TREASURY INSPECTOR GENERAL FOR TAX ADMINISTRATION

Substantial Progress Has Been Made in Implementing the Insider Threat Capability, but Improvements Are Needed

August 19, 2020

Reference Number: 2020-20-043

TIGTACommunications@tigta.treas.gov | www.treasury.gov/tigta | 202-622-6500

HIGHLIGHTS: Substantial Progress Has Been Made in Implementing the Insider Threat Capability, but Improvements Are Needed

Final Audit Report issued on August 19, 2020
Reference Number 2020-20-043

Why TIGTA Did This Audit

This audit was initiated to evaluate the effectiveness of IRS efforts to implement an insider threat capability to detect, monitor, prevent, and report on insider threats. 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 negatively affect the confidentiality, integrity, or availability of the organization's information or information systems.

Impact on Taxpayers

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 loss or degradation of system functionality. Consequently, an insider threat capability with effective controls to monitor, detect, and prevent insider threats is vital to protect taxpayer information and IRS operations.

What TIGTA Found

The IRS has made substantial progress in implementing an insider threat capability. The IRS based the design of its capability on relevant, applicable guidance and properly aligned this capability with the goals of the IRS Integrated Modernization Business Plan. The IRS has also developed and implemented processes to identify potential insider threats and refer them to appropriate stakeholders 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, activities to expedite the ability to detect and mitigate risk and to use real-time intelligence information have been initiated and are currently in process. The insider threat capability is currently in its Initial Operating Capability state, with full operating status scheduled for Fiscal Year 2021.

Additional improvements can assist the IRS to achieve an effective Full Operating Capability. Specifically, the IRS insider threat capability implementation plan did not have documented processes in place to determine its high-value assets and assess risks related to those assets as part of its implementation efforts. Without identifying and assessing the risk associated with its high-value assets, the IRS cannot ensure that those high-value assets are being evaluated for insider threats. In addition, executive status reports included many recommended metrics; however, they did not include recommendations and goals for program improvement and major impediments or challenges. Without these items, executives responsible for this program may not be aware of critical information useful to manage the program. Finally, the IRS implementation plan did not specifically address recommended training curricula. The omission of training could lead to skills and knowledge gaps, which could affect the overall effectiveness of the insider threat capability.

What TIGTA Recommended

TIGTA recommended that the Chief Information Officer include specific actions in the insider threat capability implementation plan to ensure that high-value assets are identified and their related risks assessed, add specific sections to status reports that address recommendations for program improvement and major impediments or challenges, and ensure that personnel complete recommended training.

The IRS agreed with all of our recommendations. The IRS plans to ensure that the implementation plan includes actions to determine and assess the risk posture of high-value assets; status reports align with the National Insider Threat Task Force recommendations and include sections to address program improvement and major impediments or challenges; and the implementation plan includes recommended training for personnel, documents all training efforts, and at least annually, ensures that all personnel have completed the required training.

TREASURY INSPECTOR GENERAL
FOR TAX ADMINISTRATION

U.S. DEPARTMENT OF THE TREASURY

WASHINGTON, D.C. 20220

August 19, 2020

MEMORANDUM FOR: COMMISSIONER OF INTERNAL REVENUE

FROM: Michael E. McKenney
Deputy Inspector General for Audit

SUBJECT: Final Audit Report – Substantial Progress Has Been Made in Implementing the Insider Threat Capability, but Improvements Are Needed (Audit #202020002)

This report presents the results of our review to evaluate the effectiveness of Internal Revenue Service (IRS) efforts to implement an insider threat capability. This review is part of our Fiscal Year 2020 Annual Audit Plan and addresses the major management and performance challenge of *Security Over Taxpayer Data and Protection of IRS Resources*.

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

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

Background

Threats posed by an organization's employees and contractors are commonly referred to as "insider threats." 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. Internal Revenue Service (IRS) employees and contractors can pose a substantial risk due to their knowledge of and legitimate access to IRS systems, which can 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.

An insider threat is generally defined as an employee or contractor with authorized access to a network or data who could misuse that access by conducting unauthorized activities.

