TREASURY INSPECTOR GENERAL FOR TAX ADMINISTRATION

Laptop and Desktop Sanitization Practices Need Improvement

September 20, 2021

Report Number: 2021-20-056

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

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

HIGHLIGHTS: Laptop and Desktop Sanitization Practices Need Improvement

Final Audit Report issued on September 20, 2021 **Report Number 2021-20-056**

Why TIGTA Did This Audit

In August 2019, the Information Technology organization resumed sanitizing laptops, desktops, and smartphones at its Memphis Sanitization Site. This audit was initiated to assess the effectiveness of the Information Technology organization's hardware asset sanitization process for laptops, desktops, and smartphones.

Impact on Taxpayers

The IRS is required to protect the confidentiality of taxpayer information, including taxpayer information stored on laptops, desktops, and smartphones. Sanitization is a key element in assuring confidentiality. If an unauthorized disclosure of tax or Personally Identifiable Information occurred, it could result in substantial harm, embarrassment, and loss of public confidence in the IRS. An unauthorized disclosure could also harm an individual.

What TIGTA Found

The IRS is not using an approved sanitization product to overwrite sensitive taxpayer data on laptop and desktop hard disks, nor is it annually testing its sanitization equipment and procedures at the Memphis Sanitization Site to verify that the intended sanitization results are being achieved. In addition, while the IRS is sanitizing most of its laptops and desktops, its process to independently verify the sanitization of each laptop and desktop is ineffective. Further, draft *Memphis Sanitization Site Standard Operating Procedures* need to be clarified concerning accounting for damaged or missing hard disks.

Based on a statistical interval sample of 87 laptops and desktops from a population of 3,882 computers sanitized between January and March 2021, TIGTA determined that one computer was not sanitized and two computers were missing hard disks. Projecting the sample results to the total population of computers sanitized during this period, TIGTA estimates that 45 computers may not have been properly sanitized and 89 computers may be missing hard disks. In addition, there were six computers in the sample with bad sector error messages, which could potentially allow readable information to be recovered. However, further testing did not identify any residual data.

TIGTA also observed the smartphone wiping process and tested a judgmental sample of eight smartphones to determine that the Memphis Sanitization Site had effectively sanitized them. No exceptions were noted.

What TIGTA Recommended

TIGTA recommended that the Chief Information Officer ensure that: 1) the IRS only uses approved sanitization products; 2) sanitization equipment and procedures are tested annually; 3) hard disks that were not sanitized or that had bad sector errors are degaussed or destroyed; 4) hard disks separated from their respective computers are properly accounted for throughout the sanitization process; 5) guidance is clarified to further define accounting for damaged or missing hard disks; and 6) hard disk sanitization results are independently verified using an approved verification software tool.

The IRS agreed with our recommendations. The IRS plans to 1) purchase and implement approved sanitization tools and products (contingent upon funding); 2) implement annual testing of the Memphis sanitization equipment and procedures; 3) degauss or destroy hard disks identified during this review that were not sanitized or had bad sector errors; 4) implement procedures to properly account for hard disks separated from their computers; 5) revise the standard operating procedures to clarify and further define procedures to account for damaged or missing hard disks; and 6) evaluate the Memphis hard disk sanitization process and implement an approved independent sanitization verification tool.

TREASURY INSPECTOR GENERAL
FOR TAX ADMINISTRATION

U.S. DEPARTMENT OF THE TREASURY

WASHINGTON, D.C. 20220

September 20, 2021

MEMORANDUM FOR: COMMISSIONER OF INTERNAL REVENUE

FROM: Michael E. McKenney
Deputy Inspector General for Audit

SUBJECT: Final Audit Report – Laptop and Desktop Sanitization Practices Need Improvement (Audit # 202120013)

This report presents the results of our review to assess the effectiveness of the Information Technology organization's hardware asset sanitization process for laptops, desktops, and smartphones. This review is part of our Fiscal Year 2021 Annual Audit Plan and addresses the major management and performance challenge of *Enhancing Security of Taxpayer Data and Protection of IRS [Internal Revenue Service] Resources*.

