TREASURY INSPECTOR GENERAL FOR TAX ADMINISTRATION

Improvements Are Needed to Accurately Track and Safeguard Seized Digital Assets

July 1, 2025

Report Number: 2025-IE-R018

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

HIGHLIGHTS: Improvements Are Needed to Accurately Track and Safeguard Seized Digital Assets

Final Evaluation Report issued on July 1, 2025 **Report Number 2025-IE-R018**

Why TIGTA Did This Evaluation

In December 2023, IRS Criminal Investigation (IRS-CI) reported having seized digital assets totaling approximately $8 billion associated with open criminal investigations. A digital asset is any digital representation of value which is recorded on a cryptographically secured distributed ledger or any similar technology. Digital assets are stored electronically and can be bought, sold, owned, transferred, or traded.

This evaluation was initiated to assess the processes for the safeguarding and disposition of digital assets seized by IRS-CI.

Impact on Tax Administration

Digital assets pose a risk of facilitating money laundering, cybercrime, ransomware, narcotics, human trafficking, terrorism, and tax crimes. It is imperative that IRS-CI has adequate controls and processes to ensure that digital assets seized are safeguarded while in IRS custody and the underlying case is being adjudicated.

In addition, accurate inventory and recordkeeping of seized digital assets ensures proper protection of such assets.

What TIGTA Found

Our evaluation found that IRS-CI did not always follow established guidelines when seizing and safeguarding digital assets. Internal guidelines require that every seized digital asset be captured in a memorandum to ensure its tracking and accountability while in the IRS's control. However, seizure memorandums were not completed for all seized digital assets. Also, important information was not always included in completed seizure memorandums. For example, some memorandums did not include the seizure amount prior to transfer, the public addresses of the subject wallets, or the date the memorandum was completed.

We also identified deficiencies in the IRS's management and safeguarding of seized digital assets. For example, IRS-CI did not monitor a virtual wallet for subsequent criminal activity after IRS-CI identified the possibility of additional deposits being made into the wallet from dark web activity.

Additionally, IRS-CI's internal guidelines do not reference activities performed by its [redacted] related to seizing and safeguarding digital assets. The guidelines also do not address time frames for completing the required seizure memorandum and updating IRS-CI's seized assets inventory tracking system.

What TIGTA Recommended

We made six recommendations to the Chief, Criminal Investigation, to improve processes for the safeguarding and disposition of seized digital assets. IRS-CI agreed with five recommendations and partially agreed with one recommendation.

The recommendations that IRS-CI agreed with include: ensuring that IRS-CI personnel are familiar with and adhere to seizure memorandum requirements; establishing an inventory system that can manage seized digital assets to include accurately tracking the quantity of digital assets and ensure the consistent treatment of all seized digital assets; and updating internal guidelines to include time frame requirements for preparing the seizure memorandum and updating records in its inventory tracking system.

IRS-CI partially agreed with our recommendation to ensure that steps are taken to preserve the form of digital assets seized. While IRS-CI has notified its personnel to return assets to their original form, as frequently and intelligently as possible, and will document any divergences from this mandate, it may encounter situations where it cannot return the assets to their original form. We believe that IRS-CI's corrective actions are acceptable for this recommendation.

TREASURY INSPECTOR GENERAL
for Tax Administration

DATE: July 1, 2025

MEMORANDUM FOR: COMMISSIONER OF INTERNAL REVENUE

FROM: Nancy A. LaManna
Deputy Inspector General for Inspections and Evaluations

SUBJECT: Final Evaluation Report – Improvements Are Needed to Accurately Track and Safeguard Seized Digital Assets (Evaluation No.: IE-24-031)

This report presents the results of our evaluation to assess the processes for the safeguarding and disposition of digital assets seized by the Internal Revenue Service Criminal Investigation (IRS-CI). This review is part of our Fiscal Year 2025 Annual Program Plan and addresses the major management and performance challenge of *Tax Compliance and Enforcement*.

Management's complete response to the draft report is included as Appendix II. If you have any questions, please contact me or Kent Sagara, Director, Inspections and Evaluations.

Table of Contents

Background

The Internal Revenue Service Criminal Investigation (IRS-CI) has the authority to enforce the criminal provisions of Internal Revenue laws, as well as investigate violations of Internal Revenue laws and related statutes. As part of that authority, IRS-CI special agents can serve search warrants and seize personal property used, or intended for use, in violation of Internal Revenue laws or regulations.

Digital assets are stored electronically and can be bought, sold, owned, transferred, or traded. For tax purposes, a digital asset is defined as "any digital representation of value which is recorded on a cryptographically secured distributed ledger or any similar technology."[1]

Owners of digital assets use virtual wallets as an easy-to-use interface for sending, receiving, and storing these assets. Access to their digital assets is via the use of public and private keys.[2] Virtual wallets store these keys securely to enable owners to access and view their digital assets. Virtual wallets exist in several different forms, including:

A software or virtual wallet, which is a nonphysical storage coding downloaded as a software program that remains connected to the internet.