After the Calendar Year 2010 leak of classified material by a U.S. Army intelligence analyst, the President issued Executive Order 13587.[1] The executive order created the National Insider Threat Task Force (hereafter referred to as the National Task Force)[2] 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 (InTC) in support of the Treasury Department program.

The need for an IRS InTC is highlighted by internally reported concerns, such as an overreliance on perimeter defense security solutions that result in IRS networks being vulnerable to insider threats. In addition, the growth of cloud computing and mobility solutions is expanding and diversifying the cyberperimeters in need of protection. Finally, in June 2018, the Treasury Inspector General for Tax Administration (TIGTA) reported as a security weakness that the IRS was failing to sufficiently monitor the activities of system administrators, database administrators, and analysts who have increased access to data on its networks to carry out their roles and responsibilities.[4] These vulnerabilities could result in tax return data or Personally Identifiable Information being compromised.

The IRS has had various controls in place to deter and detect insider threats for several years. For example, the IRS's Unauthorized Access, Attempted Access, or Inspection of Taxpayer

[1] Executive Order 13587, *Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information* (October 7, 2011).
[2] See Appendix III for a glossary of terms.
[3] Treasury Department, Treasury Order 105-20, *Insider Threat Program* (August 9, 2013).
[4] TIGTA, Ref. No. 2018-20-030, *The Cybersecurity Data Warehouse Needs Improved Security Controls* (June 2018).

Records (also known as UNAX) Program to identify unauthorized access by employees to tax return data and Personally Identifiable Information was established in response to the Taxpayer Browsing Protection Act of 1997.[5] However, the requirements created by Executive Order 13587 and subsequent guidance have required the IRS to look at the insider threat in a more structured fashion. The IRS began formally implementing an InTC in Fiscal Year 2016. As of May 2020, the InTC is in an Initial Operating Capability state, with Full Operating Capability scheduled for Fiscal Year 2021.

Results of Review

Insider Threat Capability Implementation Efforts Have Resulted in Substantial Progress

Federal guidance related to insider threat programs stems from Executive Order 13587, which created the National Task Force and directed all agencies that operate or access classified computer networks to establish an insider threat and detection program. The National Task Force has released numerous documents designed to provide detailed guidance to agencies implementing an insider threat program. The Treasury Department subsequently issued Treasury Order 105-20 to establish its own Insider Threat Program.

The National Institute of Standards and Technology issued a revised Special Publication 800-53 (Revision 4), *Security and Privacy Controls for Federal Information Systems and Organizations* (April 2013), which included specific controls related to insider threats. Based on this revision, the IRS updated the Internal Revenue Manual to reflect the new internal control requirements and Treasury Department requirements to implement an InTC in support of the Treasury Department's program. TIGTA concluded that the IRS adhered to Federal guidance when designing its InTC and that controls generally are in place and effective. TIGTA noted the following accomplishments.

The IRS used relevant, applicable guidance to design the InTC and ensured that it is aligned with modernization goals

The IRS completed its initial InTC implementation plan in Fiscal Year 2017. The implementation plan included a description of the planned phases of the project as well as the expected services and elements needed to meet IRS Cybersecurity function goals for delivery of a mature InTC. The implementation plan also included information about the reporting processes and analytical tools to be deployed incrementally and how it would build advanced capability within the staff. The goal of the initial plan was to drive compliance with National Institute of Standards and Technology controls governing or directly related to the mitigation of insider threats. In Fiscal Year 2019, the InTC was incorporated into the IRS Integrated Modernization Business Plan and renamed the User Behavior Analytics Capability (UBAC) project. We reviewed this plan and determined that the UBAC project is properly aligned with the strategic goals expressed in the plan. Specifically, it addresses the modernization objective to proactively identify emerging threats and vulnerabilities through the use of real-time intelligence

[5] Pub. L. No. 105-35 (1997).

information and analytics, which supports the strategic goal to protect taxpayer data and address emerging threats.

