DEPARTMENT OF JUSTICE | OFFICE OF THE INSPECTOR GENERAL

MANAGEMENT ADVISORY MEMORANDUM

24-093

AUGUST 2024

Notification of Concerns Identified in the Federal Bureau of Investigation's Inventory Management and Disposition Procedures of Electronic Storage Media

AUDIT DIVISION

August 21, 2024

Management Advisory Memorandum

To: Christopher Wray
Director
Federal Bureau of Investigation

From: Michael E. Horowitz
Inspector General

Subject: Management Advisory Memorandum - Notification of Concerns Identified in the Federal Bureau of Investigation's Inventory Management and Disposition Procedures of Electronic Storage Media

---

The purpose of this memorandum is to advise you of concerns that we identified during an ongoing audit of a Federal Bureau of Investigation (FBI) contract. During this contract audit, we identified significant weaknesses related to the FBI's inventory management and disposition procedures for its electronic storage media containing sensitive but unclassified (SBU) information, such as law enforcement sensitive information, as well as classified national security information (NSI).[1] We also identified concerns regarding the physical security over these items at an FBI-controlled facility where the media destruction takes place (Facility).[2] While these concerns are outside the objectives of our ongoing contract audit, we believe they are significant enough to warrant the FBI's immediate attention and action to better safeguard electronic storage media containing SBU or classified NSI.

Specifically, our concerns are that the FBI:

- does not have adequate policies and procedures or controls to account for electronic storage media extracted from larger devices and thumb drives;
- does not label its electronic storage media with the appropriate NSI classification or SBU levels; and
- needs to improve the internal physical access and security controls in relevant areas at the Facility.

---

[1] Contractors performing the sanitization and destruction of disposed assets have access to protected information and/or information systems. "Protected information" includes classified information; Foreign Intelligence Surveillance Act information; and Sensitive but Unclassified information, including Law Enforcement Sensitive, personally identifiable information, business proprietary information, and any other information that is non-public and/or protected from disclosure by law or policy.

[2] Due to the asset accountability gaps and internal physical access issues identified within this memorandum, the name and location of the Facility is kept undisclosed.

The Office of the Inspector General (OIG) makes three recommendations for the FBI to address these concerns.

The FBI's Program for Disposition of Electronic Storage Media

The FBI's Asset Management Unit (AMU) utilizes contracts and contractor personnel to process at a central location the collection, sanitization, destruction, and disposal of electronic media from across the FBI.[3] As of June 2024, AMU receives assets from FBI headquarters, FBI offices around the National Capital Region, and 36 FBI field offices from across the United States and Puerto Rico. According to AMU personnel, the FBI field offices and divisions that do not utilize AMU's destruction services may excess and destroy media using their own vendors. AMU's Property Turn-in Team (PTI) performs the intake of media while AMU's Media Destruction Team (MDT) performs the sanitization and destruction of media. The electronic media that is received and processed for destruction includes, but is not limited to, desktop computers, laptops, servers, hard drives, USB drives, CDs, DVDs, smartphones, and other portable electronic devices. Given the sensitivity of the information contained on these devices, the contract requires all memory components to be treated as though they contain SBU or classified NSI.

Intake

There are two locations for the intake of electronic media, PTI's office at the FBI's J. Edgar Hoover headquarters building in Washington, D.C., and at the Facility. Media received at FBI headquarters are transferred to the Facility while FBI field offices utilizing AMU's destruction services ship their electronic media directly to the Facility. Upon receipt, PTI assumes custody of the media and places the items into pallet-sized boxes, which are stored awaiting MDT's sanitization and destruction.

Media Destruction

According to AMU, the MDT sanitizes and destroys electronic media in order of priority. Specifically, capitalized assets valued at over $100,000, assets used in concealments and special cases, and assets containing Top Secret information are the highest priorities. This is followed by other accountable electronic media, such as laptops, printers, fax machines, televisions, and digital cameras, which are processed based on a first-in-first-out method. Other non-accountable property, such as answering machines, shredders, and other bulky items are processed daily by two designated MDT personnel. Finally, other non-accountable property, such as extracted internal hard drives are processed last. The MDT disassembles electronic media, stores similar components together, and then sanitizes electronic media components using a degausser, shredder, and disintegrator. The sanitized components are stored in large pallet-sized boxes. MDT stated that once a component-specific pallet box is full, it will make arrangements to have the pallets picked up and shipped to be recycled, smelted or incinerated, or reused, depending on the raw materials.