A hardware wallet, which is a physical device, such as an external storage drive, used to secure digital assets by storing private keys offline. Since a hardware wallet is not connected to the internet, it is viewed as the most secure type of wallet.

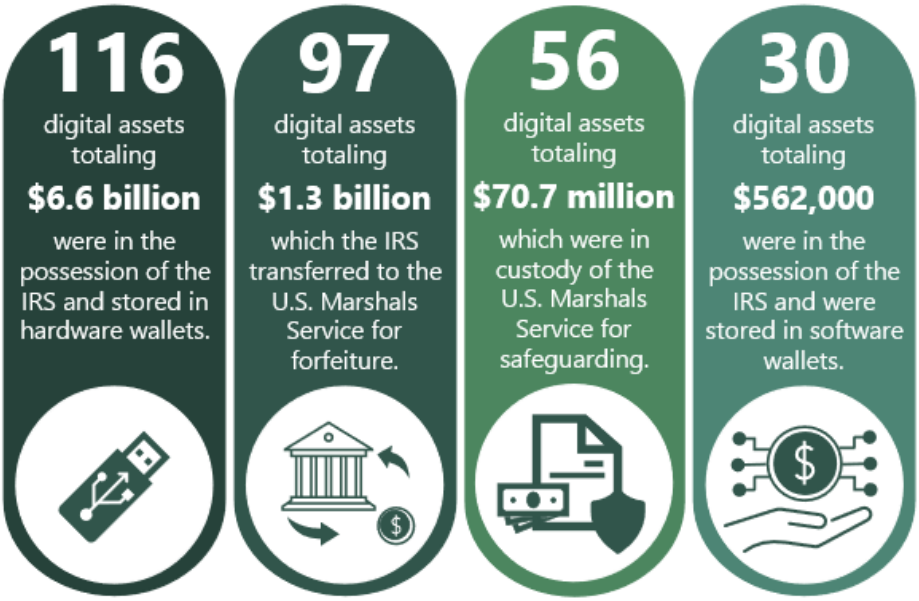
A paper wallet, which is a physical printout of the private keys.

In December 2023, IRS-CI reported having seized 299 digital assets totaling approximately $8 billion associated with open criminal investigations. IRS-CI seized these digital assets from individuals or businesses during the period of September 2017 to October 2023. Figure 1 presents a further explanation of these digital assets.

[1] Internal Revenue Code § 6045(g)(3)(D).

[2] A public key is a string of alphanumeric characters that functions as an address that the owner provides to receive digital assets. A private key is a string of alphanumeric characters or quick reference "QR" code known only to the owner that provides proof of ownership and allows the owner to send digital assets to others.

Figure 1: Seized Digital Assets From Open Investigations



Source: TIGTA-created infographic based on data obtained from IRS-CI, as of December 8, 2023.

Prior to Calendar Year 2021, the United States Marshals Service (USMS) took custody of some of the IRS-seized digital assets and liquidated the assets for the IRS upon forfeiture. The IRS now keeps custody of its seized digital assets until forfeiture, at which time the digital assets are transferred to the USMS for disposition. Criminal forfeiture in these cases generally occurs when a Final Order of Forfeiture is issued by the court.

Tracking and Accountability of Digital Asset Seizures

Within the IRS, the Asset Recovery & Investigative Services (ARIS) section of IRS-CI is responsible for the tracking and accountability from seizure to disposition of all seized digital assets held as evidence or for potential forfeiture. Several other IRS-CI offices and agencies are involved with seizing, processing, storing, safeguarding, and disposing of seized assets.

In October 2020, IRS-CI developed its *Crypto Seizure Guide version 1.2* that includes the following steps when seizing and securing digital assets:

- The IRS-CI case special agent prepares and submits Form 10908, *Computer Investigative Specialist (CIS) Request for Assistance,* to the [redacted].[3] Form 10908 engages and alerts the [redacted] about the digital asset seizure. The [redacted] uses Form 10908 to open a case in their system for tracking purposes.
- The CIS contacts and provides case details to the Digital Assets Seizure Specialist Group.
- A subject matter expert (SME) within the group will aid the requesting CIS to create the necessary types of virtual wallets required to seize the digital assets. Specifically, the SME helps the assigned CIS with the actual seizure (*i.e.*, the transfer of the seized digital assets into government-controlled wallets).

[3] [redacted] personnel are trained [redacted] to ensure digital evidence is acquired, authenticated, analyzed, and reported in a [redacted] sound manner according to [redacted] best practices.

