet, for the purpose of electronic Government and commerce.

The risk of unauthorized access to tax accounts will continue to grow as the IRS focuses its efforts on delivering online tools to taxpayers. The increasing number of data breaches in the private and public sectors means more personal information than ever before is available to unscrupulous individuals. Much of these data are detailed enough to enable circumvention of most authentication processes. No single authentication method or process will prevent unscrupulous individuals from filing identity theft tax returns or attempting to inappropriately access IRS services. However, strong authentication processes can reduce the risk of such activity by making it harder and more costly for such individuals to gain access to resources and information. Therefore, it is important that the IRS ensure that its authentication processes are in compliance with National Institute of Standards and Technology (NIST) standards in order to

[1] Pub. L. No. 105-206, 112 Stat. 685 (codified as amended in scattered sections of 2 U.S.C., 5 U.S.C. app., 16 U.S.C., 19 U.S.C., 22 U.S.C., 23 U.S.C., 26 U.S.C., 31 U.S.C., 38 U.S.C., and 49 U.S.C. (2013)).
[2] Office of Management and Budget Memorandum M-04-04 *E-Authentication Guidance for Federal Agencies* (Dec. 2003), and the President's *National Strategy for Trusted Identities in Cyberspace* (Apr. 2011).
[3] Per Office of Management and Budget, M 04-04, *E-Authentication Guidance for Federal Agencies* (Dec. 2003), authentication focuses on confirming a person's identity, based on the reliability of his or her credential. This differs from *authorization* in that authorization focuses on identifying the person's user permissions.

provide the highest degree of assurance required and ensure that authentication processes used to verify individuals' identities are consistent among all methods used to access tax account information.

In January 2014, the IRS implemented the eAuthentication Release 2 application as a means for public users to authenticate their identity with the IRS. Public users requesting access to an online application, such as Get Transcript, are first routed through the eAuthentication application, which acts as an authentication service for IRS online applications. A key component of security and privacy risk is the manner in which individual users identify (proof) themselves to the system and how they subsequently re-authenticate.

The IRS designed eAuthentication to allow for variable levels of assurance regarding identity proofing depending on the risk assessment of the IRS applications being protected. Applications determined to be less risky can be protected at a lower level of assurance, with increased levels of assurance needed to access applications with more sensitive information. The eAuthentication service, once fully developed, will enable the IRS to require multifactor authentication[4] for all applications that warrant a high level of assurance. The eAuthentication identity-proofing process can validate identity information provided by public users against a combination of IRS and third-party data. The applications that used eAuthentication in Calendar Years 2014 and 2015 included Get Transcript, Identity Protection Personal Identification Number (PIN), and Online Payment Agreements.

Get Transcript incident

Starting in January 2014, taxpayers could request tax information online using the IRS's Get Transcript application on its public website (www.IRS.gov). Information requested could include account transactions, line-by-line tax return information, and income reported to the IRS. Taxpayers could generate all five types of transcripts (tax account, tax return, record of account, wage and income, and verification of nonfiling) and either view online, print, or download a transcript. From October 1, 2014, through April 15, 2015, the IRS provided 23 million transcripts to individuals using the Get Transcript application.

In May 2015, the IRS discovered that fraudsters, using personal information stolen from third parties, had been able to perpetrate an attack on the Get Transcript application by authenticating via eAuthentication. In many cases, the fraudsters were able to obtain or view copies of taxpayer transcripts. A previous Treasury Inspector General for Tax Administration (TIGTA) audit[5] found that the IRS did not require multifactor authentication for its online services. The IRS used a multistep, but single-factor, process to authenticate Get Transcript users before tax

[4] Multifactor authentication is a characteristic of an authentication system or a token that uses two or more authentication factors to achieve authentication. The three types of authentication factors are something you know, something you have, and something you are.

[5] TIGTA, Ref. No. 2016-40-007, *Improved Tax Return Filing and Tax Account Access Authentication Processes and Procedures Are Needed* (Nov. 2015).

account information could be accessed. TIGTA also determined that the single-factor process used by the IRS to authenticate taxpayers accessing Get Transcript did not meet NIST standards for single-factor authentication.

To prevent further unauthorized accesses, the IRS removed the Get Transcript application from its website soon after the incident was discovered. Over the next several months, the IRS took steps to enhance the authentication process and re-launched the application in June 2016. During the time the application was offline, taxpayers could still place an order for a transcript online and have it mailed to their address of record.

Get Transcript impact on taxpayers

To date, the IRS, with assistance from TIGTA, has estimated the total number of potential unauthorized accesses to the Get Transcript application at 724,000 taxpayer accounts. The IRS has identified approximately 252,400 potentially fraudulent returns that were filed related to the Get Transcript incident. For these potentially fraudulent returns, the IRS stated that it stopped approximately 189,400 returns that claimed $1.55 billion in refunds from being issued, but unfortunately had issued refunds on 63,000 returns that had $490 million in refund amounts.

The IRS cautioned that its analysis is still ongoing, and some of the apparently unauthorized accesses might yet be determined to have been legitimate. For example, in some instances multiple taxpayer accounts used the same e-mail address, which could be suspicious. However, more research is needed to determine if family members, tax return preparers, or financial institutions could have been using a single e-mail address to attempt to access more than one account. Taking a cautious approach, the IRS notified any and all taxpayers whose accounts met these criteria.

Challenges exist to strengthen authentication while providing an acceptable level of service

While recognizing the importance of security, IRS management has stated that they must balance strengthened authentication processes with ensuring that legitimate taxpayers are able to access services successfully without excessive burden. The IRS estimated that about 22 percent of legitimate taxpayers were unable to successfully authenticate and access the Get Transcript application using the IRS's single-factor authentication process. Federal guidance recognizes the need to balance both costs and benefits of implementing security controls. Security should be appropriate and proportionate to the value of and degree of reliance on the information technology systems and to the severity, probability, and extent of potential harm.[6]

However, because the Get Transcript incident has shown that cyber thieves have the ability to acquire vast amounts of personal information from third parties and use it to access taxpayer

[6] NIST, Special Publication (SP) 800-14, *Generally Accepted Principles and Practices for Securing Information Technology Systems* (Sept. 1996).

information, the IRS has recognized the need to improve its controls over authentication. The IRS anticipates that under the multifactor authentication protocol to be implemented, an even higher percentage of taxpayers will be unable to authenticate. All taxpayers will continue to be able to order a transcript, online or by telephone, and have it mailed to their address of record, if the online tool does not work for them, or if they prefer not to interact with the IRS online.

Actions are in process to strengthen electronic authentication

According to the NIST,[7] securing information and systems against the full spectrum of threats requires the use of multiple, overlapping protection approaches addressing the people, technology, and operational aspects of information systems. This is due to the highly interactive nature of the various systems and networks, and the fact that any single system cannot be adequately secured unless all interconnecting systems are also secured. By using multiple, overlapping protection approaches, the failure or circumvention of any individual protection approach will not leave the system unprotected. Through user training and awareness, well-crafted policies and procedures, and redundancy of protection mechanisms, layered protections enable effective protection of information technology for the purpose of achieving mission objectives.

Consistent with the need to address security through multiple approaches, the IRS has undertaken a number of steps to improve systems and provide for more secure authentication.

- The IRS worked with the United States Digital Service[8] to identify its most pressing needs and implement an appropriate method of delivering secure account multifactor authentication.
- Through the Security Summit initiative, the IRS is working with the States and the tax industry to jointly develop additional steps to combat stolen identity refund fraud.
- The IRS established an Executive position for addressing authentication enterprise-wide. The Executive has authority over all channels of authentication, including face-to-face and telephone, as well as electronic authentication.
- The IRS is developing capabilities to quickly detect malicious activity and fraudulent transactions occurring over the network. This new initiative includes plans to deploy the infrastructure and a 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.

[7] NIST, SP 800-27 Rev. A, *Engineering Principles for Information Technology Security (A Baseline for Achieving Security), Revision A* (June 2004).
[8] The United States Digital Service is part of the Federal Chief Information Officer Team and is tasked with working with agencies to ensure that they have the resources and talent needed to deliver great services on time, on spec, on budget, and with optimal user functionality.

- The IRS completed a number of eAuthentication improvements (called builds) to implement stronger authentication, including requiring that users establish profiles and preventing one-to-many relationships for identity information (for example, an e-mail address cannot be used by more than one user).
- The IRS implemented additional network controls to enhance prevention and detection of automated attacks.
- The IRS started sending a letter to taxpayers when they first create a login and password for any web application on IRS.gov. If the taxpayer was not the one who registered, the notice instructs the taxpayer to contact the IRS.

