TREASURY INSPECTOR GENERAL FOR TAX ADMINISTRATION

Improvements Are Needed for an Effective User Behavior Analytics Capability

September 21, 2022

Report Number: 2022-20-055

TIGTACommunications@tigta.treas.gov | www.treasury.gov/tigta

HIGHLIGHTS: Improvements Are Needed for an Effective User Behavior Analytics Capability

Final Audit Report issued on September 21, 2022 **Report Number 2022-20-055**

Why TIGTA Did This Audit

An insider threat is defined as an employee or contractor who has authorized access to an organization's network, systems, or data and could intentionally misuse that access to have a negative effect on information or information systems. The IRS implemented its insider threat capability (renamed the User Behavior Analytics Capability (UBAC)) to detect and mitigate risks to data and systems arising from insider threats.

The overall objective of this audit was to evaluate the effectiveness of the insider threat capabilities and follow up on TIGTA, Report No. 2020-20-043, *Substantial Progress Has Been Made in Implementing the Insider Threat Capability, but Improvements Are Needed* (Aug. 2020), recommendations.

Impact on Tax Administration

The IRS collects, processes, and stores large amounts of taxpayer information. IRS employees and contractors can pose a substantial risk due to their knowledge of and legitimate access to IRS systems, which could be leveraged for illegal or nefarious purposes. The potential harm includes unauthorized disclosure of taxpayer information and the loss of the confidentiality, integrity, or availability of the IRS's information or information systems.

What TIGTA Found

The IRS did not have a complete inventory of systems to monitor for the UBAC. The UBAC list of systems that store or process Federal Tax Information and Personally Identifiable Information is missing 234 (67 percent) of 351 systems included in the Enterprise Security Audit Trails system list. The systems not included in the UBAC list are not subject to user behavior analysis. While the UBAC team has been developing their analytics and inventory of systems for analysis, they have not coordinated with the Enterprise Security Audit Trails team to ensure that they have all the correct systems in place.

The UBAC team is experiencing delays in receiving access to systems with information to improve its analytics. For example, the UBAC team requested access to the Human Resources Connect System and is waiting on approval. Data from this system will allow the UBAC team to incorporate 16 risk indicators into the UBAC.

TIGTA determined that UBAC analysts performed appropriate reviews of the incidents of potential insider threats, documented the reviews in the anomaly report, and either escalated the incidents as necessary or closed the incidents if the analysts determined the risks of insider threats were low.

TIGTA reviewed UBAC Anomaly Reports for 229 incidents and found that 109 (48 percent) of the incidents were forwarded to the TIGTA Office of Investigations for review and possible investigation. TIGTA also determined there is no formal process to document feedback from stakeholders on referred incidents. The IRS recorded feedback in anomaly reports for only three (3 percent) of the 109 incidents. Finally, implemented planned corrective actions generally addressed prior TIGTA recommendations.

What TIGTA Recommended

TIGTA recommended that the Chief Information Officer ensure that the UBAC team coordinates with the Enterprise Security Audit Trails Project Management Office to identify and update the inventory of all systems on a regular basis and subject the systems to user behavior analysis, and the UBAC team implements a process to document feedback from stakeholders on referred incidents.

The IRS agreed with all of our recommendations. The Cybersecurity function plans to coordinate with the Enterprise Security Audit Trails Project Management Office to establish a process to access and review the central repository where the inventory of all auditable systems is maintained. In addition, the IRS stated that the primary source of feedback on referred incidents is TIGTA, which provides information to the Human Capital Office. The Cybersecurity function plans to partner with the Human Capital Office to implement a process to receive updates and document feedback, as appropriate.

TREASURY INSPECTOR GENERAL
FOR TAX ADMINISTRATION

U.S. DEPARTMENT OF THE TREASURY
WASHINGTON, D.C. 20024

September 21, 2022

MEMORANDUM FOR: COMMISSIONER OF INTERNAL REVENUE

Heather Hill

FROM: Heather M. Hill
Deputy Inspector General for Audit

SUBJECT: Final Audit Report – Improvements Are Needed for an Effective User Behavior Analytics Capability (Audit # 202220008)

This report presents the results of our review to evaluate the effectiveness of the insider threat capabilities and follow up on prior audit recommendations. This review is part of our Fiscal Year 2022 Annual Audit Plan and addresses the major management and performance challenges of *Enhancing Security of Taxpayer Data and Protection of IRS [Internal Revenue Service] Resources*, and *Addressing Emerging Threats to Tax Administration*.

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

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).

Table of Contents

Appendices

Background

Threats posed by an organization’s own employees and contractors are commonly referred to as “insider threats.”[1] For Federal Government agencies, an insider threat is generally defined as a current or former employee, contractor, or other business partner who has or had authorized access to an organization’s network, systems, or data and could intentionally misuse that access to negatively affect the confidentiality, integrity, or availability of the organization's information or information systems. The Internal Revenue Service (IRS) collects, processes, and stores large amounts of taxpayer information. IRS employees and contractors can pose a substantial risk due to their knowledge of and legitimate access to IRS systems, which could be leveraged for illegal and nefarious purposes. The potential harm can include damage through espionage, terrorism, unauthorized disclosure of taxpayer information, or loss or degradation of system functionality.