The UBAC function is staffed by both IRS employees and contractors, each with specific responsibilities. In general, IRS employees are responsible for reviewing potential insider threats identified, including research and analysis to determine if the threat should be referred. The contractor staff are responsible for:

- Coordinating requirements and agreements for obtaining data; documenting threat data models; and developing, maintaining, and scheduling scripts.
- Developing predictive analytics and anomaly detection models, interpreting models and scripts, and developing model metrics and reports.
- Developing procedures, supporting the governance process, coordinating mitigation of insider threat anomalies with stakeholders, and training.

As part of its implementation efforts, the IRS designed and implemented a cross-functional committee to promote communications and shared responsibility across the IRS. This committee includes representatives from the Information Technology organization, the Human Capital Office, Criminal Investigation, and the Treasury Department. Agenda items have included employee awareness, training, data use, identification of cases, and reporting. In addition to the oversight provided by the cross-functional committee, the IRS assigned the Associate Chief Information Officer, Cybersecurity, as the executive responsible for deployment of the UBAC project.

Processes are implemented to identify and refer potential insider threats

The UBAC project is in an Initial Operating Capability state, and processes have been implemented that use specifically designed criteria, known as use cases, to identify potential insider threats. The IRS developed behavioral analytics processes based on various insider threat types defined by the Carnegie Mellon University's Computer Emergency Response Team and tailored them to the specific IRS threat landscape.

Potential insider threats are identified from a predefined series of machine and application log events that were combined to constitute a "behavior" that is potentially threatening to IRS systems, people, resources, and taxpayer content residing on these systems. The use cases have been incorporated into an analytics tool.

Although the UBAC project is still in an Initial Operating Capability state, processes have been implemented to identify potential insider threats.

The IRS implemented the following process that the UBAC function uses to identify and report on potential insider threat cases.

- The Enterprise Security Audit Trails and Cybersecurity Data Warehouse domains receive data feeds and notifications that support UBAC or compliance activities. The data are reviewed or stored in their domains or ingested into an analytics application.
- UBAC teams analyze the data via the appropriate platform, use cases, and Audit Control Response defined parameters.
- Output is collected and documented by an analyst.

- Cybersecurity management discusses the suspected cases of anomalous activity and determines appropriate action.

Development and implementation of processes for reporting on insider threats

The reporting process begins when UBAC analysts review an anomaly and a suspicious activity is identified. The overall reporting process is as follows.

- UBAC analysts:
  - Derive information from behavioral analysis of systems and other intake mechanisms, such as tips.
  - Review the use cases dashboard in analytics tools to identify anomalous conditions.
  - Render a decision about information that is derived, reported, or otherwise discovered, including whether it is a potential anomaly, risk, or related issue with relevance to an insider threat.
  - If it is a potential anomaly, risk, or related issue with relevance to insider threat, document information concerning the anomalous behavior.
- The project manager:
  - Coordinates with Cybersecurity Advisory Committee members, as appropriate.
  - Determines whether further analysis is required. If so, the issue is referred back to UBAC analysts for further review.
- The Cybersecurity Advisory Committee chair:
  - Reviews the final analysis from UBAC analysts.
  - If the issue is determined to be an anomalous finding, the matter is referred to the Decision Board for a final decision to refer the issue to the appropriate organization.
  - If the issue is not an anomalous finding, the issue is archived.

Initial operating capability results

Using the work flow and reporting processes described previously, from October 1, 2016, through February 29, 2020, the IRS identified 112 potential insider threats. Of these, nine potential threats were referred to the relevant stakeholders for investigation or resolution. The nature of these threats included potential unapproved access, manipulation of data, and a disgruntled employee. For the remaining 103 potential insider threats, the IRS closed 78 because the initial review concluded that the activity was not an insider threat. The other 25 were open and the UBAC function was in the process of determining whether they should be referred as potential insider threats. Figure 1 provides the number of Cybersecurity function referrals to other functions for additional analysis.

Figure 1: Cybersecurity Function Referrals

Function	Referrals
TIGTA	5
Information Technology Security Operations	2
Human Capital Office	1
Network Security	1
Total	9

Source: UBAC Inventory Status Reports, as of February 29, 2020.

Activities to achieve Full Operating Capability

To reach the Full Operating Capability state, the IRS has initiated the following activities that are currently in process:

- Developing enhanced user behavioral analytics for 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.
- Developing enhanced user behavioral analytics to proactively identify emerging insider threats through the use of real-time intelligence information and analytics to mitigate risks to data and systems arising from insider threats.