Because many of the IRS's actions were implemented late in our audit, we were unable to fully assess the effectiveness of its solutions. However, we plan to initiate a new audit in Fiscal Year 2017 to continue our assessment of the effectiveness of IRS solutions to address authentication weaknesses. The IRS requested and received approval for $10 million in Fiscal Year 2016 funding to support the Get Transcript program, which it has applied to multiple improvement projects.

During March 2016, the Cybersecurity Operations organization lost three layers of management or supervisory employees, in part due to a Human Resources initiative to downgrade employee positions. Management turnover within the Cybersecurity Operations organization increases the risk of problems occurring during implementation of these new efforts. The IRS Commissioner has requested that Congress reauthorize streamlined critical pay authority so that key information technology positions can be filled and valued employees retained.

This review was performed at the IRS Information Technology organization offices at the New Carrollton Federal Building in Lanham, Maryland. We obtained information from management and personnel in the Information Technology's Cybersecurity and Enterprise Operations organizations and the Wage and Investment Division offices in Lanham, Maryland, during the period September 2015 through May 2016. We conducted this performance audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objective. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objective. Detailed information on our audit objective, scope, and methodology is presented in Appendix I. Major contributors to the report are listed in Appendix II.

Results of Review

The Get Transcript Incident Response Generally Followed Federal Guidance

On May 14, 2015, the IRS Computer Security Incident Response Center (CSIRC) identified a significant number of undeliverable e-mails sent by the eAuthentication application. The e-mails were the confirmation code e-mails that the system sends individuals as part of the eAuthentication process. Because of suspicious characteristics, the CSIRC reviewed the undeliverable e-mails as a potential computer security incident.

The IRS generally followed NIST guidance related to responding to and reporting the incident. The CSIRC reported the backlog of undeliverable e-mails to the IRS Information Technology Cybersecurity organization. Cybersecurity organization officials reviewed these e-mails and provided the Office of Compliance Analytics information on the suspicious domains that generated the e-mails for further analysis. Cybersecurity organization officials also notified the IRS Office of Privacy, Governmental Liaison, and Disclosure of the breach to Personally Identifiable Information. The IRS Office of Privacy, Governmental Liaison, and Disclosure is responsible for managing incidents involving the loss, theft, or disclosure of Personally Identifiable Information. Cybersecurity organization officials also notified the contractor that administers the IRS Integrated Enterprise Portal, the Department of the Treasury, and the TIGTA Office of Investigations regarding the incident. Other IRS organizations, including Criminal Investigation and the Wage and Investment Division, were provided daily status updates on Get Transcript progress and activities to be performed. IRS business units coordinated to perform an analysis of the cause. Based on the analysis, the Get Transcript application was taken offline until a more secure approach to accessing online taxpayer information could be implemented.

We compared the IRS response to the Get Transcript incident to steps recommended by the NIST.[9] The response involved actions taken by several IRS offices, including the Cybersecurity organization; the Information Technology Enterprise Operations office; the Office of Privacy, Governmental Liaison, and Disclosure; the Office of Compliance Analytics (now part of the Research, Applied Analytics, and Statistics office); and the Wage and Investment Division. The IRS's initial actions to respond to and handle the incident followed Federal guidance. Figure 1 provides a summary of IRS incident handling activities.

[9] NIST, SP 800-61 Revision 2, *Computer Security Incident Handling Guide* p. 42 (Aug. 2012).

Figure 1: Incident Handling Checklist

	Action	Assessment (as of May 2016)
Detection and Analysis		
1.	Determine whether an incident has occurred.	
1.1	Analyze the precursors and indicators.	Completed.
1.2	Look for correlating information.	Partially completed by the IRS. Additional schemes and victims were identified by subsequent TIGTA analysis.
1.3	Perform research, *e.g.*, search engines, knowledge base.	Completed.
1.4	As soon as the handler believes an incident has occurred, begin documenting the investigation and gathering evidence.	Completed.
2.	Prioritize handling the incident based on the relevant factors (functional impact, information impact, recoverability effort, *etc*.).	Completed.
3.	Report the incident to the appropriate internal personnel and external organizations.	Completed.
Containment, Eradication, and Recovery		
4.	Acquire, preserve, secure, and document evidence.	Completed.
5.	Contain the incident.	Completed.
6.	Eradicate the incident.	
6.1	Identify and mitigate all vulnerabilities that were exploited.	In process.
6.2	Remove malware, inappropriate materials, and other components.	Not applicable—no direct incursion into IRS systems.
6.3	If more affected hosts are discovered, *e.g.*, new malware infections, repeat the Detection and Analysis steps (1.1, 1.2) to identify all other affected hosts, then contain (5) and eradicate (6) the incident for them.	Not applicable—no direct incursion into IRS systems.

	Action	Assessment (as of May 2016)
7.	Recover from the incident.	
7.1	Return affected systems to an operationally ready state.	Completed.
7.2	Confirm that the affected systems are functioning normally.	In process.
7.3	If necessary, implement additional monitoring to look for future related activity.	In process.
Post-Incident Activity		
8.	Create a follow-up report.	Partially completed.
9.	Hold a lessons learned meeting (mandatory for major incidents, optional otherwise).	Completed.

Source: *TIGTA analysis of IRS interviews and documents.*

Action 1.2 in Figure 1, related to looking for correlating information to identify the full scope of the incident and other similar incidents, was partially completed. A TIGTA audit[10] subsequent to the incident identified more than 355,000 additional potential victims of the Get Transcript incident than the IRS had previously identified. The results of the audit prompted the IRS to issue a public statement in February 2016 to more fully disclose the number of affected taxpayers and describe its efforts to protect taxpayers from identity theft. Another TIGTA audit[11] notified the IRS about concerns regarding fraudulent uses of the Identity Protection PIN application, which also authenticates users through the eAuthentication system. The IRS and TIGTA continued to monitor the Identity Protection PIN situation and after two months, the IRS took the application offline. The IRS is in the process of implementing a comprehensive program to look for fraudulent transactions occurring over the network with increased capabilities for real-time monitoring and detection of malicious activity.

Action 8 in Figure 1, related to creating a follow-up report, was partially completed. The IRS Cybersecurity organization had a contractor-prepared report evaluating the authentication design supporting the Get Transcript application. The Office of Privacy, Governmental Liaison, and Disclosure had lessons learned meeting notes which listed potential action items. However, NIST guidance states that there are multiple other uses for such a report in addition to its use in handling any similar incidents in the future. A follow-up report can document monetary impacts and can be important in legal cases. Other uses include indicating systemic security weaknesses, assisting in the risk-assessment process, and ultimately leading to the addition of any needed

[10] TIGTA, Ref. No. 2016-40-037, *The Internal Revenue Service Did Not Identify and Assist All Individuals Potentially Affected by the Get Transcript Application Data Breach* p. 7 (May 2016).
[11] TIGTA, Audit No. 201640017, *Identity Protection Personal Identification Numbers – Follow-Up*.

controls. Although certain key information such as an initial assessment of the mode of attack, preliminary impacts, and so forth were included in the documents provided by the IRS, the IRS had not yet consolidated this information so that it could readily be used for the purposes described in NIST guidance.

Network Monitoring Tools Were Not Sufficient to Detect Automated Attacks

IRS guidance[12] 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.

While the IRS does employ extensive monitoring of network resource activity, those efforts were not sufficient to identify characteristics of an automated attack in some of the Get Transcript incident transactions. The attackers were able to mimic taxpayers because they had a significant amount of information on taxpayers prior to the attack, which they had obtained from non-IRS sources. However, some of the transactions were occurring at a speed that was too fast to be from a human user, which should have allowed the IRS to identify the attack sooner.

There was a shared responsibility between IRS offices and a contractor for detecting this type of automated attack. The attack itself involved various IRS systems: the contractor-operated Integrated Enterprise Portal, the IRS network, and the eAuthentication and Get Transcript applications. Due to poor communication between the IRS and its contractor, the IRS did not have complete knowledge of what was being screened at the Integrated Enterprise Portal, thus it was unaware of the weaknesses related to detecting automated attacks or which tools it might need to address them. The IRS did not clearly specify which parties, including IRS divisions and contractors, were responsible to detect and prevent this type of automated attack.