After the Calendar Year 2010 leak of classified material by a U.S. Army intelligence analyst, the President issued Executive Order 13587.[2] The Executive Order created the National Insider Threat Task Force (hereafter referred to as the National Task Force) and directed all agencies that operate or access classified computer networks to designate a senior official to oversee the safeguarding of classified information and establish an insider threat detection program.

In August 2013, the Department of the Treasury (hereafter referred to as the Treasury Department) issued Treasury Order 105-20[3] with the requirement to “establish a Department of the Treasury Insider Threat Program in accordance with Executive Order 13587 and its implementing policies and standards.” Per Treasury Department guidance to the IRS, the Treasury Department is responsible for implementing and operating the overall Treasury Department Insider Threat Program, and the bureaus, such as the IRS, are responsible for maintaining an insider threat capability in support of the program.

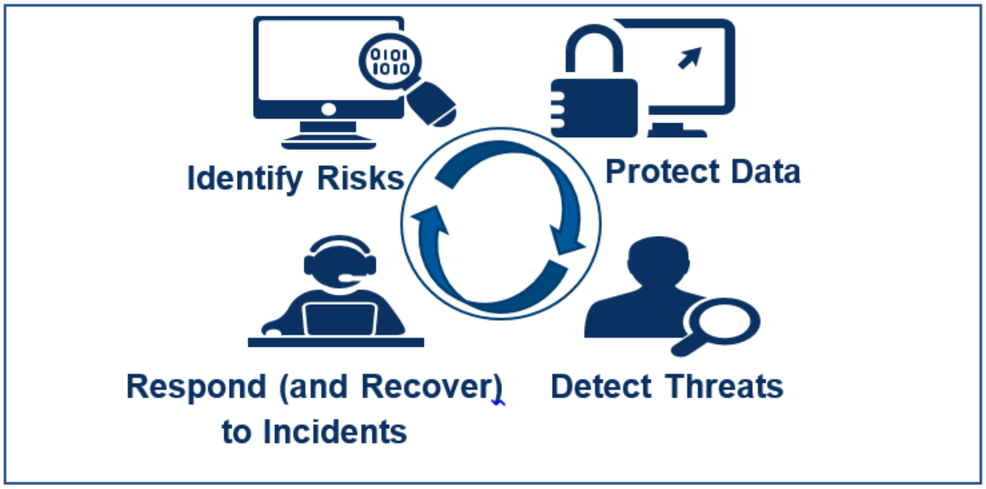
The IRS began implementing an insider threat capability in Fiscal Year 2016 with the objectives shown in Figure 1.

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

[2] Exec. Order No. 13587, *Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information* (Oct. 7, 2011).

[3] Treas. Order 105-20, *Insider Threat Program* (Aug. 9, 2013), superseded by Treas. Order 105-20, *Insider Threat Program* (Jan. 6, 2020).

Figure 1: Insider Threat Capabilities Objectives



Source: Insider Threat Capabilities Objectives, Insider Threat Capabilities Current State Maturity Assessment September 29, 2021.

In November 2018, the National Task Force issued additional program implementation guidance in the form of the Insider Threat Maturity Framework. In Fiscal Year 2019, the insider threat capability was incorporated into the IRS Integrated Modernization Business Plan and renamed the User Behavior Analytics Capability (UBAC). The UBAC was deployed to detect, report, and mitigate risks to data and systems arising from insider threats. In March 2020, the IRS established the Enterprise Security Audit Trails (ESAT) Project Management Office within the Information Technology organization's Cybersecurity function. The ESAT office's mission is to protect Sensitive But Unclassified data, including taxpayer information and IRS electronic systems, service, and data, from internal and external cybersecurity-related threats by incorporating security practices in planning, implementation, risk management, and operations.

In Fiscal Year 2020, the Treasury Inspector General for Tax Administration (TIGTA) reported[4] that the IRS made substantial progress in implementing an insider threat capability, basing its design on relevant, applicable guidance and properly aligning the capability with the goals of the IRS. The IRS also developed and implemented processes to identify potential insider threats and refer them to appropriate stakeholders[5] for review. From October 1, 2016, through February 29, 2020, the IRS identified 112 potential insider threats and referred nine to the relevant stakeholders for investigation or resolution. In addition, the IRS initiated and implemented activities to expedite the ability to detect and mitigate risk and to use real-time intelligence information.

TIGTA also reported that the IRS could improve its UBAC by better documenting and including insider threat risks associated with high-value assets, including recommendations and challenges in executive status reports, and addressing recommended training for UBAC personnel. We present more details from the prior audit report later in this report.

[4] TIGTA, Report No. 2020-20-043, *Substantial Progress Has Been Made in Implementing the Insider Threat Capability, but Improvements Are Needed* (Aug. 2020).

[5] Appropriate stakeholders are key personnel from a particular business unit including TIGTA; Human Capital Office; Privacy, Governmental Liaison, and Disclosure; Computer Security Incident Response Center; Cyber Fraud Analytics Monitoring; and Facilities Management and Security Services.