- Following the seizure of the digital assets, the Digital Assets Seizure SME inventories the government wallets and compares them with the expected transfer amounts. Once completed, the SME emails an inventory of the seized digital assets to the CIS, case special agent, and ARIS personnel.
- Internal guidelines require the CIS or SME to complete a memorandum documenting the transfer of the digital asset following the seizure.

ARIS uses the previously mentioned memorandum to enter a new record or update an existing record in its *Asset Forfeiture Tracking and Retrieval System* (AFTRAK). AFTRAK is used to track and account for all seized assets, including digital assets. ARIS is responsible for maintaining, updating, and verifying AFTRAK information. Within ARIS, each IRS-CI field office Asset Forfeiture Coordinator is responsible for the accuracy and timeliness of information in AFTRAK.[4]

After these steps are completed, IRS-CI is then responsible for the accounting and safeguarding of the digital assets until disposition. Along with the requirements outlined previously, IRS-CI further updated its procedures and guidelines related to planning for a seizure, safeguarding, and disposition of seized digital assets in July 2024.

Results of Review

Our evaluation found that IRS-CI did not always follow established guidelines when seizing and safeguarding digital assets. Specifically, we identified the following:

- Seizure memorandums were not completed for all seized digital assets, as required.
- Required information was not always included in completed seizure memorandums.[5]
- Deficiencies managing and safeguarding seized digital assets.
- Inaccuracies associated with tracking some seized digital assets in AFTRAK.

We also found that internal guidelines were incomplete as they did not address:

- Important activities performed by the [redacted]; or
- The time frame for completing the required seizure memorandum and updating AFTRAK with digital asset seizure information.

Digital assets pose a risk of facilitating money laundering, cybercrime, ransomware, narcotics, human trafficking, terrorism, proliferation financing, and tax crimes. IRS-CI must have adequate controls and processes to ensure that digital assets seized are safeguarded while in IRS custody and the underlying case is being adjudicated. In addition, accurate inventory and recordkeeping of seized digital assets ensures proper accountability and demonstrates the IRS's stewardship for protecting such assets.

[4] The Asset Forfeiture Coordinator acts as the field office's expert in the seizure and forfeiture process, providing advice, performing analysis, and giving guidance to special agents and managers.

[5] While the IRS-CI did not complete memorandums for three seized digital assets, we found that an additional eight digital assets did not require memorandums, as they were frozen and not seized. As a result, we evaluated 66 memorandums that supported 288 digital assets.

IRS-CI Did Not Always Follow Established Guidelines for Seizing, Processing, Documenting, and Safeguarding Digital Assets

Our evaluation found that seizure memorandums were not completed for all seized digital assets as required. The 299 seized digital assets are associated with 45 criminal investigations involving 110 seizures.[6] We found that the required memorandums were not prepared to document the IRS's seizure for 3 (1 percent) of the 299 seized digital assets. These 3 digital assets totaled over $2.8 million.[7]

Completing the seizure memorandum is critical because it documents the securing and transfer of digital assets following the seizure. The memorandum also documents pertinent seizure information that supports the custody and value of seized assets, particularly through disposition proceedings.

Important information was not always included in seizure memorandums

We found that important information was not always included in completed seizure memorandums. For example, some memorandums did not include the seizure amount prior to transfer, the public addresses of the subject wallets, or the date when the memorandum was completed.

For records missing the public address(es) of the subject wallets, the documentation provided did not consistently identify the source of the funds (*i.e.*, the target wallet or a temporary government-controlled wallet). The absence of this information makes it more difficult to determine custody of the funds through digital asset transactions.

In addition, we identified two instances where the wallet address listed in the memorandum was not the correct wallet address. In another instance, the subject and government-controlled wallet addresses were switched in the memorandum.

Recommendation 1: The Chief, Criminal Investigation, should ensure that the CIS and SME are familiar with seizure memorandum requirements. This includes ensuring that seizure memorandums are completed with key activity information; and enforcing, monitoring, and adhering to guidelines.

> **Management's Response:** IRS management agreed with our recommendation. IRS-CI has procedures in place requiring CISs and SMEs involved with the digital asset seizure program to write a memorandum documenting each seizure. IRS management also implemented a quarterly reconciliation process to monitor memorandums for quality control purposes, ensuring that key activity information is included in the memorandums. The reconciliation process also serves to timely correct any identified recordation errors.

[6] There is no direct correlation between the number of seizures and the number of memorandums prepared. One investigation can have multiple seizures, and the CIS or SME can complete one memorandum per investigation or one memorandum per seizure.

[7] Asset value obtained from AFTRAK data, as of December 8, 2023. IRS-CI uses the asset value at the time of seizure for asset valuation. The actual total asset value could differ based on present day values. The market value for these assets totaled over $26 million on January 8, 2025.