FBI Must Properly Account for and Mark Its Electronic Storage Media Prior to Submission for Destruction

Our audit found that the FBI is not properly securing classified NSI or SBU information and is neither marking all electronic storage media as required, nor accounting for this media consistent with FBI internal policies and Department of Justice (DOJ) guidance. The lack of accountability of this electronic storage

[3] AMU is responsible for oversight of all FBI-owned or FBI-leased accountable property. AMU oversees the disposition and destruction of assets that are determined to be obsolete, defective, unserviceable, or no longer needed and is required to do so in accordance with National Security Administration standards, National Institute of Standards and Technology guidelines, and DOJ security requirements.

media is compounded by inadequate internal physical access and security controls at the Facility, potentially placing these media at risk of loss or theft without the possibility of detection.

Electronic Storage Media Containing SBU Information or Classified NSI Should be Tracked

During our audit, we observed that the FBI does not always account for its loose electronic storage media received from FBI offices such as computer hard drives, thumb drives, floppy disks, and server drives. FBI personnel affix property asset labels to the chassis of computers and servers, but not on the internal electronic storage media, such as the hard drive, which may contain sensitive data. The FBI confirmed that the chassis with the property label affixed is tracked within the Asset Management System (AMS) and the electronic storage media extracted from within is not tracked.

During our observations of PTI's receiving process, we found shipments were received of non-accountable media from FBI field offices that included hard drives that were extracted from computers and servers, as well as other media storage devices stored individually or in boxes on the floor of the Facility. The media we observed did not always include property labels. The PTI staff explained that although field offices may affix the original assets' property numbers on the media extracted from computers, PTI would include the media in the non-accountable pallet and do not track these media individually in AMS because they are considered non-accountable assets. Furthermore, the PTI supervisor explained that the field offices may not identify the number of internal hard drives they shipped. As a result, PTI is unable to verify that the quantities received are the same quantities shipped. We additionally observed that computers and servers were sometimes received without any internal hard drives, and PTI personnel confirmed that they would not question why a computer is missing a hard drive. The PTI personnel further explained that PTI tracks external or removable hard drives, but they do not track extracted internal hard drives. Thus, according to the FBI, when an unclassified computer or computer that may have processed Secret information is missing the hard drive, the PTI staff processes the computer "as is" without the hard drive. For computers that processed Top Secret information, FBI staff are required to remove the electronic storage media to be couriered through Defense Courier Services separately to save shipping cost. In doing so, as with Secret internal hard drives, these extracted Top Secret storage media do not bear property labels and are not individually accounted for in AMS.

We believe that the FBI's practice of not accounting for extracted internal hard drives, thumb drives, and other media devices is not consistent with FBI or DOJ policies to ensure accountability of media containing sensitive or classified information. When we informed FBI officials of our concerns, the FBI affirmed that it views hard drives as accountable assets, albeit when the hard drives are extracted from the computer chassis, the property number remains only with the computer chassis. The FBI explained that extracted internal hard drives are not currently tracked in AMS because under FBI best practices, hard drives are removed by MDT to be degaussed. However, the FBI confirmed that not all hard drives, particularly hard drives extracted by local FBI field office IT specialists and shipped from field offices, are being handled in accordance with this best practice.

The FBI's Personal Property Management Policy Guide (1226PG) makes a distinction between an internal hard drive and a removable hard drive. The policy only requires accountability of removable hard drives and does not require accountability of internal hard drives, as they are defined as expendable assets with normal life expectancy of less than 2 years. However, FBI policy also does not discuss the handling of thumb drives and other electronic storage devices, which are explicitly required to be accounted for under

DOJ Policy Statement 1600.02.[4] Additionally, the FBI's Removable Electronic Storage Media Protection (0247D) policy requires reporting of media that are lost, stolen, or used in violation of FBI policy directives. This policy defines removable electronic storage as portable, electronic storage media, such as magnetic, optical, and solid-state devices, that can be inserted into and extracted from a computing device and that is used to store and transfer text, video, audio, and image information. Such devices have no independent processing capability and include hard disks, floppy disks, zip drives, compact disks, thumb drives, and similar USB storage devices.