Results of Review

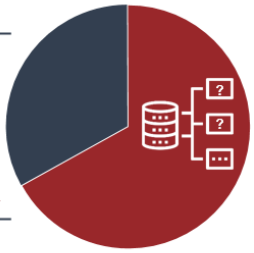
The IRS Did Not Have a Complete Inventory of Systems to Monitor for Its User Behavior Analytics Capability

In September 2021, the UBAC progressed from its Initial Operating Capability to Full Operating Capability. The IRS defined Full Operating Capability as the UBAC being able to provide:

- Cross-functional data sharing, communications, data correlation, and reporting to expedite the ability to detect and mitigate risks to data and systems arising from insider threats.
- Proactive identification of emerging insider threats through the use of real-time intelligence information and analytics to mitigate risks to data and systems arising from insider threats.

During our audit, the IRS was initially unable to provide an accurate number of systems with Federal Tax Information and Personally Identifiable Information. Following our request in January 2022, we obtained a list from the ESAT team in March 2022 that contained 365 systems. However, in May 2022, the ESAT team reviewed the accuracy of the number and naming conventions of the systems on the list and provided an updated list that contained 351 systems. We reviewed the list of systems and determined that 234 (67 percent) of the 351 systems with Federal Tax Information and Personally Identifiable Information were missing from UBAC inventory and were not subject to user behavior analysis.

We determined that 234 of the 351 systems with Federal Tax Information and Personally Identifiable Information were missing from the UBAC inventory.



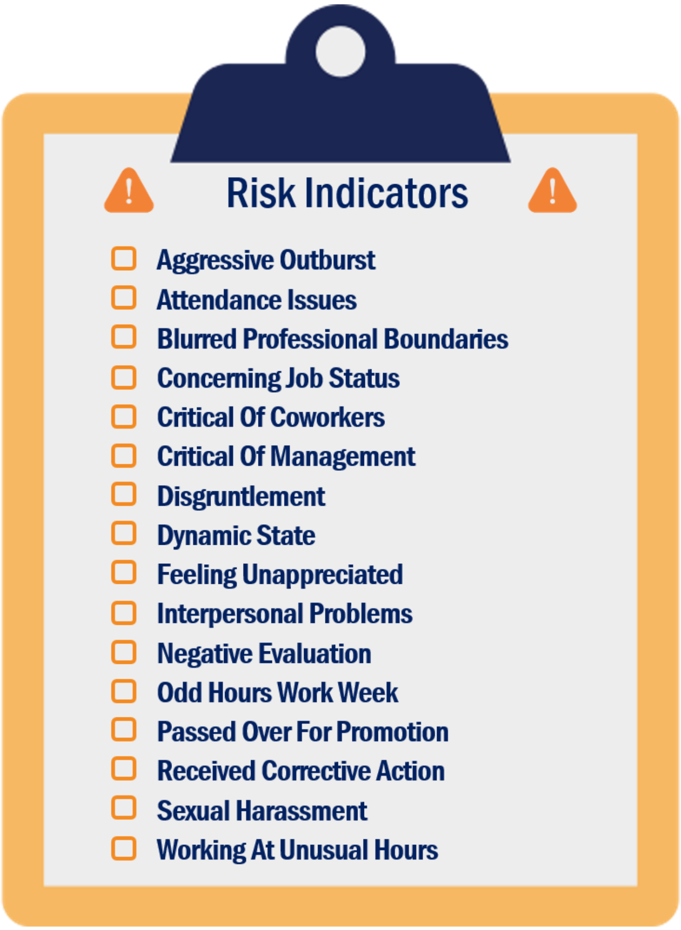
The Internal Revenue Manual requires the IRS to: 1) develop and update an inventory of systems as systems are commissioned and decommissioned, and at a minimum annually; 2) maintain a comprehensive inventory of systems and relevant security information for those systems; and 3) establish, maintain, and update an inventory of all systems, applications, and projects that process Personally Identifiable Information annually.

While the UBAC team has been developing their analytics and inventory of systems for analysis, they have not coordinated with the ESAT team to ensure that they have all the correct systems in place. After the UBAC team reviewed their list of systems, a UBAC official stated they needed to organize their inventory because some of their system naming conventions were different from those in the ESAT team's inventory. Cybersecurity function personnel stated that they plan to add the remaining systems with Federal Tax Information and Personally Identifiable Information data to UBAC inventory.

In addition, the UBAC team is experiencing delays in receiving access to systems with information to improve their analytics. For example, the UBAC team requested access to the

Human Resources Connect System and is waiting on approval. Once approved, it would allow the UBAC team to leverage the data from this system and incorporate the 16 risk indicators in Figure 2 into the UBAC.

Figure 2: Human Resources Connect System Risk Indicators



⚠ Risk Indicators ⚠

- □ Aggressive Outburst
- □ Attendance Issues
- □ Blurred Professional Boundaries
- □ Concerning Job Status
- □ Critical Of Coworkers
- □ Critical Of Management
- □ Disgruntlement
- □ Dynamic State
- □ Feeling Unappreciated
- □ Interpersonal Problems
- □ Negative Evaluation
- □ Odd Hours Work Week
- □ Passed Over For Promotion
- □ Received Corrective Action
- □ Sexual Harassment
- □ Working At Unusual Hours

Source: UBAC team-provided e-mail on June 2, 2022.