Deficiencies in the management and safeguarding of some seized digital assets

We identified deficiencies related to managing and safeguarding seized digital assets. Examples include:

- One instance where three hardware wallets associated with a seizure could not be located. In an investigation of an IRS-CI case, the TIGTA Office of Investigations was informed that an IRS-CI special agent received five hardware wallets that were acquired through the Federal Bureau of Investigation (FBI) warrant process. The FBI transferred the wallets to IRS-CI because the FBI was not able to decrypt three of the five wallets. The IRS-CI special agent who received the wallets from the FBI separated from the IRS and allegedly turned in the three hardware wallets to their supervisor. At the time of our verification, ARIS and the [redacted] were not aware of these three wallets.
- One instance of an inadvertent shredding of the recovery seed phrase for a specific government-controlled wallet.[8] This shredding necessitated an additional transfer of the asset to a new wallet and incurred an additional transaction fee to generate a new set of seed words. In this scenario, the private key still worked, and the wallet was accessible. Had the private key not worked, the seized funds would have been permanently lost.
- One instance of a conversion of a digital asset to a different digital asset type during seizure. An error when inputting the government wallet address while attempting to seize a litecoin asset prevented the special agent from executing the seizure without converting the litecoin asset to bitcoin.[9] However, after the conversion and transfer to the government-controlled wallet, the special agent did not convert the seized digital asset back to its original litecoin digital currency. Best practices dictate that digital assets be kept in the form they were seized until a final order of forfeiture is entered.

The IRS stated that this conversion of a digital asset only happened once and is not standard practice. In this case, IRS-CI found a device containing digital assets while conducting a federal search warrant. An attempt was made to transfer the digital asset from the subject wallet to an IRS-controlled wallet; however, an error within the software prohibited the transfer. As a result, the litecoin found on the wallet was converted to bitcoin to complete the transfer to a government-controlled wallet. A memorandum documenting this conversion was memorialized at the time of transfer.

In a May 2024 alert, we recommended that IRS-CI take immediate action to 1) issue interim guidance to all personnel involved in the seizure of digital assets instructing them to maintain seized assets in the original digital asset type when transferring to a government wallet, and 2) adopt these interim policies until official guidance is formalized. When the May 2024 alert was issued, IRS-CI had not formalized the requirement that a digital asset should be maintained in the form it was seized until a final order of forfeiture. This requirement is now included in IRS-CI's internal guidance, effective July 2024.

[8] A seed phrase is a sequence of random words that stores the data required to access or recover virtual currency.

[9] Litecoin and bitcoin are types of virtual currencies.

Recommendation 2: The Chief, Criminal Investigation, should ensure that steps are taken to preserve the form of the digital asset seized. Policies and procedures should be implemented to restore a seized digital asset to its original currency type in the event the asset is converted to a different digital currency type to execute the seizure.

Management's Response: IRS management partially agreed with our recommendation. IRS-CI notified all personnel involved with the digital asset seizure program of the interim requirements to maintain seized assets in the original digital asset type, with the understanding that each case would be examined on its own merits. However, seizure warrants are fluid, dynamic operations that might be influenced by outside factors. For example, digital assets could get delisted (*i.e.*, no longer publicly traded), which means those digital assets should be issued in alternate digital assets.

In response to this recommendation, IRS-CI notified its personnel to return assets to their original form, as frequently and intelligently as possible, in consultation with applicable attorneys, case agents, and management as necessary. They will also document any divergences from this mandate by way of a memorandum.

Office of Inspections and Evaluations Comment: We believe that IRS-CI's corrective actions are acceptable for this recommendation.

- One instance where a virtual wallet was not monitored for subsequent criminal activity after the seizure of digital assets. For one seized digital asset, the SME documented as part of the seizure the possibility of additional deposits being made into the target's wallet from dark web activity. The SME stated that the wallet would be monitored for continued activity.

[redacted] management informed us that the case special agent identifies specific wallets to receive real-time updates, if there is the possibility for continued criminal activity. If the wallets receive additional funds known to be criminally related, the case special agent could seek additional seizure warrants or charges as part of the case.

For this wallet, the SME retired shortly after the seizure in 2018. Our review found no indication that IRS-CI continued to monitor the wallet beyond the SME's departure or made any attempts to seize the additional funds. When asked about this specific asset, IRS-CI officials stated that this wallet is used for training purposes and is in an IRS controlled wallet. As of October 2024, there were 3 additional transactions, totaling 0.22939139 bitcoin or approximately $14,060, posted to this account after the asset was forfeited.[10]

Recommendation 3: The Chief, Criminal Investigation, should implement policies and procedures to ensure that cases are appropriately transferred and adhere to the evidentiary chain of custody requirements when a special agent leaves the IRS.