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

Background

The Internal Revenue Service (IRS) collects, processes, and maintains tax returns and related information. The IRS is required to protect the confidentiality of taxpayer information, including taxpayer information stored on laptops, desktops, and smartphones. Specifically, Internal Revenue Manual 10.5.1, *Privacy and Information Protection Privacy Policy* (September 2020), requires the IRS to protect and safeguard sensitive but unclassified data, including tax information and Personally Identifiable Information.

Within the Information Technology organization,[1] the User and Network Services (UNS) function manages the Memphis Sanitization Site (MSS) located at the Enterprise Computing Center – Memphis. The MSS is responsible for receiving IRS end-user laptops, desktops, and smartphones for sanitization, properly sanitizing them, and transferring them to the Facilities Management and Security Services (FMSS) function for disposal.

Sanitization refers to a process that renders access to target data on the laptop, desktop, or smartphone unrecoverable. Sanitization is a key element in assuring confidentiality. The National Institute of Standards and Technology (NIST) Special Publication 800-60, Volume II, Revision 1, *Appendices to Guide for Mapping Types of Information and Information Systems to Security Categories* (August 2008), defines confidentiality as preserving authorized restrictions on information access and disclosure, including the means to protect personal privacy and proprietary information. A loss of confidentiality is the unauthorized disclosure of information. Hard disk sanitization and disposal is significant because of the sensitive or critical information stored on the laptops, desktops, and smartphones.

Applying effective sanitization techniques and tracking hardware asset inventory are critical aspects to ensure that sensitive data are protected against unauthorized disclosure. It is important to ensure that no residual data remain on the laptops, desktops, and smartphones before they leave the IRS's control. Overwriting or wiping with sanitization software is a process whereby sensitive information on a computer is overwritten with at least a single write pass of nonsensitive information with a fixed data value, such as all zeros. Comparatively, degaussing uses a machine to apply a reverse magnetic field on a computer's hard disk to render it permanently unusable. While the goal of sanitization software is to replace the sensitive data on the hard disk with nonsensitive data, the goal of degaussing is to ensure complete erasure of the hard disk.

NIST guidance further outlines the security categories of the information types that the IRS uses, which include 1) taxation management information and 2) personal identity and authentication information. Both information types are assigned a security category of moderate confidentiality. If an unauthorized disclosure of information having a moderate confidentiality occurred, this could be expected to have a serious adverse effect on organizational operations, organization assets, or individuals.

In January 2016, the Associate Chief Information Officer, UNS function, issued a memorandum that mandated that UNS function personnel refrain from sanitizing the data from any hard disk associated with an end-user. This applied to all end-user computers and smartphones, including

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

those belonging to separating employees. In addition, personnel were instructed that hard disks were to remain intact with their respective computers.

In July 2019, the Associate Chief Information Officer, UNS function, issued a memorandum lifting the sanitization moratorium, advising UNS function personnel that, effective August 5, 2019, they were to resume information technology equipment wiping and disposal operations. This guidance applied to all end-user computers and smartphones. The MSS subsequently resumed sanitization operations using a first in, first out rotation of stockpiled computers and smartphones. As of October 2020, the MSS had 61,809 unsanitized computers (28,370 laptops and 33,439 desktops) and 7,996 unsanitized smartphones.

Results of Review

Laptops and Desktops Were Sanitized Using an Unapproved Sanitization Product

The UNS function was unable to provide sufficient evidence that the software product it is using as a sanitization tool is properly approved for use by the Federal Government. [redacted]. However, the UNS function only provided:

1) A statement from the vendor's website that its product conformed to 1995 Department of Defense standards.
2) Internal guidance from a decade ago that stated, "The purging process is the removal of sensitive but unclassified data from computer media by using the approved [product name] overwriting process or degaussing the media."
3) A screenshot from the IRS's Enterprise Standards Profile mentioning that the sanitization software was an IRS-approved product.

We reviewed the list of sanitization software that the Common Criteria Recognition Arrangement[2] has certified using the Common Criteria for Information Technology Security Evaluation.[3] The Common Criteria Recognition Arrangement is comprised of 31 government agencies representing their respective member countries, with the Department of Defense representing the United States. While the Common Criteria Recognition Arrangement certified at least four sanitization software products between November 2017 and August 2020, the product that the UNS function is using is not on the list of certified products. Once certified, the products remain on the Certified Products List for five years.