Subsequent to discovering the attack on the Get Transcript application, the IRS initiated several actions to more closely conform to IRS guidance and harden network operations against automated attacks. Figure 2 provides the additional network controls.

[12] Internal Revenue Manual (IRM) 10.8.1, *Information Technology Security, Policy and Guidance* pp. 192-193 (Jul. 2015).

Figure 2: Additional Network Controls Completed or in Process Since May 2015

	Control Description	Implementation Status (as of May 2016)
1	Install an application that determines if human users, not automated processes, are making the transactions.	Completed.
2	Adjust firewall filters to limit the rate of network activity.	Completed.
3	Increase enterprise perimeter controls to detect automated attacks.	Completed.
4	Increase filtering of suspicious Internet Protocol addresses.	Completed.
5	Develop increased capability to analyze network activity in near real-time.	In development.

Source: IRS Integrated Enterprise Portal Security Enhancements for eAuthentication Artifacts showing operations as of March 3, 2016, and e-mails from IRS staff.

In January 2016, these increased capabilities allowed the IRS to identify and halt an ongoing automated attack on its Electronic Filing PIN application on IRS.gov. The IRS identified the issue during the testing of a new tool to detect automated attacks at the IRS perimeter. The IRS reported that it had identified unauthorized attempts involving approximately 464,000 unique Social Security Numbers (SSN), of which about 101,000 SSNs were used to successfully obtain an Electronic Filing PIN. The accesses did not directly result in any disclosure of taxpayer information.

The IRS takes its responsibility to safeguard taxpayer information very seriously. However, these automated attacks were successful in getting access to sensitive taxpayer information and persisted for a period of months undetected because of the lack of sufficient network monitoring and coordinated responsibility efforts at the time of Get Transcript deployment. The consequences to taxpayers include expanding the taxpayers' preexisting identity theft issues and potential delays in tax return processing while identity theft issues are resolved. If automated attacks are not prevented, more taxpayer records could be compromised.

Recommendations

The Chief Information Officer should:

Recommendation 1: Clarify IRS and contractor responsibilities related to preventing automated attacks, including tracking contractor activities and tools with respect to their responsibilities.

Management's Response: The IRS agreed with this recommendation. The IRS has completed this action, reflected by the acquisition of specified security-centric contractor services and technology tools managed by the IRS Integrated Enterprise Portal contractor. The IRS has met and continues to meet with the contractor to clarify its responsibilities. A monthly meeting between the IRS and the contractor takes place at the Executive and at the working group level. These discussions are directly related to the prevention of automated attacks, tools in use, and the procedures implemented by the contractor in the use of these tools to prevent automated attacks.

Recommendation 2: Establish a process to monitor the results and effectiveness of controls to prevent/detect automated attacks.

Management's Response: The IRS agreed with this recommendation. The IRS has completed this action, reflected in the establishment of a new IRS organization within the Cybersecurity Operations organization with responsibility for monitoring protected applications to prevent and detect against automated attacks. This organization has established processes to monitor the results and effectiveness of the layered protections in place.

The eAuthentication Audit Logs Were Captured, but Were Not Adequately Monitored

Audit log monitoring and analysis is a key security control. While the IRS has undertaken an ambitious effort to improve network monitoring and address emerging issues in near real-time, as of March 2016, this program was not yet fully implemented, and in any case, cannot completely take the place of a traditional audit log monitoring program.[13]

According to the NIST,[14] routine log analysis is beneficial for identifying security incidents, policy violations, fraudulent activity, and operational problems. Logs are also useful when performing auditing and forensic analysis, supporting internal investigations, establishing baselines, and identifying operational trends and long-term problems. In addition to these purposes, organizations may store and analyze certain logs to comply with Federal legislation and regulations, including the Federal Information Security Modernization Act of 2014.[15] The NIST recognizes that it is difficult to manage audit logs due to the variability and volume of these records and the resources needed to manage and analyze them.

[13] Traditionally, audit logs are analyzed in a batch mode at regular intervals, *e.g.*, daily. Audit records are archived during that interval for later analysis. Audit analysis tools can also be used in a real-time or near real-time fashion. Such intrusion detection tools are based on audit reduction, attack signature, and variance techniques. Manual review of audit records in real-time is almost never feasible on large multiuser systems due to the volume of records generated.

[14] NIST, SP 800-92, *Guide to Computer Security Log Management* p. ES-1 (Sept. 2006).

[15] Pub. L. No. 113-283. This bill amends chapter 35 of title 44 of the United States Code to provide for reform to Federal information security.

IRS policy[16] identifies security specialists (working in the Security Operations organization) as having the primary role in audit log monitoring and analysis. These responsibilities include: monitoring user or system activities; detecting inappropriate user and system actions that could indicate security incidents; investigating possible security incidents; and notifying management or other personnel as appropriate.

To successfully carry out such responsibilities, NIST[17] guidance states that staff with log management responsibilities should be provided the necessary training regarding their log management responsibilities, as well as skill instruction for the needed resources to support log management. Support also includes providing log management tools and tool documentation, providing technical guidance on log management activities, and disseminating information to log management staff.

The Security Operations organization was not monitoring or analyzing system audit logs for the eAuthentication application in compliance with IRS policy or the eAuthentication Audit Plan. Security Operations organization management agreed that its staff was responsible for producing reports of audit log security events and sending the reports to the business unit program managers to review; however, they also stated that Security Operations organization employees were not responsible for the actual analysis. This statement contradicts the IRM guidance which specifies that security specialists (Security Operations organization) have the primary responsibility for analysis.

In addition, the IRS did not provide the security specialists with the tools and training needed to monitor and analyze large amounts of data. While audit trails from the eAuthentication application were captured by the Security Audit and Analysis System (SAAS),[18] the Security Operations organization was not generating reports for security events that the eAuthentication Audit Plan[19] specified should be investigated as possible security incidents. Moreover, due to inadequate tools to generate reports, the staff was unable to produce and send reports of security events to the business unit program managers. Consequently, audit log security events for the eAuthentication application were not being routinely reviewed in accordance with stated policy.

TIGTA analysis of the IRS's eAuthentication audit logs (using the SAS Enterprise Guide data analysis tool) showed that producing and analyzing the reports related to unusual activity triggers as defined in the eAuthentication Audit Plan could have raised red flags that indicated automated bot activity due to large numbers of transactions taking place very quickly. Thresholds in some

[16] IRM 10.8.2, *Information Technology Security, IT Security Roles and Responsibilities* pp. 35-37 (May 2014), IRM 10.8.3, *Information Technology Security*, *Audit Logging Security Standards* pp. 3-4 (Jul. 2015); and IRS, *Information Technology Cybersecurity Operations Standard Operating Procedure* (Nov. 2014).
[17] NIST, SP 800-92, *Guide to Computer Security Log Management* p. 2-11 (Sept. 2006).
[18] The SAAS is the IRS's enterprise solution to collect audit trails from systems that store or process taxpayer or other sensitive information. SAAS data can be accessed by those responsible for reviewing questionable activities and investigating potential unauthorized access violations.
[19] Audit Plan documents cover audit trail requirements for the application or system as implemented at the IRS.

of the unusual activity triggers were exceeded months before the incident was finally discovered in May 2015. For example, in July 2014, one user attempted to authenticate 902 times within one 24-hour period, which far exceeded the unusual activity trigger. The series of transactions showed that the attempts to authenticate persisted until the user was finally able to pass both the IRS and knowledge-based-authentication identity questions. Closer examination of these types of transactions would have revealed that there was probably an automated process attacking the system.

The SAAS, the system that captures eAuthentication audit logs, does not have adequate reporting or analytic capabilities to support sophisticated on-demand audit review, analysis, and reporting requirements; after-the-fact investigations of incidents; or the ability to correlate audit records across different repositories, as required by Federal guidance. Consequently, Security Operations organization staff used an Excel spreadsheet to download and extract the pertinent log events from the SAAS. However, the millions of records of data were more than Excel could handle. Therefore, the Security Operations organization could not produce reports for its own review or to send to the business unit that owned the application. In November 2015, the Security Operations organization produced its first reports, which it created using the Access database application.

The lack of proper audit log monitoring allowed the criminal activity occurring within the eAuthentication application to go undetected longer than it should have, which led to numerous unauthorized accesses to taxpayer records. If the IRS had been adequately monitoring the audit trails, the automated attacks and improper accesses could have been identified much sooner and stopped.