Having system data for these risk indicators would improve UBAC analytics. As part of their ongoing efforts to improve their behavioral analytics process, the UBAC team established a new indicator management team that is dedicated to establishing requirements for developing use cases and indicators for systems added to their inventory.

By not having access to system data for risk indicators and a complete inventory of systems that store or process Federal Tax Information and Personally Identifiable Information, the UBAC team's improvements to their analytics may be limited and some systems may not have specific use cases for analysis. Consequently, the IRS may be unable to identify insider threat activity that may negatively affect the confidentiality, integrity, or availability of the IRS's information or information systems. An effective insider threat capability is vital to protect taxpayer information and IRS operations.

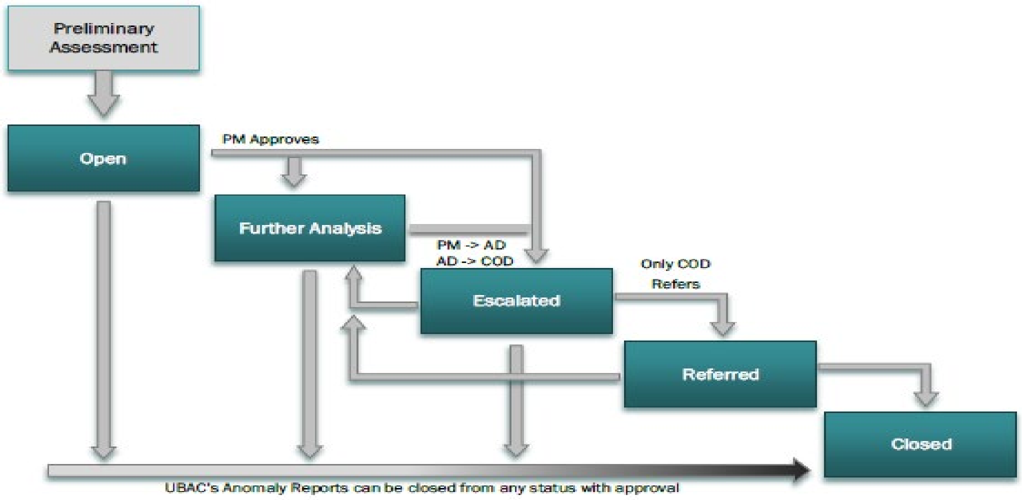
Recommendation 1: The Chief Information Officer should ensure that the UBAC team coordinates with the ESAT Project Management Office to identify and update the inventory of all systems on a regular basis and subject the systems to user behavior analysis.

> **Management's Response:** The IRS agreed with this recommendation. The Cybersecurity function will coordinate with the ESAT Project Management Office to establish a process to access and review the central repository where the inventory of all auditable systems is maintained.

Feedback Regarding Potential Insider Threats Is Needed to Improve Assessments and Referrals

The UBAC has two primary Standard Operating Procedures that guide the handling of incidents of potential insider threats. The first Standard Operating Procedure[6] provides the basic procedures for incident response on an ad hoc basis when there is an immediate event-reporting requirement. Figure 3 shows the statuses that an identified potential insider threat progresses through during the UBAC Anomaly Reporting Process.

Figure 3: UBAC Anomaly Reporting Process Statuses



Source: UBAC Anomaly Reporting Standard Operating Procedure January 15, 2021. AD = Associate Director; COD = Cyber Operations Director; and PM = Project Manager

We reviewed all incidents documented in the Counter Insider Threat Archer system and identified 229 incidents that occurred from March 1, 2020, through December 31, 2021. Figure 4 provides a list of the 229 incidents as categorized by the analysts.

[6] IRS, Information Technology Cybersecurity Operations Interim Standard Operating Procedures, *User Behavior Analytics Capability Incident Response* (SO-022-2021) (Nov. 9, 2021).

Figure 4: UBAC Insider Threat Activity

Count	Primary Use Case
69	Privacy, Governmental Liaison, and Disclosure Unauthorized Access: Access to Family/Extended Family
46	Attempted Access to Own
40	Behavioral Risk Classification
35	Privacy, Governmental Liaison, and Disclosure Unauthorized Access: Access to Tax Preparer
6	Verbal Threats
5	Suicide Attempt
3	Failure to Return Government-Owned Property
2	Attempts to Access a Service Account
2	E-mail Personally Identifiable Information to Personal E-mail
2	Physically Aggressive Actions
2	Privacy, Governmental Liaison, and Disclosure Unauthorized Access: Access to Day Care Provider
2	Privacy, Governmental Liaison, and Disclosure Unauthorized Access: Access to Other Business Relationship Records
2	Privacy, Governmental Liaison, and Disclosure Unauthorized Access: Access Without Assignment
2	Separated or Absent Employee Not Returning Government-Owned Property
1	Criminal/Legal Actions or Sanctions
1	E-mail Social Security Number to Non-IRS Domain
1	Extended Unexcused Absence/Absent Without Leave
1	Improper Handling of Sensitive Material
1	Inappropriate Conduct
1	Lost Information Technology Asset
1	Not Following Directions/Procedures
1	Privileged User Activity in Security Audit and Analysis System
1	Transfer Personally Identifiable Information to Removable Media
1	Video Recording Screen Captures of Sensitive Data
1	Workplace Disruption

Source: TIGTA's review of insider threat incidents from March 1, 2020, through December 31, 2021.