In addition, the IRS has not tested the MSS's sanitization equipment and procedures to verify that the intended sanitization is being achieved. [redacted]

[2] The Common Criteria Recognition Arrangement is composed of each signatory's country representatives, where member countries recognize the products certified by the arrangement.

[3] An international standard (ISO/IEC 15408) for evaluating and certifying information security products.

[redacted]. The IRS responded that this policy, Internal Revenue Manual 10.8.1, is only applicable to systems categorized as having a Federal Information Processing Standards Publication 199, *Standards for Security Categorization of Federal Information and Information Systems* (February 2004), rating for high confidentiality. We asked the IRS to provide a list of IRS systems with a security categorization of high confidentiality. There were two [redacted]-owned systems, which deal with [redacted] and two IRS systems that [redacted] assigned this categorization. However, [redacted] are also stored on [redacted] that do not have this security categorization.

We believe that security over [redacted], regardless of where or how it is stored, should not be treated differently. This is consistent with Internal Revenue Manual 10.5.1, which provides that systems "…with moderate or high confidentiality levels means the potential for harm ranges from serious to severe or catastrophic, with significant to severe impact to an individual or the IRS. [redacted] is an example of high risk Personally Identifiable Information."

In addition, UNS function management stated that they used the sanitization software with the understanding that the IRS had attained approval to use the tool in the past. However, without using a currently approved sanitization product and annually testing the sanitization equipment and procedures to ensure that the desired results are being achieved, the risk exists that the sanitization product could fail to remove residual information from laptop and desktop hard disks. If not sanitized properly, release of the hard disks outside of the IRS could lead to unauthorized disclosure of confidential taxpayer information.

Management Action:

In June 2021, UNS function management stated that they acquired and are now using a National Security Agency–approved degausser to purge data on hard disks at the MSS for laptops and desktops that will be disposed of outside of the IRS. Because the IRS acquired the degausser at the end of our audit work, we were unable to test its effectiveness. However, if calibrated correctly, we believe that the degausser will effectively ensure complete erasure of the hard disks.

For the remaining computers that the UNS function expects to reuse within the IRS, UNS function management is working to identify and implement a sanitization software solution. The UNS function is also in the process of acquiring a Solid State Drive Disintegrator, which is designed specifically for the destruction of solid state hard drives.

The Chief Information Officer should ensure that:

Recommendation 1: The IRS only uses sanitization products that are approved by the Department of Defense, the Department of Homeland Security, or the National Security Agency.

Management's Response: The IRS agreed with this recommendation. The IRS will purchase and implement sanitization tools and products that are approved by the Department of Defense, the Department of Homeland Security, or the National Security Agency (contingent upon funding).

Recommendation 2: Sanitization equipment and procedures are tested annually to verify that the intended sanitization results are being achieved.

> **Management's Response:** The IRS agreed with this recommendation. The Chief Information Officer will implement annual testing of the Memphis sanitization equipment and procedures to verify that the intended sanitization results are being achieved.

Most Sampled Laptops and Desktops Were Sanitized

To test the effectiveness of the computer sanitization process, we selected and tested a random statistical sample[4] of sanitized laptops and desktops to determine whether residual data remained on the computers' hard disks. Specifically, we randomly selected a statistical interval sample of 87 (2.24 percent) computers from a population of 3,882 computers that the MSS sanitized between January and March 2021. We used sanitization verification software from a different vendor to independently test if the sanitization was effective. Figure 1 shows the results of our sanitization verification testing.

Figure 1: Sample Results of Testing Sanitized Computers for Residual Data

Test Results	Computers in Sample
Hard Disk Not Sanitized but Encrypted	1
Hard Disk Was Missing	2
Hard Disk With "Error Accessing Drive Sectors"[5] Message	6
Hard Disk Sanitized	78
Total	**87**

Source: Treasury Inspector General for Tax Administration analysis of a statistical interval sample of laptops and desktops the MSS sanitized between January and March 2021.

For the one unsanitized computer, we observed that the hard disk was encrypted. [redacted]. If encryption is properly enabled, the risk of inadvertent disclosure of confidential information is significantly reduced even if the hard disk was not sanitized. At our request, the IRS tried to locate the two computers with missing hard disks, but it ultimately was unable to do so. As a result, we were unable to test these two hard disks to determine if they had been sanitized and if the sanitization process was effective.