Recommendations

The Chief Information Officer should:

Recommendation 3: Ensure that Security Operations organization management supports and implements IRM policy with respect to security specialists' role in monitoring and analyzing audit trails.

> ***Management's Response:*** The IRS agreed with this recommendation. The IRS completed this action. Security Operations organization management has implemented the program improvements to ensure that security specialists are fulfilling their role to monitor and analyze audit trails in accordance with IRM policy.

Recommendation 4: Ensure that the IRS provides security specialists with adequate tools and related training to perform analysis as described in audit plans.

> ***Management's Response:*** The IRS agreed with this recommendation. The Associate Chief Information Officer, Cybersecurity, has ensured that security specialists with responsibilities for monitoring the audit plan have been provided adequate tools to

perform analysis. Additional related training has begun and will be completed by March 31, 2017.

Requirements for Correlating Audit Log Information Were Not Fully Implemented

Federal and IRS policies[20] require information systems to employ automated mechanisms to integrate audit review, analysis, and reporting processes to support organizational processes for investigation and response to suspicious activities. These policies also require analysis and correlation of audit records across different repositories to gain organization-wide situational awareness.

Correlation across different systems is important because all relevant information is not contained within only one system's audit log. For example, one system's audit logs may contain account usage information, while other audit logs may capture whether remote connections were employed or whether there was physical access to facilities. Such information can be of use to an incident response team, a help desk, or the information security department. Organizational processes benefiting from integrated audit review, analysis, and reporting include incident response, continuous monitoring, and contingency planning.

The IRS routinely collects audit logs for its critical applications and systems, but it has not fully implemented requirements related to correlating audit log information. Security Operations is the organization within the IRS tasked with primary responsibility for audit log analysis. However, the Security Operations organization was not monitoring or analyzing system audit logs for the eAuthentication application across different repositories. The eAuthentication Audit Plan indicated that key information related to eAuthentication was captured by related supporting systems, not by eAuthentication itself. We asked the IRS how it implemented the requirement to automate and correlate audit trail data from different repositories. The response from the Security Operations organization was that it uses the SAAS for audit log monitoring for eAuthentication. However, the IRS keeps some of the audit log information from platforms and operating systems in another repository, ArcSight. Because the SAAS does not have the capability to support sophisticated analysis or correlate across different systems or repositories, we concluded that the IRS does not have a mechanism to perform such analysis and does not have the ability to correlate audit log data. The lack of integrated and correlated information makes risk management and organizational awareness more difficult.

Looking forward, the IRS has plans to include eAuthentication audit trails as part of its expanded analytics and monitoring capabilities. The IRS provided TIGTA a briefing on its upcoming capabilities in March 2016 and advised TIGTA at that time that testing had begun on parts of the monitoring process. The briefing described the processes and technologies the IRS is in the

[20] NIST, SP 800-53 Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations* p. F-45 (Apr. 2013); and IRM 10.8.1, *Information Technology Security, Policy and Guidance* p. 50 (Jul. 2015).

process of implementing during Fiscal Years 2016 and 2017. The briefing explained how the IRS plans to track transactions through the Integrated Enterprise Portal, through eAuthentication, and down to the final application level. The briefing also contained some sample metrics/behavioral indicators related to anomaly, threat, and incident detection that the IRS may use in its monitoring efforts. In May 2016, the IRS told TIGTA that it had hired a contractor to monitor some information 24 hours a day, which is a key step in its monitoring strategy. While the expanded analytics and monitoring effort is in its early stages and is limited to only certain applications (including eAuthentication), if it proves effective, it holds promise for correlating audit trails.

Recommendation

Recommendation 5: The Chief Information Officer should implement enhancements to audit log analysis to provide for automated mechanisms to integrate audit review, analysis, and reporting processes and to correlate audit records across different repositories to gain organization-wide situational awareness.

> ***Management's Response:*** The IRS agreed with this recommendation. The IRS has completed this action, reflected in the automated capability to: 1) collect and aggregate transaction logs in a secure data repository; 2) automate the creation of analytic datasets for in-depth analysis, correlation of transactions attempted to eAuthentication, and gain access to protected applications; 3) automate the indexing, filtering, and correlation of transactions used by 24 x 7 monitoring of eAuthentication; and 4) establish reporting and management processes for security-related events.

Additional Information Would Improve the Usefulness of Audit Log Reports

Periodic reports on audit log trends can help to identify anomalies that could be indicative of malware or other problems. The NIST states[21] one of the purposes of audit log reporting is to summarize significant activity over a particular period of time or to record detailed information related to a particular event or series of events.

IRS policy explains the basic information that should be captured in audit logs by all systems. The policy states that these audit events represent the minimum set of events. When a system is new, the IRS must make an initial decision related to which audit events to capture in anticipation of how the data will be used. This initial decision is generally made prior to implementing the system, but it is supposed to be reassessed on a periodic basis. IRS policy[22] requires that auditable events be reviewed and updated at a minimum of every two years. NIST

[21] NIST SP 800-92, *Guide to Computer Security Log Management* pp. 3-5 (Sept. 2006).
[22] IRM 10.8.1 *Information Technology Security, Policy and Guidance* p. 49 (Jul. 2015).

guidance[23] also describes the need for periodically reassessing which events are captured. NIST 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."

In November 2015, the Security Operations organization began to produce reports from the eAuthentication audit logs that listed suspicious transactions as described in the eAuthentication Audit Plan criteria for unusual activity. However, the reports were just lists of transactions and did not contain summary information on the number of events. For example, if a trigger is more than three unsuccessful logons by a user, the report currently lists all of the unsuccessful logon attempts consecutively for all transactions that meet the criteria. This is necessary information to investigate the transactions and determine if any action needs to be taken in response to the events. However, it is also useful to compile summary data and compare trigger event quantities over time, such as monthly, to look for trends. For example, such data could include total unsuccessful logon attempts by individual users over the period of a month, how many total individuals had unsuccessful logon attempts, and how this compares to the previous period and the same period from the prior year. It is easier to identify trends when reviewing summary data than from a list of hundreds or thousands of consecutive transactions.

Additionally, during the authentication process, eAuthentication does not currently capture an event indicating it was the Get Transcript application for which the user was authenticating. In terms of the eAuthentication audit log, it could also have been either of the other two applications currently using eAuthentication for authentication. In looking at the IRS's eAuthentication data after the Get Transcript incident occurred, analysis was complicated in part because it could not be determined from the eAuthentication logs which application was accessed by the users. Because there were three active applications using the eAuthentication service (Get Transcript, Identity Protection PIN, and Online Payment Agreements), investigators had to consider the audit logs for all three applications in their analysis to determine which one had been accessed through the eAuthentication service process. Considering that the IRS intends to expand use of the eAuthentication service to other applications it will offer taxpayers, this will also expand the number of target applications and further complicate tracking user issues or incidents.

The IRS did not foresee the need for producing summary reports to aid in trend identification or capturing an event related to the transaction to access the target application. Spikes or anomalies in transactions that could be identified through trend analysis are not as evident when data are not aggregated. More meaningful information on transactions can help identify whether the IRS has been successful in stopping all suspicious activity that it previously identified, in addition to helping to identify any future incidents. Also, the lack of data on the target application that users intended to access complicates analysis and investigation and obscures underlying data

[23] NIST 800-53 Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations* p. F-42 (Apr. 2013).

trends. This problem will expand as more applications are added to use this enterprise designated authentication solution.

Recommendations

The Chief Information Officer should:

Recommendation 6: Compile periodic summary data of eAuthentication volume and unusual activity trigger event transactions, so that data can be compared over time to identify trends or outliers.

> **Management's Response:** The IRS agreed with this recommendation. The Cybersecurity organization will produce monthly reports that aggregate information for the unusual activity trigger event transactions identified in the eAuthentication Audit Plan.

Recommendation 7: Ensure that the eAuthentication audit trail includes an EventID that indicates which target application the user intended to access after authenticating.

> **Management's Response:** The IRS agreed with this recommendation. The IRS will ensure that SAAS events are captured for: 1) ID Proofing to provide target application information; 2) activation and security codes; and 3) SiteMinder target application information.