The primary document used to capture an incident is the *User Behavior Analytics Capability Anomaly Report*. During our review of the incidents, we assessed each report by:

- Overall status.
- Open and close dates.
- Date of information collection for analysis.
- Referral status.
- Incident summary.
- Result of the analysis conducted by UBAC analysts.
- Feedback from referrals.

We determined that UBAC analysts performed appropriate reviews of the incidents, documented the reviews in the anomaly report, and either escalated the incidents as necessary or closed the incidents if the analysts determined the risks of insider threats were low.

The second Standard Operating Procedure[7] provides the procedures for the assessment, reporting, referral, and closure of anomalies detected by the UBAC or referred by stakeholders. It also states that if the stakeholder is able to inform the UBAC of the outcome of the referral, the UBAC team uses that feedback to improve their analytics, which ensures the relevance of future referrals barring any confidentiality and need-to-know restrictions on the mitigation action, outcome, or resolution.

We reviewed the anomaly report for each of the incidents and determined that 109 (48 percent) of 229 incidents were forwarded to the TIGTA Office of Investigations for review and possible investigation. After TIGTA investigates a referral, a Report of Investigation[8] is provided to IRS management via the Automated Labor and Employee Relations Tracking System.

The IRS recorded feedback in anomaly reports for only three (3 percent) of 109 incidents. We discussed the lack of feedback within the anomaly reports with the IRS and determined there is no formal process for documenting feedback from stakeholders. By not receiving feedback on referred incidents, the UBAC team does not know if they produced credible incidents of potential insider threats. The stakeholders' feedback could improve future incidents produced by the UBAC.

Recommendation 2: The Chief Information Officer should ensure that the UBAC team implements a process to document feedback from stakeholders on referred incidents.

> **Management's Response:** The IRS agreed with this recommendation. The primary source of feedback on referred incidents is TIGTA, which provides information to the Human Capital Office. The Cybersecurity function will partner with the Human Capital Office to implement a process to receive updates and document feedback, as appropriate.

Implemented Planned Corrective Actions Generally Addressed Prior TIGTA Recommendations

In the Fiscal Year 2020 report, TIGTA determined that the IRS had made substantial progress in implementing an insider threat capability, but that additional improvements could assist the IRS in achieving an effective Full Operating Capability. Specifically, TIGTA recommended that:

- The IRS should ensure that the UBAC project implementation plan included actions to determine and assess the risk posture of high-value assets and that those risks should be addressed as part of the capability implementation.

[7] IRS, Information Technology Cybersecurity Operations Standard Operating Procedures, *User Behavior Analytics Capability Anomaly Reporting* (SO-013-2020) (Jan. 15, 2021).

[8] TIGTA Form OI-2028R, *Report of Investigation* (Apr. 2007).

- The Chief Information Officer should ensure that status reports align with the National Insider Threat Task Force recommendations and include sections to address program improvement and major impediments or challenges.
- The Chief Information Officer should ensure that the UBAC project implementation plan includes the National Insider Threat Task Force's recommended training for UBAC personnel. In addition, the IRS should document all UBAC training efforts and, at least annually, ensure that all UBAC personnel have completed the required training.

We reviewed the recommendations, the actions taken by the IRS to addresses those recommendations, and the documentation to support those actions. Overall, we determined that the IRS met the intent of the recommendations and addressed the weaknesses identified. The IRS assessed the risk posture of the high-value assets, updated its status reports to include sections to address program improvements and major impediments or challenges, and ensured that all UBAC personnel completed the required training.

However, according to the Joint Audit Management Enterprise System report and the documentation provided, the IRS did not update the UBAC project implementation plan as recommended in the first and third recommendations. Instead, IRS officials updated a Standard Operating Procedure[9] with an appendix containing three numbered items addressing each of the three recommendations made in the prior report.

[9] IRS, Information Technology Cybersecurity Operations Standard Operating Procedures, *User Behavior Analytics Capability Anomaly Reporting* (SO-013-2020) (Jan. 15, 2021).

Appendix I

Detailed Objective, Scope, and Methodology

The overall objective of this audit was to evaluate the effectiveness of the insider threat capabilities and follow up on prior audit recommendations. To accomplish our objective, we:

- Determined whether corrective actions for the recommendations from TIGTA, Report No. 2020-20-043, *Substantial Progress Has Been Made in Implementing the Insider Threat Capability, but Improvements Are Needed* (Aug. 2020), were effectively implemented by reviewing the Joint Audit Management Enterprise System documentation and assessing whether the corrective actions addressed the reported weaknesses.
- Evaluated the UBAC's guidelines by comparing them to the Federal, National Institute of Standards and Technology, and other applicable requirements.
- Assessed the UBAC's system inventory process by reviewing criteria for whether an IRS system should be included in UBAC inventory and interviewing Cybersecurity officials to determine why systems were not included.
- Identified information available to improve the UBAC's analytics capabilities by reviewing the Human Resources system's risk indicators.
- Evaluated potential insider threats identified from March 1, 2020, through December 31, 2021, and the disposition of the threats (non-threat, referred for investigation) by reviewing potential threat information from the Archer system and/or other applicable sources. We also reviewed the documentation and processing of 229 potential threats.