[4] Because the population of sanitized devices was constantly changing due to new assets being received and stockpiled assets being sanitized, we used interval attribute sampling, a form of random sampling that allowed for the selection of sample items from the sanitized population of devices as the sanitization occurred during our audit work.

[5] A bad sector is a tiny cluster of storage space that is defective on the hard disk. Such disk sectors can result from physical or software damage and could potentially allow readable information to be recovered from the damaged sectors.

Projecting our sample results to the total population of computers the MSS sanitized between January and March 2021, we estimate that 45 (1.16 percent)[6] of the 3,882 sanitized computers may not have been properly sanitized. Further, we estimate that 89 (2.30 percent)[7] of the 3,882 computers may have been missing hard disks that were not identified in the MSS's hardware asset inventory (the inventory issue is discussed in the next section).

For the remaining six computers with bad sector error messages, we used a different vendor's data recovery software to retest the hard disks for the existence of residual data. Although our additional testing did not identify any residual data, NIST Special Publication 800-88, Revision 1, *Guidelines for Media Sanitization* (December 2014), states that overwriting cannot be used for media that are damaged or not rewriteable. However, degaussing or destruction are acceptable methods to purge damaged media containing sensitive information.

Draft *MSS Standard Operating Procedures* need to be clarified concerning accounting for damaged or missing hard disks

During our review, two sampled computers with missing hard disks were incorrectly stored on a pallet with sanitized devices and incorrectly recorded as accounted for in the MSS's hardware asset inventory. Internal Revenue Manual 2.149.1, *Asset Management, Asset Management (AM) Policy* (September 2018), states that the Information Technology organization is "responsible for the accounting and recording of IT [information technology] property in the inventory system.... This process supports the integrity of the data by ensuring accurate and complete asset records are maintained." However, draft *MSS Standard Operating Procedures* state that personnel should remove the computer's damaged hard disk and give it to the tape library at the Enterprise Computing Center – Memphis but does not clearly define under what circumstances to do so, any time frame for doing so, or how to account for the hard disks in the MSS's hardware asset inventory. In addition, these procedures do not explain how to account for computer shells sent to the MSS with missing hard disks. This lack of detailed guidance resulted in the IRS misplacing hard disks most likely containing taxpayer data and errors in the hardware asset inventory records.

The tape library at the Enterprise Computing Center – Memphis stores the damaged disks until they are eventually shipped to the Enterprise Computing Center – Martinsburg for degaussing. Keeping an inventory of hard disks is problematic because they are not labeled with an inventory barcode, which are affixed to the laptop or desktop shells that initially contained the hard disks. The IRS has established an Asset Sanitization Certification process, which includes procedures for documenting the removal of a hard disk from its computer shell when required. However, we question whether the IRS is consistently following this process because UNS function personnel were unable to find an *Asset Sanitization Certification Form* or a Standard Form 120, *Report of Excess Personal Property*, for our two sampled computers with missing hard disks. The IRS believes that the two computers may have been inadvertently

[6] We selected this sample using a 95 percent confidence interval, 3 percent error rate, and ±3 percent desired precision factor. When projecting the results of our statistical sample, we are 95 percent confident that the actual total number of unsanitized computers is between two and 239.

[7] We selected this sample using a 95 percent confidence interval, 3 percent error rate, and ±3 percent desired precision factor. When projecting the results of our statistical sample, we are 95 percent confident that the actual total number of missing hard disks is between 12 and 310.

placed on the wiped pallet given the IRS's challenging environment of sanitizing the large stockpile of computers that accumulated during the moratorium.

While we acknowledge that resuming hard disk sanitization and establishing the Asset Sanitization Certification process were a huge undertaking, some improvement can be made. We believe that clarification is needed in the draft *MSS Standard Operating Procedures* to allow for better accountability over hard disks throughout the entire MSS sanitization process that are too damaged to wipe or missing from their respective computers.

Smartphone Sanitization

In addition to testing sanitized computers, we reviewed the process the IRS uses to wipe smartphones. MSS personnel enter an incorrect password several times to initiate the wipe. We observed this wiping process and also tested a judgmental sample[8] of eight smartphones and determined that the MSS had effectively sanitized them. To verify the success of the wipes, we observed that the smartphones booted up to the initial setup screens.