Appendix I

Detailed Objective, Scope, and Methodology

Our overall objective was to evaluate the appropriateness of the IRS's response to the Get Transcript incident and the effectiveness of the proposed solution to address the authentication weakness which allowed the incident to occur. To accomplish our objective, we:

I. Determined whether the IRS responded to and handled the Get Transcript incident appropriately.

   A. Determined whether the IRS's incident response and reporting policies and procedures were in accordance with Federal standards.

   B. Determined whether the IRS complied with Federal incident response and reporting requirements in response to the Get Transcript breach.

      1. Obtained and reviewed the incident response reports.

      2. Described the steps the IRS took to report and mitigate the cyberattack, and determined whether the IRS's response was in accordance with Federal requirements.

      3. Reviewed the documentation of steps taken by the CSIRC to remediate the cyberattack and determined whether they were effective or whether more should have been done.

   C. Determined whether the CSIRC should implement improvements in order to be able to identify similar cyberattacks sooner.

II. Determined whether the IRS is monitoring its network traffic and audit logs in compliance with Federal requirements.

   A. Determined whether the IRS's policies and procedures for monitoring network traffic and audit logs are in accordance with Federal standards.

   B. Determined whether the IRS was monitoring network traffic in accordance with its policy.

   C. Determined whether the IRS was monitoring audit log transactions related to the eAuthentication and Get Transcript applications in accordance with its policy.

   D. Determined why the IRS did not identify the incident through means other than an e-mail backlog.

III. Evaluated the IRS's plans to improve the eAuthentication solution and its overall ability to prevent and detect future cyberattacks to minimize the chance of another breach.

A. Obtained any updated information as it became available on the scope and impact of the Get Transcript breach.

B. Determined whether the IRS is on track to implement eAuthentication assurance Level 3 in Fiscal Year 2016 considering financial and technological challenges, and whether the IRS's solution will meet the NIST standard.

C. Determined whether changes are needed to the eAuthentication application's rules to help prevent fraudulent activity. We obtained the IRS eAuthentication and Get Transcript audit trails from the SAAS for the period January 1, 2014, through May 30, 2015, to use in our analysis. We evaluated the reliability of the data and concluded that the files were sufficiently reliable for identifying the taxpayer IDs that were associated with eAuthentication and Get Transcript products and/or were identified by the IRS as breached. Comparisons of record counts, data type validity tests, and analytical tests were conducted to perform the data reliability and validation. The data were used to identify examples of potentially suspicious transactions as described in the eAuthentication Audit Plan.

1. Evaluated the data from the eAuthentication audit trails that indicated potential misuse of eAuthentication user IDs and Taxpayer Identification Numbers.

2. Determined whether these instances were related to the breach.

D. Evaluated the IRS's plans for preventing/detecting cyberattacks and determined whether they are sufficient or more should be done.

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: IRM Sections 10.8.1, 10.8.3, and other IRS procedures related to incident response and network monitoring. We evaluated these controls by interviewing IRS management and staff; reviewing relevant Office of Management and Budget, NIST, and IRS documentation; and reviewing relevant supporting documentation.

Appendix II

Major Contributors to This Report

Danny Verneuille, Acting Assistant Inspector General for Audit (Security and Information Technology Services)
Kent Sagara, Director
Jody Kitazono, Audit Manager
Mary Jankowski, Lead Auditor
Midori Ohno, Senior Auditor
Larry Reimer, Senior Auditor

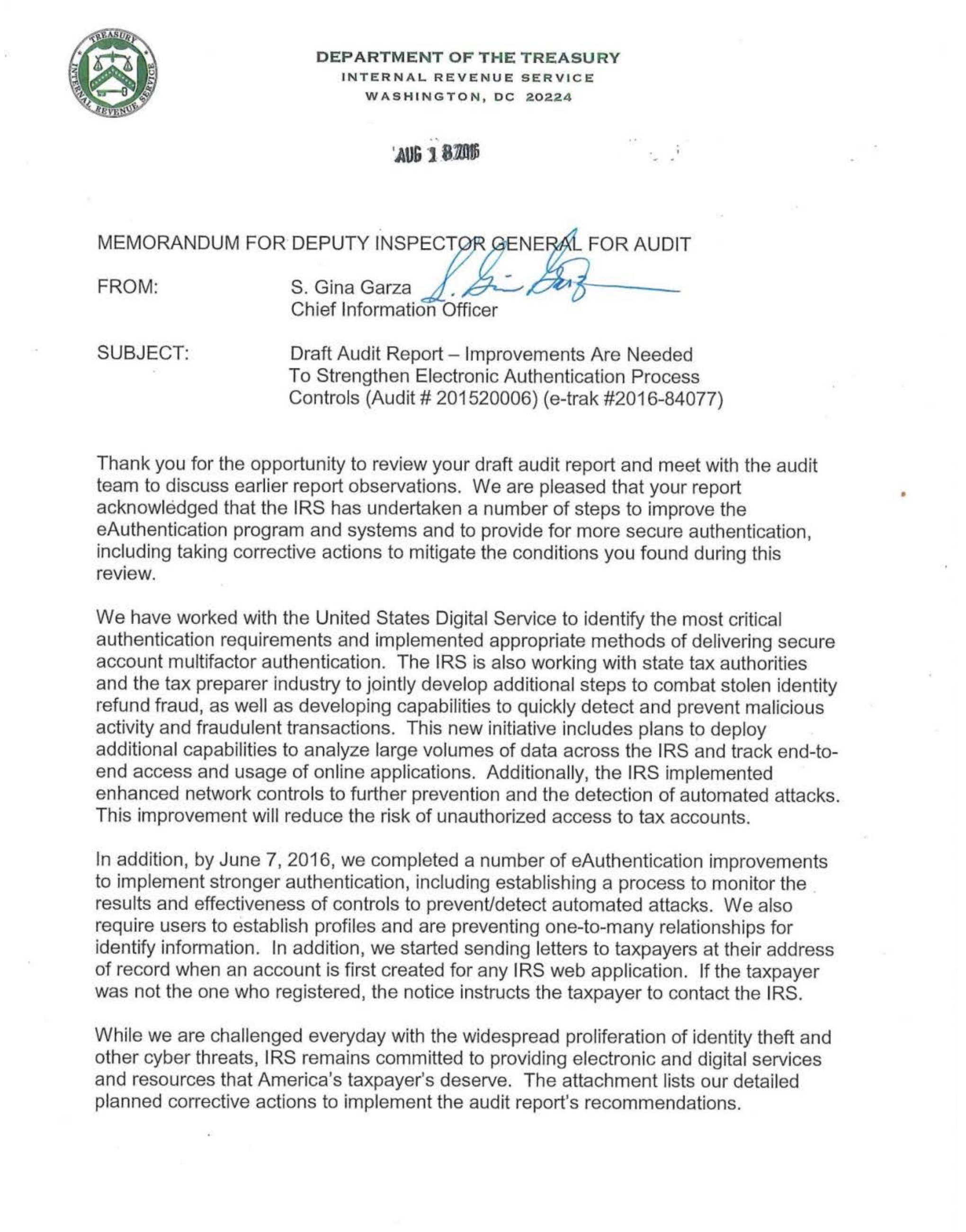
Appendix III

Report Distribution List

Commissioner
Officer of the Commissioner – Attn: Chief of Staff
Deputy Commissioner for Operations Support
Deputy Commissioner for Services and Enforcement
Commissioner, Wage and Investment Division
Associate Chief Information Officer, Cybersecurity
Director, Customer Account Services, Wage and Investment Division
Director, Office of Online Services
Director, Privacy and Policy Compliance
Director, Research, Applied Analytics, and Statistics
Director, Office of Audit Coordination