Management's Response: IRS management agreed with our recommendation. IRS-CI has implemented policies and procedures to ensure that cases are appropriately transferred, and that IRS-CI adheres to the evidentiary chain of custody rules. The issue at hand was a single event. All field offices and asset forfeiture coordinators have been notified of the need to adhere to proper chain of custody procedures.

[10] The digital asset's value was calculated using the digital asset price in U.S. dollars on October 9, 2024.

Recordkeeping inaccuracies found in AFTRAK

Our review of AFTRAK records identified inaccuracies with the recordkeeping of some seized digital assets. The AFTRAK digital asset inventory records were not always accurate, and transactions were inconsistently recorded. Additionally, AFTRAK does not include individual fields to record the quantity and amount of digital assets seized.

For example, we found inaccurate asset locations for 128 (43 percent) of the 299 digital assets listed in AFTRAK. Some digital assets were listed as being stored in hardware wallets at a secure government facility when the assets had been moved and were stored by at a third-party location. Other digital assets were listed in AFTRAK as being stored in hardware wallets when the assets had been transferred to the USMS for forfeiture.

We also found discrepancies between the pre-transfer digital asset amount and the actual amount seized. We identified 3 digital assets (1 percent) of the 299 digital assets where the asset amount did not match the AFTRAK asset amount. For example, one digital asset showed 1.0764 bitcoin in AFTRAK, while the actual amount was 1.1764 bitcoin. On January 8, 2025, bitcoin was priced at $94,487 per 1 bitcoin, so the 0.1 discrepancy resulted in the asset being undervalued by $9,449.

We also noted inconsistent recording of transfer transaction fees incurred when seizing a digital asset. After comparing the digital asset quantities listed in AFTRAK with the supporting seizure documentation, we found transaction fees are not being recorded consistently. In some instances, the amount recorded is the amount in the subject's wallet at the time of the seizure. In other instances, the amount recorded is the amount transferred to a temporary government-controlled wallet, less the transaction fee; or the amount transferred to a permanent government-controlled wallet with or without the transaction fee. As a result, the quantities of seized digital assets in AFTRAK are inconsistent and may not accurately reflect the quantity seized or the quantity in the IRS's custody.

In addition, AFTRAK does not include individual fields to record the type and quantity of digital assets seized. When seized digital assets are recorded in AFTRAK, the assets are assigned a record number and entered into the system under "Virtual Currency" in the "Asset Type" field. AFTRAK users must use the "Asset Description" field to document both the type and quantity of the digital asset seized, which are needed to value the asset.

Recommendation 4: The Chief, Criminal Investigation, should establish an inventory system that can manage seized digital assets to include accurately tracking the quantity of digital assets to the fractional digit, and ensure that there is consistent treatment of all seized digital assets within its tracking system.

Management's Response: IRS management agreed with our recommendation. IRS-CI uses two tracking systems for seized digital assets: AFTRAK is the primary system, and the [redacted] system is the secondary system. The [redacted] system was created in late 2023 and updated in July 2024. It tracks fractional digits and ensures that there is consistent treatment of all seized digital assets within its tracking system. In January 2025, Cyber Headquarters promoted a field CIS to become the Cryptocurrency Seizure Team Lead in charge of all aspects of the digital asset seizure program. That individual immediately began drafting procedures as outlined for this finding. The ARIS Crypto Seizure Team will begin auditing AFTRAK after entries are made to ensure that the data input accurately matches the data from the seizure memorandum. Going

forward, ARIS and [redacted] personnel will audit the data to ensure continued accuracy.

Digital Asset Seizure and Safeguarding Guidelines Are Incomplete

We found that IRS-CI's internal guidelines do not reference important activities related to seizing and safeguarding digital assets. The guidelines also do not address time frames for completing the required seizure memorandum or updating AFTRAK. The internal guidelines lack details regarding the following [redacted] activities:

- [redacted], which consists of individuals responsible for securely generating and overseeing [redacted] seized digital asset wallets.
- [redacted].
- Executing the seizure and securing the transfer of seized digital assets.
- Coordinating with ARIS, USMS, and others when transferring assets to USMS for liquidation.
- Detailing the process for sanitizing hardware wallets before placing them back in use.

In addition, we found that internal guidelines do not explain the role of USMS related to safeguarding IRS digital assets seized prior to 2021. Currently, USMS has custodial control of 56 digital assets totaling over $70.7 million dollars.[11]

The IRS's internal manual references the National Code of Professional Conduct for Asset Forfeiture, which requires that seizing entities (*e.g.*, the IRS) develop and maintain guidelines detailing the statutory grounds for forfeiture, and all applicable policies and procedures. As noted earlier, IRS-CI formalized its internal guidelines for the pre-seizure planning of digital assets, as well as guidelines for the custody and storage of seized digital assets in July 2024. However, these updates do not include the activities detailed above, which we believe would improve IRS-CI's ability to track and manage seized digital assets.