The Chief Information Officer should ensure that:

Recommendation 3: Steps are taken to degauss or destroy hard disks identified during this review that were not sanitized or had bad sector errors.

> **Management's Response:** The IRS agreed with this recommendation. The Chief Information Officer will degauss or destroy hard disks identified during this review that were not sanitized or had bad sector errors.

Recommendation 4: Hard disks separated from their computers are properly accounted for throughout the sanitization process.

> **Management's Response:** The IRS agreed with this recommendation. The Chief Information Officer will implement procedures to properly account for hard disks separated from their computers throughout the sanitization process.

Recommendation 5: *MSS Standard Operating Procedures* are clarified to further define accounting for damaged or missing hard disks.

> **Management's Response:** The IRS agreed with this recommendation. The Chief Information Officer will revise the *MSS Standard Operating Procedures* to clarify and further define procedures to account for damaged or missing hard disks.

The Process to Independently Verify the Sanitization of Laptops and Desktops Is Ineffective

After the computers are sanitized, the MSS transfers them to the FMSS function for disposal. At the time of transfer, MSS and FMSS function personnel together visually compare the description of the computers listed on the Standard Form 120 to the bar codes on the pallets of sanitized laptops and desktops. In addition, MSS personnel complete and sign an *Asset*

[8] A judgmental sample is a nonprobability sample, the results of which cannot be used to project to the population.

Sanitization Certification Form to document that the MSS sanitized the computers prior to physical custody of the assets being transferred to the FMSS function.[9]

The UNS function's Asset Sanitization Certification process includes procedures for UNS function personnel to document the independent verification that each individual computer was effectively sanitized. While UNS function management stated that an individual conducting the verification process should boot up the computer to a command level prompt to demonstrate that the computer was sanitized, we did not see this procedure documented in the draft *MSS Standard Operating Procedures* or observe it being performed.

Further, NIST Special Publication 800-88 suggests that the verification process should be performed using a different verification software tool, that is, not simply booting up the computer or reusing the original sanitization tool to perform the verification. The UNS function's verification procedures for computers do not include an effective test of each computer using a verification software tool to verify that the sanitization was effective and that residual data cannot be read.

NIST Special Publication 800-88 also states that effective sanitization techniques are a critical aspect of ensuring that sensitive data are effectively protected by an organization. The goal of sanitization verification is to ensure that the data were effectively sanitized prior to leaving the control of the organization. Specifically, NIST Special Publication 800-88 states:

> *Verifying the selected information sanitization and disposal process is an essential step in maintaining confidentiality. Two types of verification should be considered. The first is verification every time sanitization is applied. The second is a representative sampling verification, applied to a selected subset of the media. If possible, the sampling should be executed by personnel who were not part of the original sanitization action. The goal of sanitization verification is to ensure that the target data was effectively sanitized. A full verification should be performed, if time and external factors permit.*

Further, the *UNS Hardware Asset Management User Guide* (September 2019) states "…verification of the disk wipe will be completed on 100 percent of the assets readied for disposal. The verification ensures that sensitive but unclassified data has been removed prior to equipment transfer to [the] FMSS [function] for final disposal."

UNS function management believed that the MSS met the intent of the sanitization verification guidance through 1) performing the visual inspection of the computers on the sanitized pallets and 2) having a person independent of the sanitization process boot up the computers to a command prompt. However, if the MSS had performed actual verification testing of its sanitized computers using a verification software tool, missing hard disks and hard disks with residual data or bad sector errors would have been identified.[10]

Because the MSS verification process is ineffective, the UNS function cannot ensure that residual taxpayer data or Personally Identifiable Information does not remain on those items disposed

[9] The same process occurs for smartphones, but the visual examination compares the description of smartphones listed on the Form MI, *Miscellaneous Disposal*, to the bar codes of the smartphones in the boxes of sanitized smartphones. MSS personnel then complete and sign an Asset Sanitization Certification Form.

[10] Similar to a sanitized hard disk, bad sector errors can cause computer hard disks to not boot up properly. Without using a verification software tool, sanitized hard disks or ones with bad sector errors potentially containing taxpayer data would be indistinguishable.

outside of the IRS. If an unauthorized disclosure of tax or Personally Identifiable Information occurred, it could result in substantial harm, embarrassment, and loss of public confidence in the IRS. An unauthorized disclosure could also harm an individual.