Performance of This Review

This review was performed with information obtained from the ESAT office and the Cybersecurity and User and Network Services functions located in Lanham, Maryland, and Houston, Texas, during the period December 2021 to July 2022. 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.

Major contributors to the report were Danny Verneuille, Assistant Inspector General for Audit (Security and Information Technology Services); Jason McKnight, Director; Kasey Koontz, Audit Manager; Suzanne Westcott, Lead Auditor; and Michael Segall, Senior Auditor.

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: ESAT office and UBAC policies and procedures; Internal Revenue Manual policies related to security and privacy controls; and National Institute of Standards and Technology, Special Publication 800-53, Revision 5, *Security and Privacy Controls for Information Systems and Organizations* (December 2020). We evaluated these controls by interviewing Cybersecurity and User and Network Services function personnel including the ESAT office and the UBAC program; reviewing the Internal Revenue Manual, Joint Audit Management Enterprise System documentation, UBAC Anomaly Reporting Desk Guide, UBAC Anomaly Reporting Standard Operating Procedures, the National Institute of Standards and Technology guidelines, and the processing of identified potential insider threats; and comparing UBAC Standard Operating Procedures to the National Task Force guidance and the other previously listed guidelines.

Appendix II

Outcome Measure

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

Type and Value of Outcome Measure:

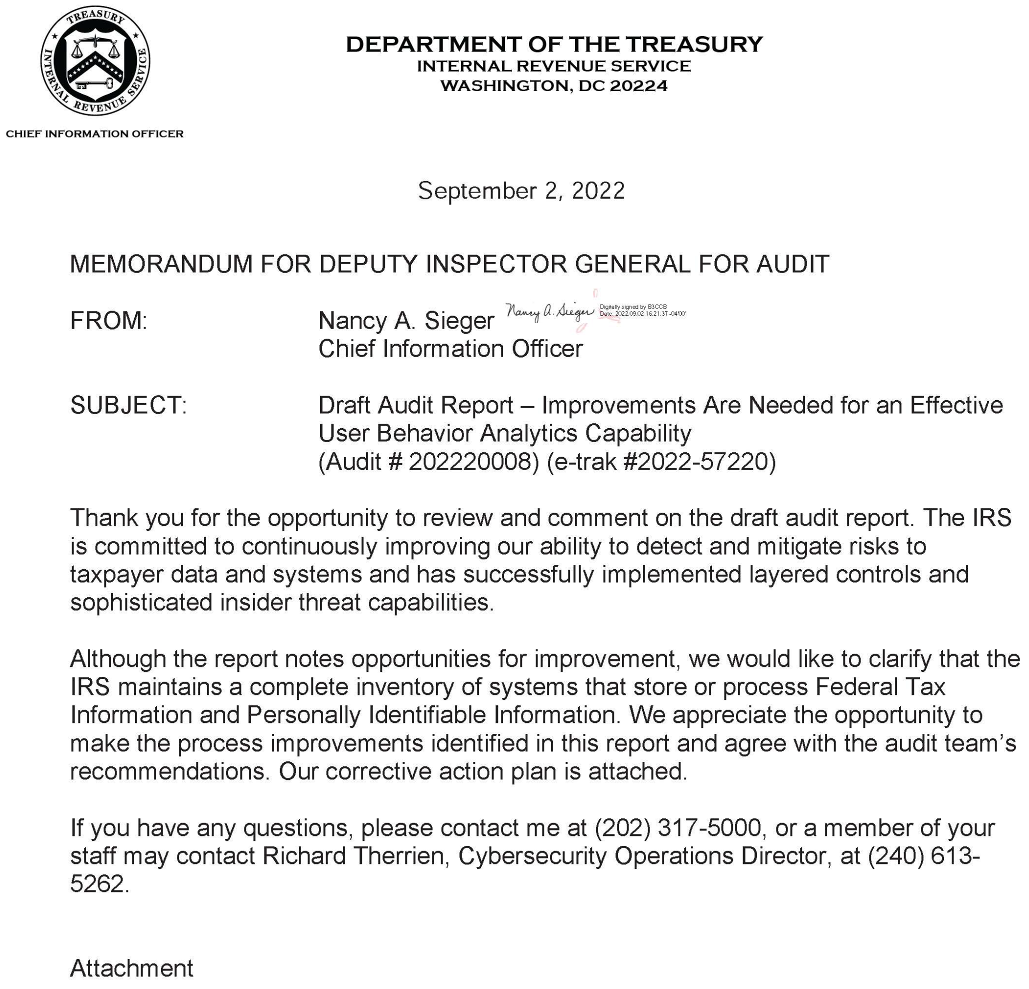
- Protection of Resources – Potential; 234 (67 percent) of 351 systems that store or process Federal Tax Information and Personally Identifiable Information are not included in UBAC inventory and subject to user behavior analysis (see Recommendation 1).