Recommendation 5: The Chief, Criminal Investigation, should update the *Pre-Seizure Planning of Digital Assets* and the *Custody and Storage of Seized Assets* guidelines to accurately reflect the processes to follow from seizure to disposition of seized digital assets.

Management's Response: IRS management agreed with our recommendation. [redacted] personnel, in cooperation with ARIS and Cyber Headquarters, updated the guidelines listed above to ensure that post-seizure memorandums are completed within five business days of the action that generated the need for the memorandum. These procedures will be made permanent in the next update of our internal procedures. The ARIS Crypto Seizure Team will begin auditing AFTRAK after entries are made to ensure that the data input accurately matches the data from the seizure memorandum. Going forward, ARIS and [redacted] personnel will audit the data to ensure continued accuracy.

[11] Total asset value obtained from AFTRAK data as of December 8, 2023. The IRS uses the asset value at the time of seizure. The actual total asset value could differ based on present day values.

Guidelines do not detail the time frame for completing required seizure memorandums and updating AFTRAK

As noted previously, IRS-CI internal guidelines do not provide a specific time frame in which the required seizure memorandum is to be prepared after the digital asset seizure date. Internal guidelines state that the seizing CIS or SME must complete a seizure memorandum that documents the securing and transferring of seized digital assets.

The timeliness of preparing and issuing the memorandums to ARIS affects how timely ARIS personnel can enter/update seized asset records in AFTRAK. Although internal guidelines require the timely updating of AFTRAK data, IRS-CI has not developed guidelines defining time frames for preparing the seizure memorandum, providing the memorandum to ARIS, and entering transaction data into AFTRAK after receipt of the memorandum.

Our review of the 299 digital assets determined that a seizure memorandum was completed for 288 of the digital assets. For these 288 digital assets, we identified 71 (25 percent) where we were unable to verify the time frame in which the required seizure memorandum was prepared after the seizure. Specifically, for these 71 digital assets, date information was not included in the seizure memorandum or the associated documentation we reviewed.

For the remaining 217 of the 288 seized digital assets, we determined that:

- 104 digital asset records showed the memorandum was prepared more than 30 days after the asset seizure date. For 19 of these, the memorandum was prepared almost 3 years after the asset seizure date.
- 70 digital asset records showed the memorandum was prepared within 5 days of the asset seizure date.
- 43 digital asset records showed the memorandum was prepared more than 5 days, but less than 30 days, from the asset seizure date.

Establishing time frames for completing these procedures can help ensure that AFTRAK data are timely and accurately updated. It is critical to update AFTRAK as soon as possible since the IRS uses AFTRAK to provide data to the Treasury Executive Office for Asset Forfeiture, and to prepare financial statements and other reports for Congress.

Recommendation 6: The Chief, Criminal Investigation, should update internal guidelines to include time frame requirements for preparing the seizure memorandum and updating records in AFTRAK.

> **Management's Response:** IRS management agreed with our recommendation. IRS-CI updated the internal guidelines to require that all memorandums drafted as part of a seizure action, or any movement of digital assets, will be completed within five business days after the time of the action that generated the need for a memorandum. This guidance is interim until final policies can be updated.

Appendix I

Detailed Objective, Scope, and Methodology

The overall objective of this project was to assess the processes for the safeguarding and disposition of digital assets seized by IRS-CI. To accomplish our objective, we:

- Evaluated policies and procedures to ensure that seized digital assets are properly handled, protected, and recorded while in IRS custody.
- Identified all digital assets seized by IRS-CI and reconciled these assets from seizure to disposition.
- Analyzed and verified AFTRAK data to assess IRS-CI's safeguarding of seized digital assets.
- Reviewed disposition information to determine the accuracy and timeliness of the data.

Performance of This Review

This review was performed at, and with information obtained from, the ARIS section of IRS-CI in Washington, D.C., and IRS-CI's [redacted], during the period of December 2023 through January 2025. We conducted this evaluation in accordance with the Council of the Inspectors General for Integrity and Efficiency's *Quality Standards for Inspection and Evaluation*. Those standards require that the work adheres to the professional standards of independence, due professional care, and quality assurance and followed procedures to ensure accuracy of the information presented. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions.

Appendix II

Management's Response to the Draft Report

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

Criminal Investigation

May 20, 2025

MEMORANDUM FOR NANCY LAMANNA
DEPUTY INSPECTOR GENERAL FOR INSPECTIONS AND EVALUATIONS TREASURY INSPECTOR GENERAL FOR TAX ADMINISTRATION

FROM: Guy Ficco
Chief, Criminal Investigation

SUBJECT: Draft Evaluation Report - Evaluation# IE-24-031, Improvements are Needed to Accurately Track and Safeguard Seized Digital Assets

Thank you for the opportunity to review and comment on the TIGTA Draft Report #IE-24-031 – *"Improvements Are Needed to Accurately Track and Safeguard Seized Digital Assets"*, dated March 25th, 2025. The IRS takes seriously our responsibility to ensure that all policies related to our administration of digital asset seizures demonstrate proper controls with only the highest levels of efficiency and security in mind. We are committed to adhering to all federal laws, regulations, and IRS policies, procedures and guidelines that are applicable to the management of our criminal restitution assessment procedures.