According to its status reports, the IRS is on schedule to deliver these capabilities during Fiscal Year 2021. As technologies evolve, the IRS plans to continue strengthening its threat intelligence capabilities even after achieving Full Operating Capability.

Additional Improvements Can Assist in Achieving an Effective Full Operating Capability

The National Task Force was created to provide standards and guidance to Federal agencies related to establishing an effective insider threat program. One type of guidance that it issued, referred to as the Insider Threat Framework, contained specific actions that can be taken to increase the effectiveness of insider threat programs, but also apply to capabilities.

Processes for determining high-value assets and assessing the related risks are not documented

The National Task Force recommends that agencies have a process in place to determine its high-value assets (also known as critical assets) and assess its risk posture as a cornerstone of an effective program. As they pertain to an InTC, high-value assets may be defined as those elements of the agency's mission that are essential to the agency and which, if damaged, stolen, or otherwise exploited, would have a damaging effect on the agency and its mission. One example is the Individual Master File, which contains up to 300 million sensitive records and supports other high-value assets.

IRS UBAC project implementation efforts did not include an assessment of risks to its high-value assets. The UBAC function was aware of the criteria but believed that the efforts were covered by other IRS functions. Therefore, the UBAC function did not include the identification and risk assessment of high-value assets in its implementation plan and did not document the results of those efforts. Without specifically addressing the identification and assessment of high-value assets, the IRS risks an incomplete capability implementation that may not consider these assets and cannot ensure that all high-value assets are included within the InTC and protected from insider threats.

The IRS did not include an assessment of risks to high-value assets as part of its UBAC project implementation efforts.

During the audit, the UBAC function initiated corrective actions to address this issue. Specifically, it obtained a list of high-value assets and conducted an initial mapping to risk indicators within its use cases.

Executive status reports did not include recommended elements

The National Task Force recommends that agencies submit status reports to executives at least annually. At a minimum, the status reports should document annual accomplishments, resources allocated, insider threat risks to the agency, recommendations and goals for program improvement, and major impediments or challenges.

Although the UBAC function's status reports included data related to accomplishments, resources, and risks, those status reports did not include:

- Recommendations and goals for program improvement.
- Major impediments or challenges.

While the UBAC function's status reports included many recommended metrics, those status reports did not include recommendations and goals for program improvement and major impediments or challenges.

The UBAC function believed that its status reports provided a vehicle for recommendations and goals for program improvement and major impediments or challenges; however, UBAC officials agreed that these items were not explicitly included within the status reports. Including these metrics in the status reports will ensure that UBAC personnel consider these metrics. In addition, without explicit reporting on recommendations and goals for program improvement and major impediments or challenges, the executives responsible for the implementation may not be aware of critical information useful for managing the implementation efforts.

During the audit, the UBAC function initiated a corrective action to address this issue. Specifically, it updated its biweekly meeting agenda to include a discussion of recommendations for program improvement and major impediments or challenges.

The implementation plan did not address recommended personnel training

The National Task Force recommends that agency heads ensure that personnel assigned to the insider threat program are fully trained in various disciplines and skills, including:

- Counterintelligence and security fundamentals.
- Procedures for insider threat response actions.

- Applicable laws and regulations regarding the gathering, integration, retention, safeguarding, and use of records and data, including the consequences of misuse of such information.
- Applicable civil liberties and privacy laws, regulations, and policies.
- Investigative referral requirements of Section 811 of the Intelligence Authorization Act for Fiscal Year 1995[6] as well as other policy or statutory requirements that require referrals to an internal entity, such as a security office or Office of Inspector General, or external investigative entities such as the Federal Bureau of Investigation, the Department of Justice, or military investigative services.

The UBAC project implementation plan did not specifically address the recommended training curricula. In addition, the IRS was only able to provide limited evidence of any specific training of UBAC personnel.