Methodology Used to Measure the Reported Benefit:

We obtained a list of 351 systems that store or process Federal Tax Information and Personally Identifiable Information from the ESAT office. We reconciled this list with UBAC inventory to determine that 234 (67 percent) of the 351 systems are not included in UBAC inventory.

Appendix III

Management's Response to the Draft Report



CHIEF INFORMATION OFFICER

DEPARTMENT OF THE TREASURY
INTERNAL REVENUE SERVICE
WASHINGTON, DC 20224

September 2, 2022

MEMORANDUM FOR DEPUTY INSPECTOR GENERAL FOR AUDIT

FROM: Nancy A. Sieger Nancy A. Sieger Digitally signed by B3CCB Date: 2022.09.02 16:21:37 -04'00'
Chief Information Officer

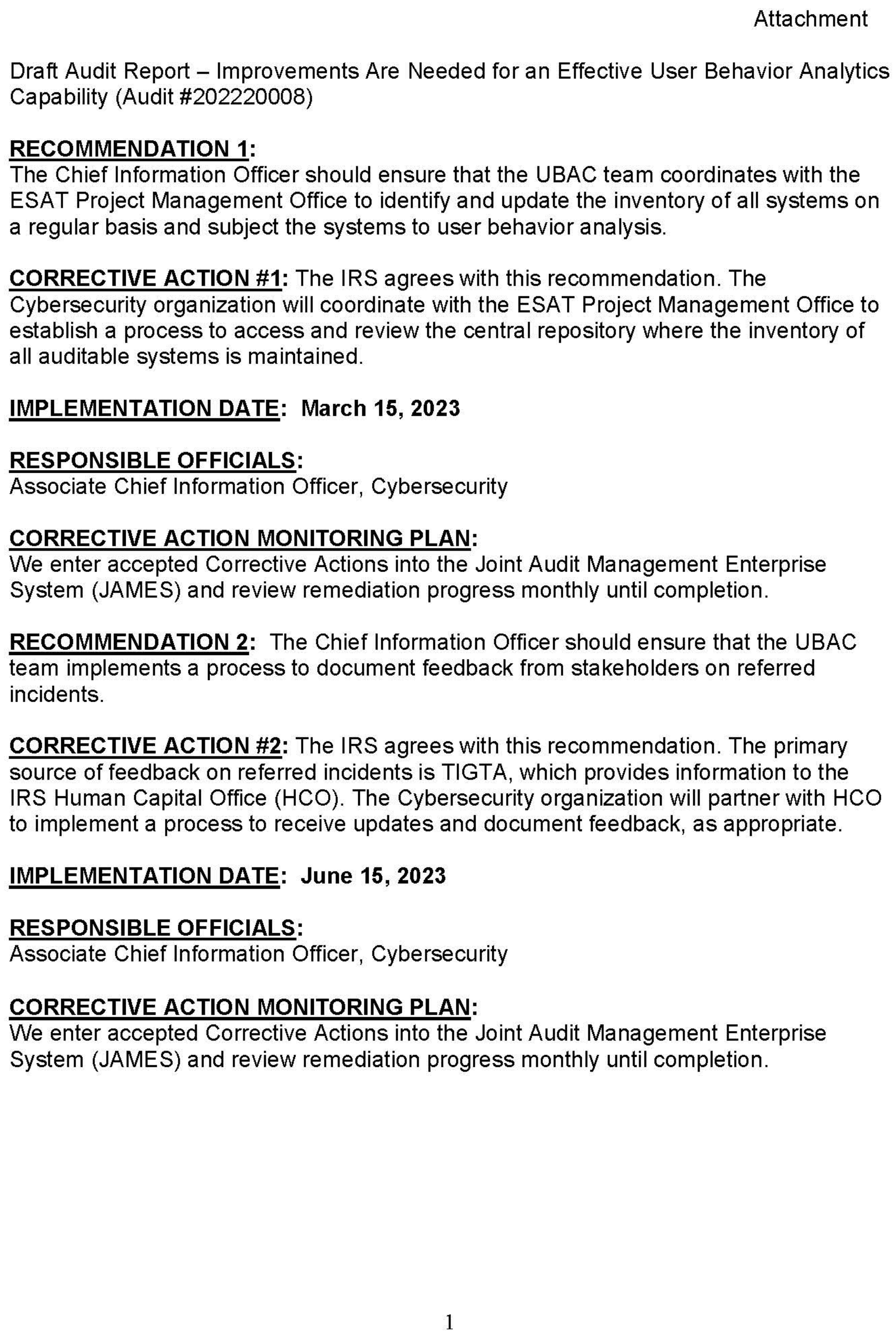
SUBJECT: Draft Audit Report – Improvements Are Needed for an Effective User Behavior Analytics Capability
(Audit # 202220008) (e-trak #2022-57220)

Thank you for the opportunity to review and comment on the draft audit report. The IRS is committed to continuously improving our ability to detect and mitigate risks to taxpayer data and systems and has successfully implemented layered controls and sophisticated insider threat capabilities.