The IRS has numerous controls in place to ensure responsible management of our digital asset seizure program. We appreciate TIGTA's recommendations to improve controls and overall management.

Attached is our response to your recommendations. If you have any questions, please contact Joleen Simpson, Acting Executive Director of Global Operations, Policy & Support, at (571) 641-5832.

Attachment

Recommendation 1
The Chief, Criminal Investigation should ensure that the CIS and SME are familiar with seizure memorandum requirements. This includes ensuring that seizure memorandums are completed with key activity information; and enforcing, monitoring, and adhering to guidelines.

CORRECTIVE ACTION
AGREE - Internal Revenue Service – Criminal Investigation (IRS-CI) has procedures in place requiring CISs and SMEs involved with the digital asset seizure program to write a memo documenting each seizure. This memo is sent to the Crypto Seizure Team, the ARIS Crypto Seizure Team, the Case Agent, and the local Asset Forfeiture Coordinator (AFC).

In the second quarter of FY 2025, IRS-CI's [redacted], Cyber Headquarters, and ARIS, implemented a quarterly reconciliation process. The reconciliation process allows IRS-CI to monitor memos for quality control purposes, ensuring key activity information is included in the memos. The reconciliation process also serves to timely correct any identified recordation errors.

IMPLEMENTATION DATE
July 1, 2024

RESPONSIBLE OFFICIAL
IRS-CI Executive Director of [redacted]

CORRECTIVE ACTION MONITORING PLAN
IRS will monitor this corrective action as part of our internal management system of controls.

RECOMMENDATION 2
The Chief, Criminal Investigation should ensure that steps are taken to preserve the form of the digital asset seized. Policies and procedures should be implemented to restore a seized digital asset to its original currency type in the event the asset is converted to a different digital currency type to execute the seizure.

CORRECTIVE ACTION
PARTIALLY AGREE - IRS-CI has a policy in place which requires CISs and SMEs to preserve the form of the digital asset upon seizure as best as possible. In May 2024, the Treasury Inspector General for Tax Administration (TIGTA) recommended IRS-CI take immediate action to: 1) issue interim guidance to all personnel involved in the seizure of digital assets instructing them to maintain seized asset in the original digital asset type when transferring to a government wallet, and 2) adopt these interim policies until official guidance is formalized.

IRS-CI immediately notified all personnel involved with the Digital Asset seizure program of the interim requirements with the understanding that each case would be examined on its own merits. Seizure warrants, and the search warrants that often predicate them, are fluid, dynamic operations which require not only extreme attention to detail but also attention to outside factors. Many of those factors are legal in nature. As an example,

two exchanges recently delisted digital assets and issued alternate digital assets in their place. If IRS-CI had held these original assets under the TIGTA policy recommendation, then we would have no action other than to attempt to return the exchanged assets back to their original form which no longer exists.

Additionally, exchanges sometimes notify their users in advance of a delisting. If IRS-CI had seized a digital asset that was then presented on an exchange's delisting list, then converting the asset back to one that will be delisted is equivalent to destroying the asset. This action goes directly contrary to the work we have been charged to do.

Even though most of our digital assets are preserved in the form we seized them, we do occasionally run into issues noted by this recommendation. Because we are a law enforcement agency, our policies require some level of flexibility. We often work with drastically varying aspects of the public. Oftentimes we work with both sophisticated and unsophisticated subjects who use specific digital assets to obfuscate or overengineer a scheme. If the recommendation was implemented unilaterally the way TIGTA has recommended, then we would be unable to complete our job in those edge cases which require flexibility and clear documentation.

In response to this recommendation, IRS-CI has notified its personnel to return the asset to their original form as frequently and intelligently as possible in consultation with the applicable attorneys, case agents, and management as necessary. We will then document any divergences from this mandate by way of a memo.

IMPLEMENTATION DATE
May 1, 2024

RESPONSIBLE OFFICIAL
IRS-CI Executive Director of [redacted]

CORRECTIVE ACTION MONITORING PLAN
IRS will monitor this corrective action as part of our internal management system of controls.

RECOMMENDATION 3
The Chief, Criminal Investigation should implement policies and procedures to ensure that cases are appropriately transferred and adhere to the evidentiary chain of custody requirements when a special agent leaves the IRS.