Appendix IV

Management's Response to the Draft Report



DEPARTMENT OF THE TREASURY
INTERNAL REVENUE SERVICE
WASHINGTON, DC 20224

AUG 1 8 2016

MEMORANDUM FOR DEPUTY INSPECTOR GENERAL FOR AUDIT

FROM: S. Gina Garza
Chief Information Officer

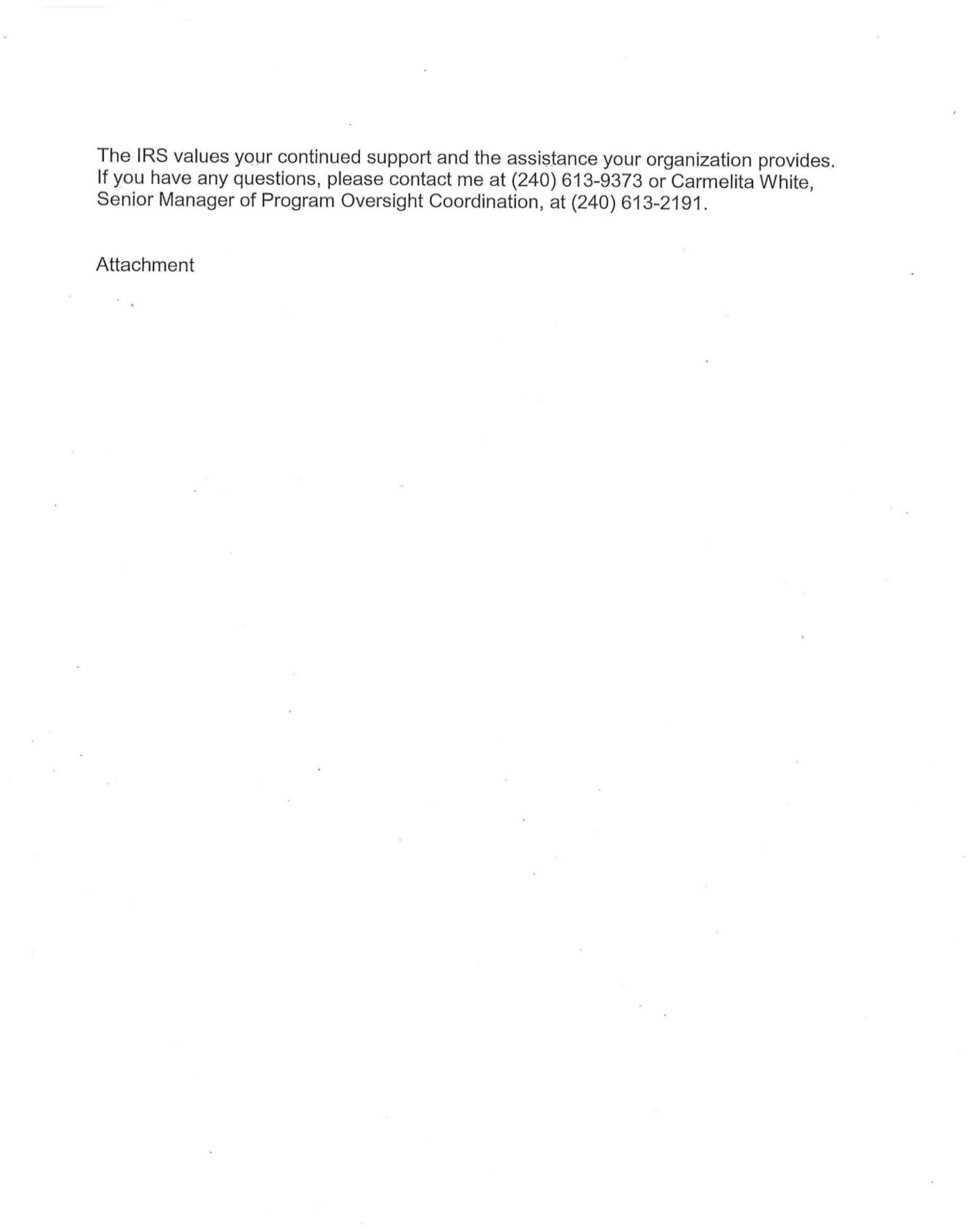
SUBJECT: Draft Audit Report – Improvements Are Needed To Strengthen Electronic Authentication Process Controls (Audit # 201520006) (e-trak #2016-84077)

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 that the IRS has undertaken a number of steps to improve the eAuthentication program and systems and to provide for more secure authentication, including taking corrective actions to mitigate the conditions you found during this review.

We have worked with the United States Digital Service to identify the most critical authentication requirements and implemented appropriate methods of delivering secure account multifactor authentication. The IRS is also working with state tax authorities and the tax preparer industry to jointly develop additional steps to combat stolen identity refund fraud, as well as developing capabilities to quickly detect and prevent malicious activity and fraudulent transactions. This new initiative includes plans to deploy additional capabilities to analyze large volumes of data across the IRS and track end-to-end access and usage of online applications. Additionally, the IRS implemented enhanced network controls to further prevention and the detection of automated attacks. This improvement will reduce the risk of unauthorized access to tax accounts.

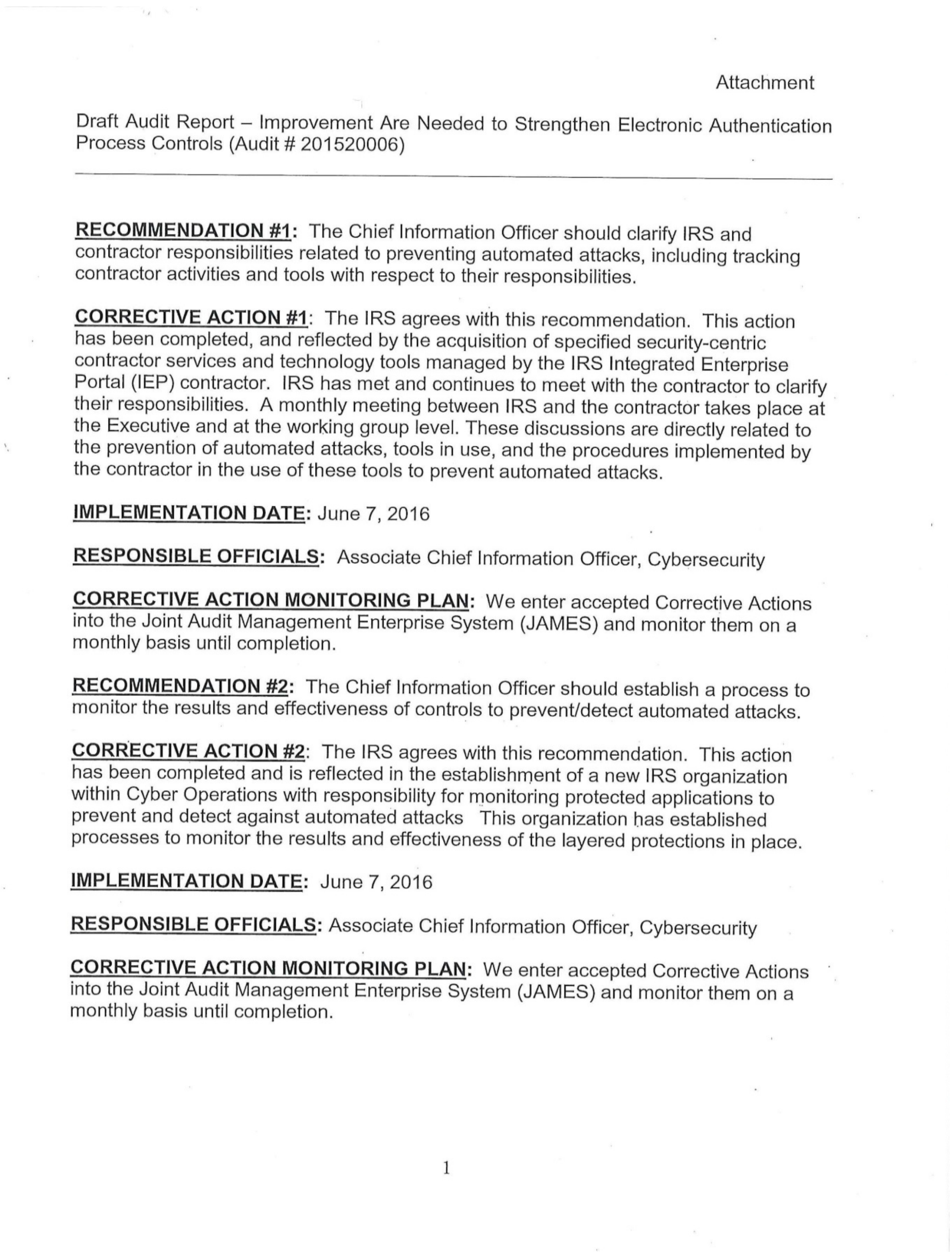
In addition, by June 7, 2016, we completed a number of eAuthentication improvements to implement stronger authentication, including establishing a process to monitor the results and effectiveness of controls to prevent/detect automated attacks. We also require users to establish profiles and are preventing one-to-many relationships for identify information. In addition, we started sending letters to taxpayers at their address of record when an account is first created for any IRS web application. If the taxpayer was not the one who registered, the notice instructs the taxpayer to contact the IRS.