Although the report notes opportunities for improvement, we would like to clarify that the IRS maintains a complete inventory of systems that store or process Federal Tax Information and Personally Identifiable Information. We appreciate the opportunity to make the process improvements identified in this report and agree with the audit team's recommendations. Our corrective action plan is attached.

If you have any questions, please contact me at (202) 317-5000, or a member of your staff may contact Richard Therrien, Cybersecurity Operations Director, at (240) 613-5262.

Attachment



Attachment

Draft Audit Report – Improvements Are Needed for an Effective User Behavior Analytics Capability (Audit #202220008)

RECOMMENDATION 1:
The Chief Information Officer should ensure that the UBAC team coordinates with the ESAT Project Management Office to identify and update the inventory of all systems on a regular basis and subject the systems to user behavior analysis.

CORRECTIVE ACTION #1: The IRS agrees with this recommendation. The Cybersecurity organization will coordinate with the ESAT Project Management Office to establish a process to access and review the central repository where the inventory of all auditable systems is maintained.

IMPLEMENTATION DATE: March 15, 2023

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 review remediation progress monthly until completion.

RECOMMENDATION 2: The Chief Information Officer should ensure that the UBAC team implements a process to document feedback from stakeholders on referred incidents.

CORRECTIVE ACTION #2: The IRS agrees with this recommendation. The primary source of feedback on referred incidents is TIGTA, which provides information to the IRS Human Capital Office (HCO). The Cybersecurity organization will partner with HCO to implement a process to receive updates and document feedback, as appropriate.

IMPLEMENTATION DATE: June 15, 2023

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 review remediation progress monthly until completion.

Appendix IV

Glossary of Terms

Term	Definition
Archer System	A commercial-off-the-shelf product that provides a web-based application for cyber threat management. The Computer Security Incident Response Center captures cybersecurity and computer-related security incidents in the Archer system.
Automated Labor and Employee Relations Tracking System	A data source that allows users to establish, track, and maintain employee relations cases and to establish and track Labor Relations activities, Unfair Labor Practice charges, and events for negotiation processes, grievances, and arbitration proceedings.
Cybersecurity Function	A function within the Information Technology organization responsible for ensuring compliance with Federal statutory, legislative, and regulatory requirements governing confidentiality, integrity, and availability of IRS electronic systems, services, and data.
Enterprise Security Audit Trails	A security auditing tool that allows the collection, retention, and review of enterprise security audit events.
Fiscal Year	Any yearly accounting period, regardless of its relationship to a calendar year. The Federal Government's fiscal year begins on October 1 and ends on September 30.
Human Resources Connect System	A system owned and managed by the Treasury Department. It provides managers with the ability to access basic data for employees they supervise, initiate awards and other personnel actions, manage positions by reviewing detailed information about authorized staffing, and initiate recruitment actions.
Indicator	A recognized action, specific, generalized, or theoretical that an adversary might be expected to take in preparation for an attack. Also, it is a sign that an incident may have occurred or may be currently occurring.
Initial Operating Capability	A point in time during the production and deployment phase when a system can meet the minimum operational (Threshold and Objective) capabilities for a user's stated need.
Insider Threat	Any employee, contractor, or vendor with authorized access, or who once had such access, to IRS assets including personnel, facilities, information, equipment, networks, or systems, who uses their access to commit, wittingly or unwittingly, an act that results in harm to the public's trust in the IRS. An insider threat may involve theft of information or physical property, workplace violence, security compromise, espionage, terrorism, fraud, or sabotage.
Insider Threat Capability	The ability to identify and take action related to insider threats.

Term	Definition
National Insider Threat Task Force	The principal interagency task force responsible for developing an Executive Branch insider threat detection and prevention program, including developing and issuing minimum standards and guidance for implementing insider threat program capabilities throughout the Executive Branch.
National Institute of Standards and Technology	A part of the Department of Commerce that is responsible for developing standards and guidelines to provide adequate information security for all Federal agency operations and assets.
Personally Identifiable Information	Information that can be used to distinguish or trace an individual's identity, such as their name, Social Security Number, and biometric records, alone or when combined with other personal or identifying information, which is linked or linkable to a specific individual, such as date, place of birth, and mother's maiden name.
Security Audit and Analysis System	This system implements a data warehousing solution to provide online analytical processing of audit trail data. This system was replaced by the ESAT tool.
System	The IRS As-Built Architecture defines application systems as production software code and databases that support business processes in all business areas. Infrastructure systems represent computing and communication platforms that application systems run on or use in the course of operation.
User Behavior Analytics	A type of analytic that detects actions taken by a human user, versus by a system.
User Behavior Analytics Capability Anomaly Report	The primary reporting vehicle for behavioral anomalies potentially indicative of insider threats.

Appendix V

Abbreviations

ESAT	Enterprise Security Audit Trails
IRS	Internal Revenue Service
TIGTA	Treasury Inspector General for Tax Administration
UBAC	User Behavior Analytics Capability

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

(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.