CORRECTIVE ACTION
AGREE - IRS-CI has implemented policies and procedures to ensure that cases are appropriately transferred, and that IRS-CI adheres to the evidentiary chain of custody rules. The issue at hand was a single event and all field offices and AFCs have been notified of the need to adhere to proper chain of custody procedures.

IMPLEMENTATION DATE
July 1, 2024

RESPONSIBLE OFFICIAL

IRS-CI Executive Director, [redacted]

CORRECTIVE ACTION MONITORING PLAN
IRS will monitor this corrective action as part of our internal management system of controls.

RECOMMENDATION 4
The Chief, Criminal Investigation should establish an inventory system that can manage seized digital assets to include accurately tracking the quantity of digital assets to the fractional digit and ensure that there is consistent treatment of all seized digital assets within its tracking system.

CORRECTIVE ACTION
AGREE – IRS-CI established an inventory management system to ensure consistent treatment of all seized digital assets. IRS-CI uses two tracking systems for seized digital assets. The primary system is AFTRAK. [redacted] uses a separate system to manage seized digital assets. The [redacted] system, in its current iteration, was created in late 2023 and updated in July 2024. It tracks fractional digits and ensures that there is consistent treatment of all seized digital assets within its tracking system. The Draft Evaluation Report also suggests that the [redacted] portion of the Seizure Team establish guidelines [redacted]; executing the seizure and securing the transfer of seized digital assets, coordinating with ARIS, the United States Marshals Service (USMS), and others when transferring assets to USMS for liquidation; and detailing the process for sanitizing hardware wallets before placing them back in use.

In January 2025, Cyber Headquarters promoted a field CIS to become the Cryptocurrency Seizure Team Lead in charge of all aspects of the digital asset seizure program. That individual immediately began drafting procedures as outlined by the TIGTA Draft Evaluation. The ARIS Crypto Seizure Team will begin auditing AFTRAK after entries are made to ensure that the data input accurately matches the data from the seizure memo. Going forward, ARIS and [redacted] personnel will audit the data to ensure continued accuracy.

IMPLEMENTATION DATE
July 1, 2024

RESPONSIBLE OFFICIAL
IRS-CI Executive Director, Global Operations Policy & Support with coordination from IRS-CI Executive Director of [redacted]

CORRECTIVE ACTION MONITORING PLAN
IRS will monitor this corrective action as part of our internal management system of controls.

RECOMMENDATION 5

The Chief, Criminal Investigation should update the Pre-Seizure Planning of Digital Assets and the Custody and Storage of Seized Assets guidelines to accurately reflect the processes to follow from seizure to disposition of seized digital assets.

CORRECTIVE ACTION
AGREE - [redacted] personnel in cooperation with ARIS and Cyber Headquarters updated the guidelines listed above to ensure that post-seizure memos are completed within five business days of the action that generated the need for the memo. These procedures will be made permanent in the next update of our internal procedures. The ARIS Crypto Seizure Team will begin auditing AFTRAK after entries are made to ensure that the data input accurately matches the data from the seizure memo. Going forward, ARIS and [redacted] personnel will audit the data to ensure continued accuracy.

IMPLEMENTATION DATE
July 1, 2024

RESPONSIBLE OFFICIAL
IRS-CI Executive Director, [redacted] with coordination from IRS-CI Executive Director, Global Operations Policy & Support

CORRECTIVE ACTION MONITORING PLAN
IRS will monitor this corrective action as part of our internal management system of controls.

RECOMMENDATION 6
The Chief, Criminal Investigation should update internal guidelines to include the time frame requirements for preparing the seizure memorandum and updating records in AFTRAK.

CORRECTIVE ACTION
AGREE - IRS-CI updated the internal guidelines to require that all memos drafted as part of a seizure action, or any movement of digital assets will be completed within five (5) business days after the time of the action that generated the need for a memo. This guidance is in interim status until final policies can be updated.

IMPLEMENTATION DATE
July 1, 2024

RESPONSIBLE OFFICIAL
IRS-CI Executive Director, Global Operations, Policy & Support with coordination from IRS-CI Executive Director of [redacted]

CORRECTIVE ACTION MONITORING PLAN
IRS will monitor this corrective action as part of our internal management system of controls.

Appendix III

Abbreviations

AFTRAK	Asset Forfeiture Tracking and Retrieval System
ARIS	Asset Recovery & Investigative Services
CI	Criminal Investigation
CIS	Computer Investigative Specialist
FBI	Federal Bureau of Investigation
IRS	Internal Revenue Service
SME	Subject matter expert
TIGTA	Treasury Inspector General for Tax Administration
USMS	United States Marshals Service

To report fraud, waste, or abuse,
contact our hotline on the web at
https://www.tigta.gov/reportcrime-misconduct.

To make suggestions to improve IRS policies, processes, or systems affecting taxpayers, contact us at www.tigta.gov/form/suggestions.

Information you provide is confidential, and you may remain anonymous.