Recommendation 6: The Chief Information Officer should ensure that hard disk sanitization results are independently verified using an approved verification software tool.

Management's Response: The IRS agreed with this recommendation. The Chief Information Officer will evaluate the Memphis hard disk sanitization process and implement an approved verification tool, as needed, for independently verifying hard disk sanitization results.

Appendix I

Detailed Objective, Scope, and Methodology

The overall objective of this review was to assess the effectiveness of the Information Technology organization's hardware asset sanitization process for laptops, desktops, and smartphones. To accomplish our objective, we:

- Reviewed the UNS function's established sanitization policies and procedures for laptops, desktops, and smartphones.
- Evaluated the sanitization software used by the UNS function for sanitizing laptops and desktops to determine whether it complies with established sanitization standards.
- Used sanitization verification software to evaluate the effectiveness of UNS function sanitization activities. We tested a random interval sample of 87 of 3,882 sanitized laptops and desktops for the existence of residual data. We also tested a judgmental sample[1] of eight of 100 sanitized smartphones for the existence of residual data.

  The Treasury Inspector General for Tax Administration's contracted statistician assisted with developing our sampling plan and projections. We selected the sample using a 95 percent confidence level, a 3 percent expected error rate, and a ±3 percent desired precision factor. We used a random statistical sample because we planned to project to the population of sanitized hard disks.

Performance of This Review

This review was performed at the MSS at the Enterprise Computing Center – Memphis in Memphis, Tennessee, with information obtained from the Brookhaven Depot in Holtsville, New York, during the period November 2020 through June 2021. 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 R. Verneuille, Assistant Inspector General for Audit (Security and Information Technology Services); Bryce Kisler, Director; Carol Taylor, Audit Manager; and Mark Carder, Lead 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: NIST guidance regarding established sanitization standards as well as IRS sanitization policies and procedures. We

[1] A judgmental sample is a nonprobability sample, the results of which cannot be used to project to the population.

evaluated these controls by interviewing MSS and Brookhaven Depot personnel, reviewing relevant documentation, and reviewing a statistical interval sample of sanitized laptops and desktops and a judgmental sample of sanitized smartphones.

Appendix II

Outcome Measures

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

Type and Value of Outcome Measure:

- Taxpayer Privacy and Security – Potential; 45 unsanitized computers (see Recommendation 3).

Methodology Used to Measure the Reported Benefit:

During our audit work, we selected and tested a random statistical sample of sanitized laptops and desktops to determine whether residual data remained on the computers. Specifically, we randomly selected a statistical interval sample of 87 (2.24 percent) computers from a population of 3,882 computers that the MSS sanitized between January and March 2021. Given that one of the 87 computers that we randomly selected had not been sanitized, the error rate of one divided by 87 (1.15 percent) can be multiplied by the sample population of 3,882 sanitized computers. The result of 45[1] represents the number of computers in the sample population of 3,882 that we can statistically estimate were not sanitized properly.

Type and Value of Outcome Measure:

- Reliability of Information – Potential; 89 computers missing hard disks that were not accurately identified in the hardware asset inventory (see Recommendations 4 and 5).

Methodology Used to Measure the Reported Benefit:

Using the same statistical interval sample previously mentioned, we determined that two of the 87 computers that we randomly selected had missing hard disks and were incorrectly tracked as computers in the MSS's hardware asset inventory. The error rate of two divided by 87 (2.30 percent) can be multiplied by the sample population of 3,882 sanitized computers. The result of 89[2] represents the number of computers in the sample population of 3,882 that we can statistically estimate were missing hard disks and were incorrectly tracked as computers in the MSS's hardware asset inventory.

[1] We selected this sample using a 95 percent confidence interval, 3 percent error rate, and ±3 percent desired precision factor. When projecting the results of our statistical sample, we are 95 percent confident that the actual total number of unsanitized computers is between two and 239.

[2] We selected this sample using a 95 percent confidence interval, 3 percent error rate, and ±3 percent desired precision factor. When projecting the results of our statistical sample, we are 95 percent confident that the actual total number of missing hard disks is between 12 and 310.