While we are challenged everyday with the widespread proliferation of identity theft and other cyber threats, IRS remains committed to providing electronic and digital services and resources that America's taxpayer's deserve. 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 (240) 613-9373 or Carmelita White, Senior Manager of Program Oversight Coordination, at (240) 613-2191.

Attachment



Attachment

Draft Audit Report – Improvement Are Needed to Strengthen Electronic Authentication Process Controls (Audit # 201520006)

RECOMMENDATION #1: The Chief Information Officer should clarify IRS and contractor responsibilities related to preventing automated attacks, including tracking contractor activities and tools with respect to their responsibilities.

CORRECTIVE ACTION #1: The IRS agrees with this recommendation. This action has been completed, and reflected by the acquisition of specified security-centric contractor services and technology tools managed by the IRS Integrated Enterprise Portal (IEP) contractor. IRS has met and continues to meet with the contractor to clarify their responsibilities. A monthly meeting between IRS and the contractor takes place at the Executive and at the working group level. These discussions are directly related to the prevention of automated attacks, tools in use, and the procedures implemented by the contractor in the use of these tools to prevent automated attacks.

IMPLEMENTATION DATE: June 7, 2016

RESPONSIBLE OFFICIALS: 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.

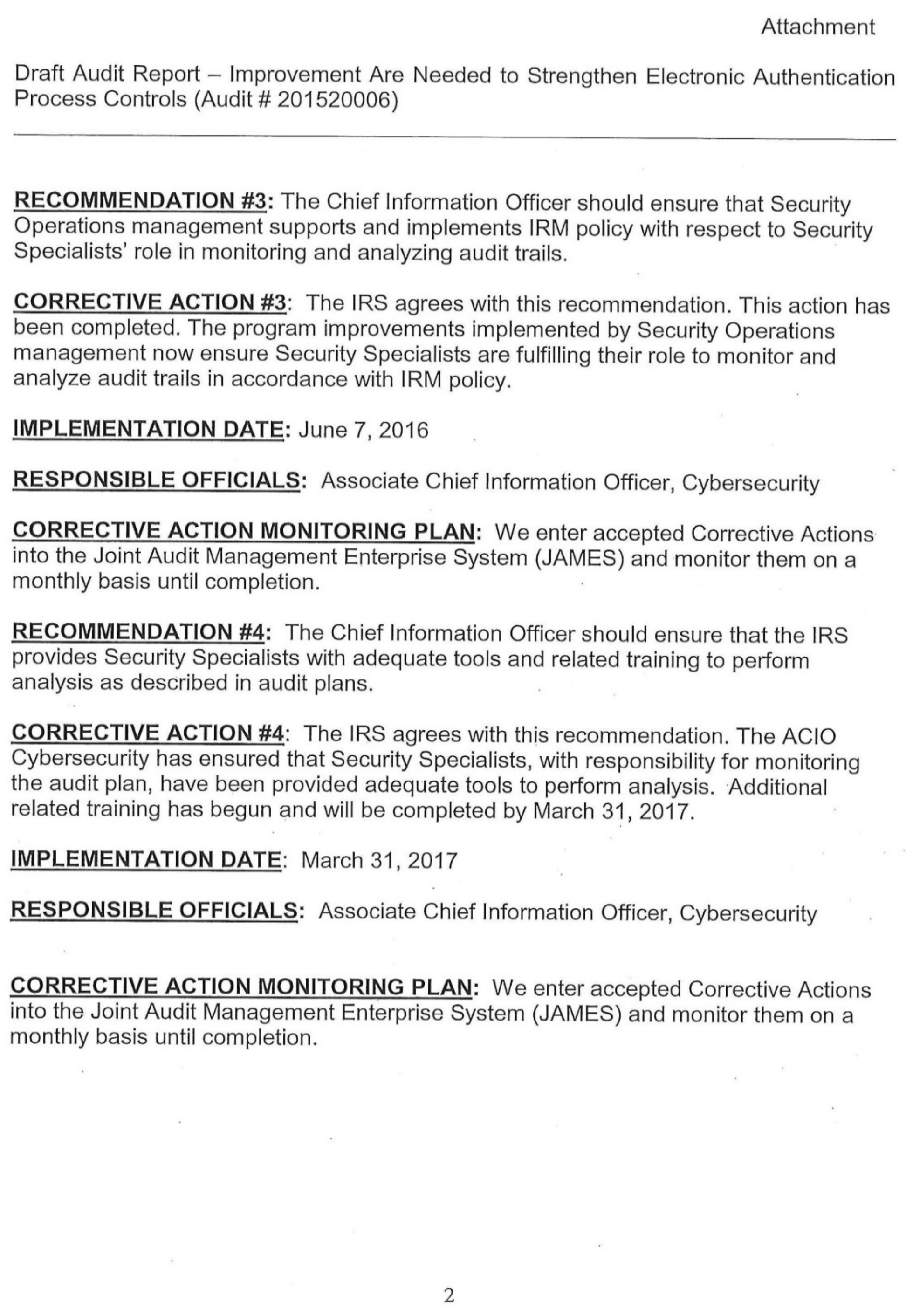
RECOMMENDATION #2: The Chief Information Officer should establish a process to monitor the results and effectiveness of controls to prevent/detect automated attacks.

CORRECTIVE ACTION #2: The IRS agrees with this recommendation. This action has been completed and is reflected in the establishment of a new IRS organization within Cyber Operations with responsibility for monitoring protected applications to prevent and detect against automated attacks This organization has established processes to monitor the results and effectiveness of the layered protections in place.

IMPLEMENTATION DATE: June 7, 2016

RESPONSIBLE OFFICIALS: 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.



Attachment

Draft Audit Report – Improvement Are Needed to Strengthen Electronic Authentication Process Controls (Audit # 201520006)

RECOMMENDATION #3: The Chief Information Officer should ensure that Security Operations management supports and implements IRM policy with respect to Security Specialists' role in monitoring and analyzing audit trails.

CORRECTIVE ACTION #3: The IRS agrees with this recommendation. This action has been completed. The program improvements implemented by Security Operations management now ensure Security Specialists are fulfilling their role to monitor and analyze audit trails in accordance with IRM policy.

IMPLEMENTATION DATE: June 7, 2016

RESPONSIBLE OFFICIALS: 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.

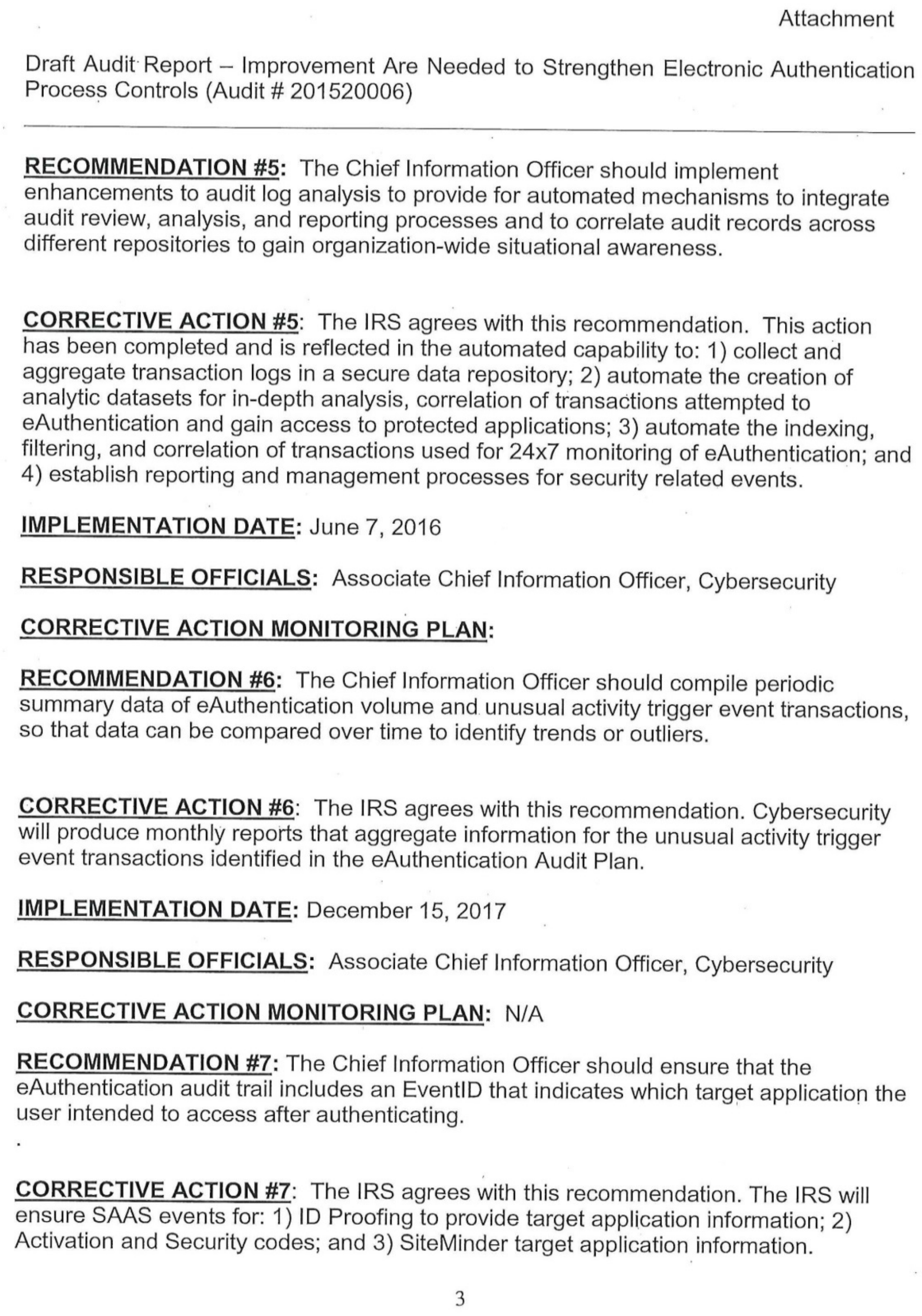
RECOMMENDATION #4: The Chief Information Officer should ensure that the IRS provides Security Specialists with adequate tools and related training to perform analysis as described in audit plans.