The UBAC function was not aware of the specific recommended training requirements for its personnel, and therefore, did not ensure that training was included in the plan and scheduled and completed by UBAC personnel. By not specifically addressing the National Task Force's recommended training in the UBAC project implementation plan, relevant training is not documented and could go unfulfilled, which may create skills and knowledge gaps. Without sufficient training on critical skillsets, the overall effectiveness of the IRS's InTC may be compromised.

Without sufficient training on critical skillsets, the overall effectiveness of the IRS's InTC may be compromised.

During the audit, the UBAC function initiated a corrective action to address this issue. Specifically, it identified three applicable training classes that were added to UBAC team members' training plans for Fiscal Year 2021. While UBAC officials acknowledged that available training classes may not mirror the titles recommended by the National Task Force, the training classes do contain the requisite content.

The Chief Information Officer should:

Recommendation 1: Ensure that the UBAC project implementation plan includes actions to determine and assess the risk posture of high-value assets. To efficiently complete these actions, the UBAC function should obtain and review the documentation of all high-value assets and related risk assessments of those assets performed by other IRS programs, if available. The identified high-value assets' risks should be addressed as part of the capability implementation.

Management's Response: The IRS agreed with the recommendation. The Cybersecurity function will ensure that the UBAC project implementation plan includes actions to determine and assess the risk posture of high-value assets. The UBAC function team will obtain and review the documentation of all high-value assets and related risk assessments of those assets performed by other IRS programs. The identified high-value assets' risks will be addressed as part of the capability implementation (Full Operating Capability).

[6] Pub. L. No. 108-359, 108 Stat. 3455 (1994).

Recommendation 2: 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.

> **Management's Response**: The IRS agreed with the recommendation. The Cybersecurity function's status reports will align with the National Insider Threat Task Force recommendations and include sections to address program improvement and major impediments or challenges.

Recommendation 3: 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.

> **Management's Response**: The IRS agreed with the recommendation. The Cybersecurity function will ensure that the UBAC project implementation plan includes the National Insider Threat Task Force's recommended training for UBAC personnel. In addition, the UBAC team will document all UBAC training efforts and, at least annually, ensure that all UBAC personnel have completed the required training. This is contingent upon budget availability.

Appendix I

Detailed Objective, Scope, and Methodology

The overall objective of this review was to evaluate the effectiveness of IRS efforts to implement an InTC. To accomplish our objective, we:

- Determined whether the development of the IRS InTC was consistent with established guidance by comparing the InTC implementation steps with identified criteria.
- Determined whether the implementation of the InTC was properly aligned with the IRS modernization effort by reviewing information in the IRS Integrated Modernization Business Plan and supporting documents.
- Evaluated the implementation status of the InTC's controls and tools by consulting with Cybersecurity management and reviewing documentation.
- Determined the effectiveness of fully implemented controls by identifying the controls and assessing their status.
- Identified new capabilities planned for the InTC for Fiscal Years 2020 and 2021, specifically those described in the project status report dated August 6, 2019.
- Determined the number of identified threats referred to stakeholders by obtaining and validating inventory information for suspicious activities identified by the UBAC function.

Performance of This Review

This review was performed with information obtained from the Cybersecurity function located in New Carrollton, Maryland, during the period September 2019 through May 2020. 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); Kent Sagara, Director; Joseph Cooney, Audit Manager; Steven Stephens, Lead Auditor; and Bret Hunter, 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: the UBAC Anomaly Reporting Standard Operating Procedures; the UBAC Process and Use Case Desk Guide; Internal Revenue Manual 10.8.1, *Information Technology Security, Policy and Guidance* (May 9, 2019); and National Institute of Standards and Technology Special Publication 800-53, Revision 4. We evaluated these controls by interviewing Cybersecurity function and UBAC function staff;

reviewing Internal Revenue Manual 10.8.1, the UBAC Anomaly Reporting Standard Operating Procedures, the UBAC Process and Use Case Desk Guide, and the National Institute of Standards and Technology guidelines; and comparing the UBAC Standard Operating Procedures to the National Task Force guidance and the other previously listed guidelines.