Appendix III

Management's Response to the Draft Report

CHIEF INFORMATION OFFICER

DEPARTMENT OF THE TREASURY
INTERNAL REVENUE SERVICE
WASHINGTON, DC 20224

September 3, 2021

MEMORANDUM FOR DEPUTY INSPECTOR GENERAL FOR AUDIT

FROM: Nancy A. Sieger
Chief Information Officer

Digitally signed by Nancy A. Sieger
Date: 2021.09.03 07:20:42 -04'00'

SUBJECT: Response to Draft Audit Report Response to Draft Report – Laptop and Desktop Sanitization Practices Need Improvement (Audit #202120013)

Thank you for the opportunity to review and comment on the draft audit report in which TIGTA acknowledges that the IRS has taken actions to improve our control and management of Laptop/Desktop and Smartphone sanitization and disposal practices. The IRS is committed to continuously improving our security procedures and remaining consistent with federal guidance.

The IRS provided information throughout the course of the audit to explain and demonstrate the IRS sanitization process from end-to-end. We appreciate your acknowledgment that most of the sampled laptops and desktops you tested were sanitized. You also observed and recognize that our smartphone sanitization efforts are sufficient and effective. Though you identify several shortcomings and the need for process improvements, you also acknowledge that the IRS already took steps to implement the use of a National Security Agency approved degausser for sanitizing laptops and desktops prior to their disposal outside the IRS. This will help to further ensure our efforts to protect taxpayer data and personal information by adhering to IRM 10.8 and other federal guidance.

In response to your recommendations, we have attached our corrective action plan. We are committed to implementing the corrective actions that will address the findings related to this audit. We agree with the outcome measures and will address them along with the associated recommendations outlined in our corrective action plan. Please note that one or more of the recommendations will be dependent on appropriate funding.

The IRS values the continued support and assistance provided by your office. Should you have any questions, please contact me at 202-317-5000, or a member of your staff may contact Kevin Sturlaugson, Director, Operations Service Support, 681-260-3681.

Attachment

Attachment

Audit# 202120013, *Laptop and Desktop Sanitization Practices Need Improvement*

Recommendations

RECOMMENDATION 1: The Chief Information Officer should ensure that the IRS only uses sanitization products that are approved by the Department of Defense, the Department of Homeland Security, or the National Security Agency.

CORRECTIVE ACTION 1: The IRS agrees with this recommendation. The IRS will purchase and implement sanitization tools and products that are approved by the Department of Defense, the Department of Homeland Security, or the National Security Agency (contingent upon funding).

IMPLEMENTATION DATE: November 15, 2022

RESPONSIBLE OFFICIAL(S): Associate Chief Information Officer, User and Network Services

RECOMMENDATION 2: The Chief Information Officer should ensure that Sanitization equipment and procedures are tested annually to verify that the intended sanitization results are being achieved.

CORRECTIVE ACTION 2: The IRS agrees with this recommendation. The Chief Information Officer will implement annual testing of the Memphis sanitization equipment and procedures to verify that the intended sanitization results are being achieved.

IMPLEMENTATION DATE: November 15, 2022

RESPONSIBLE OFFICIAL(S): Associate Chief Information Officer, User and Network Services

RECOMMENDATION 3: The Chief Information Officer should ensure that steps are taken to degauss or destroy hard disks identified during this review that were not sanitized or had bad sector errors.

CORRECTIVE ACTION 3: The IRS agrees with this recommendation. The Chief Information Officer will degauss or destroy hard disks identified during this TIGTA review, that were not sanitized or had bad sector errors.

IMPLEMENTATION DATE: February 15, 2022

RESPONSIBLE OFFICIAL(S): Associate Chief Information Officer, User and Network Services

RECOMMENDATION 4: The Chief Information Officer should ensure that hard disks separated from their computers are properly accounted for throughout the sanitization process.

CORRECTIVE ACTION 4: The IRS agrees with this recommendation. The Chief Information Officer will implement procedures to properly account for hard disks separated from their computers, throughout the sanitization process.

IMPLEMENTATION DATE: February 15, 2022

RESPONSIBLE OFFICIAL(S): Associate Chief Information Officer, User and Network Services

RECOMMENDATION 5: The Chief Information Officer should ensure that MSS Standard Operating Procedures are clarified to further define accounting for damaged or missing hard disks.