CORRECTIVE ACTION #4: The IRS agrees with this recommendation. The ACIO Cybersecurity has ensured that Security Specialists, with responsibility for monitoring the audit plan, have been provided adequate tools to perform analysis. Additional related training has begun and will be completed by March 31, 2017.

IMPLEMENTATION DATE: March 31, 2017

RESPONSIBLE OFFICIALS: 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.



Attachment

Draft Audit Report – Improvement Are Needed to Strengthen Electronic Authentication Process Controls (Audit # 201520006)

RECOMMENDATION #5: The Chief Information Officer should implement enhancements to audit log analysis to provide for automated mechanisms to integrate audit review, analysis, and reporting processes and to correlate audit records across different repositories to gain organization-wide situational awareness.

CORRECTIVE ACTION #5: The IRS agrees with this recommendation. This action has been completed and is reflected in the automated capability to: 1) collect and aggregate transaction logs in a secure data repository; 2) automate the creation of analytic datasets for in-depth analysis, correlation of transactions attempted to eAuthentication and gain access to protected applications; 3) automate the indexing, filtering, and correlation of transactions used for 24x7 monitoring of eAuthentication; and 4) establish reporting and management processes for security related events.

IMPLEMENTATION DATE: June 7, 2016

RESPONSIBLE OFFICIALS: Associate Chief Information Officer, Cybersecurity

CORRECTIVE ACTION MONITORING PLAN:

RECOMMENDATION #6: The Chief Information Officer should compile periodic summary data of eAuthentication volume and unusual activity trigger event transactions, so that data can be compared over time to identify trends or outliers.

CORRECTIVE ACTION #6: The IRS agrees with this recommendation. Cybersecurity will produce monthly reports that aggregate information for the unusual activity trigger event transactions identified in the eAuthentication Audit Plan.

IMPLEMENTATION DATE: December 15, 2017

RESPONSIBLE OFFICIALS: Associate Chief Information Officer, Cybersecurity

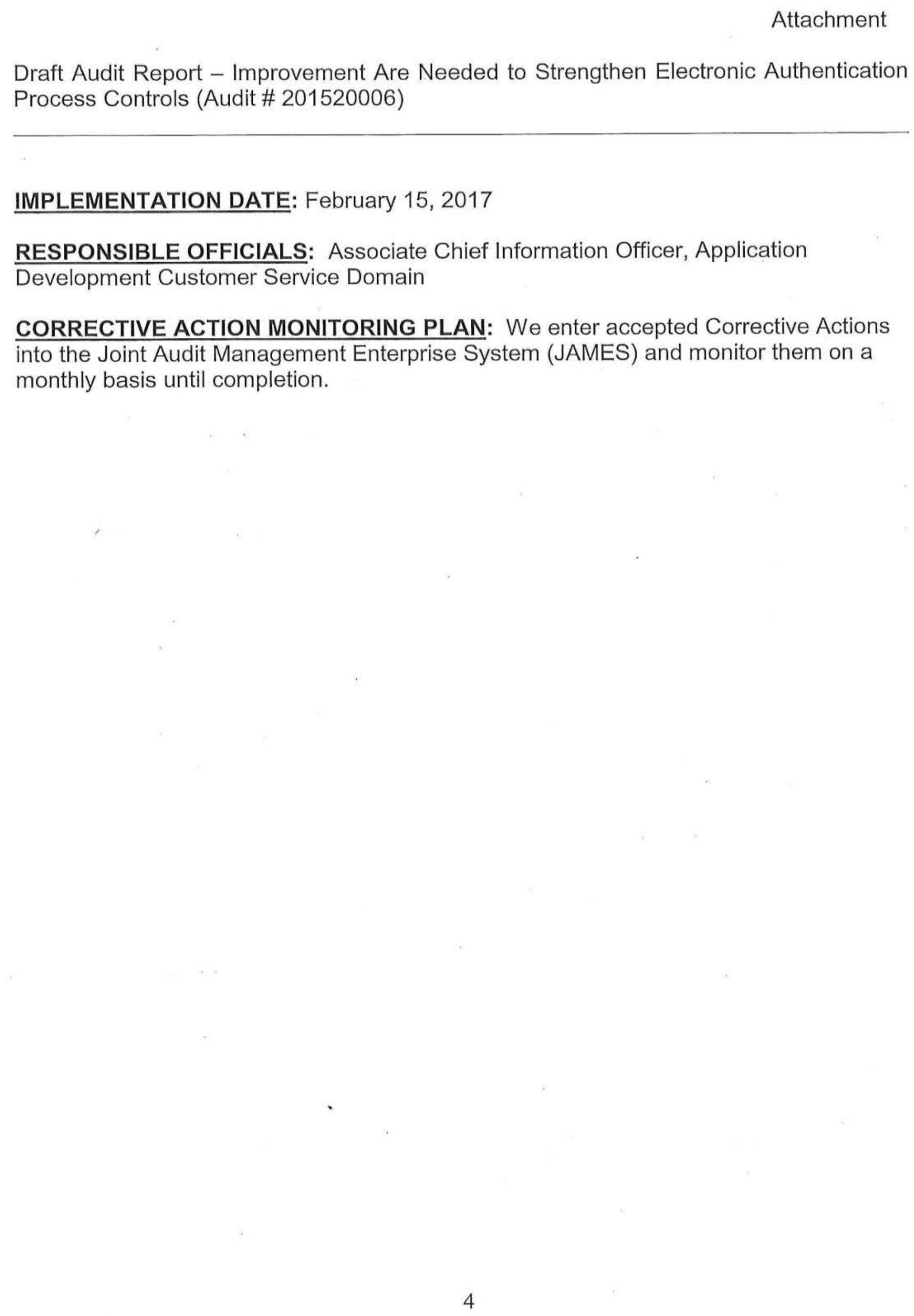
CORRECTIVE ACTION MONITORING PLAN: N/A

RECOMMENDATION #7: The Chief Information Officer should ensure that the eAuthentication audit trail includes an EventID that indicates which target application the user intended to access after authenticating.

.

CORRECTIVE ACTION #7: The IRS agrees with this recommendation. The IRS will ensure SAAS events for: 1) ID Proofing to provide target application information; 2) Activation and Security codes; and 3) SiteMinder target application information.

3



Attachment

Draft Audit Report – Improvement Are Needed to Strengthen Electronic Authentication Process Controls (Audit # 201520006)

IMPLEMENTATION DATE: February 15, 2017

RESPONSIBLE OFFICIALS: Associate Chief Information Officer, Application Development Customer Service Domain

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.