Appendix II

Management's Response to the Draft Report

CHIEF INFORMATION OFFICER

DEPARTMENT OF THE TREASURY
INTERNAL REVENUE SERVICE
WASHINGTON, DC 20224

July 27, 2020

MEMORANDUM FOR DEPUTY INSPECTOR GENERAL FOR AUDIT

FROM: Nancy A. Sieger Nancy A. Sieger Digitally signed by Nancy A. Sieger Date: 2020.07.26 08:24:06 -04'00'
Acting, Chief Information Officer

SUBJECT: Draft Audit Report – Substantial Progress Has Been Made in Implementing the Insider Threat Capability, but Improvements Are Needed (Audit # 202020002) (e-trak # 2020-24862)

Thank you for the opportunity to review your draft audit report and to discuss draft report observations with the Cybersecurity organization.

Insider Threat Capability (also known as User Behavior Analytics Capability) is an important Federal program with the goal of identifying, monitoring and reporting anomalous behaviors indicating potential insider threat activities. We appreciate the acknowledgement that the Internal Revenue Service (IRS) has made significant progress in implementing the Initial Operating Phase of our Insider Threat Program. We are committed to continuously improving cybersecurity capabilities and processes that will effectively improve mitigating controls to protect taxpayer information and IRS operations. We are encouraged by your acknowledgement of the progress we have made.

We will incorporate your recommendations into our processes moving forward. The continued support, assistance, and guidance your team provides is very valuable to us in this regard. Our corrective action plan for the recommendations is attached. If you have any questions, please contact me at (202) 317-5000 or a member of your staff may contact Malcolm Sykes, Director, Cybersecurity Operations at (901) 707-3062.

Attachment

Attachment

Draft Audit Report – Substantial Progress Has Been Made in Implementing the Insider Threat Capability but Improvements Are Needed (Audit #202020002)

RECOMMENDATION 1: The Chief Information Officer should ensure that the UBAC implementation plan includes actions to determine and assess the risk posture of high-value assets. To efficiently complete these actions, the UBAC function should obtain and review the documentation of all high-value assets and related risk assessments of those assets performed by other IRS programs, if available. The identified high-value assets' risks should be addressed as part of the capability implementation.

CORRECTIVE ACTION #1:
The Internal Revenue Service (IRS) agrees with the recommendation. Cybersecurity will ensure that the User Behavior Analytics Capability (UBAC) implementation plan includes actions to determine and assess the risk posture of high-value assets. The UBAC Team will obtain and review the documentation of all high-value assets and related risk assessments of those assets performed by other IRS programs. The identified high-value assets' risks will be addressed as part of the capability implementation (Full Operating Capability).

IMPLEMENTATION DATE: February 15, 2021

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 status reports align with the National Insider Threat Task Force recommendations and include sections to address program improvement and major impediments or challenges.

CORRECTIVE ACTION #2:
The Internal Revenue Service (IRS) agrees with the recommendation. Cybersecurity status reports will align with the National Insider Threat Task Force recommendations and include sections to address program improvement and major impediments or challenges.

IMPLEMENTATION DATE: October 15, 2020

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 on a monthly basis until completion.

Attachment

Draft Audit Report – Substantial Progress Has Been Made in Implementing the Insider Threat Capability but Improvements Are Needed (Audit #202020002)

RECOMMENDATION 3: The Chief Information Officer should ensure that the UBAC 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.

CORRECTIVE ACTION #3:
The Internal Revenue Service (IRS) agrees with the recommendation. Cybersecurity will ensure that the User Behavior Analytics Capability (UBAC) implementation plan includes the National Insider Threat Task Force's recommended training for UBAC personnel. In addition, the UBAC Team will document all UBAC training efforts and, at least annually, ensure that all UBAC personnel have completed the required training. This is contingent upon budget availability.

IMPLEMENTATION DATE: May 15, 2021

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 on a monthly basis until completion.

Appendix III

Glossary of Terms

Term	Definition
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.
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.
Individual Master File	The IRS database that maintains transactions and records of individual tax accounts.
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 Capability	The ability to identify and take action related to insider threats.
National Insider Threat Task Force	The principle 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 his or her 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.

Appendix IV

Abbreviations

InTC	Insider Threat Capability
IRS	Internal Revenue Service
TIGTA	Treasury Inspector General for Tax Administration
UBAC	User Behavior Analytics Capability