CORRECTIVE ACTION 5: The IRS agrees with this recommendation. The Chief Information Officer will revise the Memphis Sanitization Site Standard Operating Procedures to clarify and further define procedures to account for damaged or missing hard disks.

IMPLEMENTATION DATE: February 15, 2022

RESPONSIBLE OFFICIAL(S): Associate Chief Information Officer, User and Network Services

RECOMMENDATION 6: The Chief Information Officer should ensure that hard disk sanitization results are independently verified using an approved verification software tool.

CORRECTIVE ACTION 6: The IRS agrees with the above recommendation. The Chief Information Officer will evaluate the Memphis hard disk sanitization process and implement an approved verification tool, as needed, for independently verifying hard disk sanitization results.

IMPLEMENTATION DATE: November 15, 2022

RESPONSIBLE OFFICIAL(S): Associate Chief Information Officer, User and Network Services

Appendix IV

Glossary of Terms

Term	Definition
Common Criteria	Provides assurance that the process of specification, implementation, and evaluation of a computer security product has been conducted in a rigorous, standard, and repeatable manner at a level that corresponds with its target use environment. Once the vendor completes this process, the product achieves Common Criteria certification.
Enterprise Standards Profile	The authoritative repository for IRS-approved products and standards. The Enterprise Standards Profile allows project owners and other stakeholders to select preapproved technology products and standards. Development teams should determine which standards and approved products apply to their areas of responsibility. Listings in the Enterprise Standards Profile include guidance for usage that should be reviewed for useful, relevant information.
Federal Information Processing Standards Publication 199	Standards for categorizing information and information systems; establishes security categories for both information and information systems. The security categories are based on the potential impact on an organization should certain events occur that jeopardize the information and information systems.
First In, First Out Rotation	An inventory valuation method in which the assets acquired first are disposed of first.
Hardware	The physical parts of a computer and related devices; it includes motherboards, hard disks, monitors, keyboards, mice, printers, and scanners.
Information Technology Organization	The IRS organization responsible for delivering information technology services and solutions that drive effective tax administration to ensure public confidence.
Media	Physical devices or writing surfaces, including but not limited to magnetic tapes, optical disks, magnetic disks, large-scale integration memory chips, and printouts onto which information is recorded, stored, or printed within an information system.
Personal Identity and Authentication Information	Information necessary to ensure that all persons who are potentially entitled to receive any Federal benefit are identified so that Federal agencies can have reasonable assurance that they are paying or communicating with the right individuals. This information includes an individual's Social Security Number, name, date of birth, place of birth, and parents' names.
Personally Identifiable Information	Information that can be used to distinguish or trace an individual's identity, such as 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 of birth, place of birth, and mother's maiden name.

Purging	Applies physical or logical techniques that render target data recovery infeasible using state of the art laboratory techniques.
Sector	The smallest physical storage unit on a hard disk, which is 512 bytes in size.
Security Categories	Security categories are based on the potential impact on an organization should certain events occur. The potential impact could jeopardize the information and information systems needed by the organization to accomplish its assigned mission, protect its assets, fulfill its legal responsibilities, maintain its day-to-day functions, and protect individuals. Security categories are to be used in conjunction with vulnerability and threat information in assessing the risk to an organization.
Sensitive But Unclassified	Any information that requires protection due to the risk and magnitude of loss or harm to the IRS or the privacy to which individuals are entitled under the Privacy Act,[1] which could result from inadvertent or deliberate disclosure, alteration, or destruction.
Taxation Management Information	Information that includes activities associated with the implementation of the Internal Revenue Code and the collection of taxes in the United States and abroad.
User and Network Services Function	Within the Information Technology organization, this function supplies and maintains all desk-side (including telephone) technology, provides workstation software standardization and security management, inventories data processing equipment, conducts annual certification of assets, and provides other services.

[1] 5 U.S.C. § 552a.

Appendix V

Abbreviations

FMSS	Facilities Management and Security Services
IRS	Internal Revenue Service
MSS	Memphis Sanitization Site
NIST	National Institute of Standards and Technology
UNS	User and Network Services

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.