Once the internal electronic storage media is extracted from the computer chassis and no longer a component of the larger accountable asset, the extracted drive, containing the data and information, essentially becomes a standalone asset. Thus, the FBI should ensure that extracted internal hard drives, thumb drives, and other electronic storage media are tracked to ensure accountability of media containing sensitive or classified information as well as to ensure the ability to report media that are lost, stolen, or used in violation of FBI policy directives. In response to our concerns, the FBI told us that it will assess the tracking of hard drives that have been extracted from computers by the respective hard drive serial number. The FBI also stated that it will require FBI field offices or divisions to enter the hard drive and storage media extracted from the computer into AMS, documenting the serial number, prior to shipping it to PTI. The FBI stated that this process will ensure hard drives are tracked from the point of leaving a field office through the AMU PTI and destruction process. Regarding thumb drives, the FBI stated that PTI requires offices to enter thumb drives into AMS prior to sending them to PTI for destruction. For all other thumb drives, (i.e., those not going through PTI) the FBI stated that it is in the process of assessing its policies and procedures for ensuring they are appropriately tracked in AMS.

Thus, we recommend that the FBI revise its procedures to ensure all electronic storage media containing sensitive or classified information, including internal hard drives that are extracted from computers slated for destruction, are appropriately accounted for, tracked, timely sanitized, and destroyed.

Electronic Storage Media Extracted from Larger Components Should be Marked with the Appropriate Classification

FBI policy requires storage media extracted from the large components to have classification labels affixed at the time of deinstallation. According to an AMU personnel, the FBI affixes classification labels on the chassis of a computer or server, but not on the internal electronic storage media. Further, when extracting internal electronic media for disposal, we found that the FBI does not mark the media to identify the level of classification of the information contained on the storage device. Additionally, we found that the FBI does not label small media flash drives to identify its classification. These practices are not in accordance with FBI and DOJ policies, as shown in Table 1.

[4] The DOJ Policy Statement 1600.02, approved in August 2022 and updated in March 2023, requires all DOJ components to manage physical inventories of all government-controlled accountable personal property and to establish physical controls for securing and safeguarding vulnerable assets. These assets include all inherently portable information technology equipment with memory capability and storage media such as CDs, DVDs, USB flash drives, and external hard drives that hold sensitive data.

Table 1

Certain FBI and DOJ Policies and Regulations on Marking NSI

Document Title	Applicable Policy
FBI's External Security Marking of Information Technology Hardware and Electronic Data Storage Policy Directive (0636D) – FBI Security Division, August 2013	All information system components (e.g., rack-mount chassis, workstations, laptops, servers, attached storage devices, portable electronic devices) with fixed electronic data storage media (e.g., memory and hard drives) must display classification labels on the unit/equipment/device that contain the storage media. All fixed electronic data storage media removed from the information system must be marked with a label at the time of removal. When the size or the material of the removable storage media does not allow for a complete label (e.g. small media flash drive), the media must be marked with as much of a classification label as practical, or marked with a color corresponding to the classification. Chief Security Officers must ensure that electronic data storage media for all systems are labeled to identify the classification level, compartments, and dissemination and handling controls for information systems under their cognizance.
DOJ Security Program Operating Manual – DOJ Justice Management Division Security and Emergency Planning Staff, December 2010	Classified computer media such as USB sticks, hard drives, CD ROMs, and diskettes shall be marked to indicate the highest overall classification of the information contained within the media.

Sources: The FBI and DOJ

Thus, we recommend that the FBI implement controls to ensure its electronic storage media are marked with the appropriate NSI classification level markings, in accordance with applicable policies and guidelines.

The FBI Needs to Physically Secure the Electronic Storage Media Slated for Disposal

We found that the FBI does not have sufficient internal physical security of the media turned in for disposal at the Facility we visited. Coupled with FBI's practice of not accounting for the extracted internal hard drives, thumb drives, and disk drives containing information of varying classification levels, the lack of adequate physical security at the Facility increases the risk of classified information being compromised. As shown in Figure 1, during our site visit to the Facility in October 2023, we observed that PTI maintained in its working space an open pallet-sized box of extracted electronic storage media, specifically hard drives and solid-state drives. The pallet we observed was marked "NON-ACCOUNTABLE" and contained electronic media without any marking or label, as well as media marked unclassified and Secret. A PTI staff member told us that the pallet for the loose media was unsecured for extended periods, sometimes spanning days or even weeks because PTI would wrap the pallets and move them to the Facility shelves only when the box reached full capacity.

Figure 1

Large Open Box of Non-accountable Media in the Property Turn-in Area

Source: OIG, date October 23, 2023 (OIG removed commercial brand names in the photo)

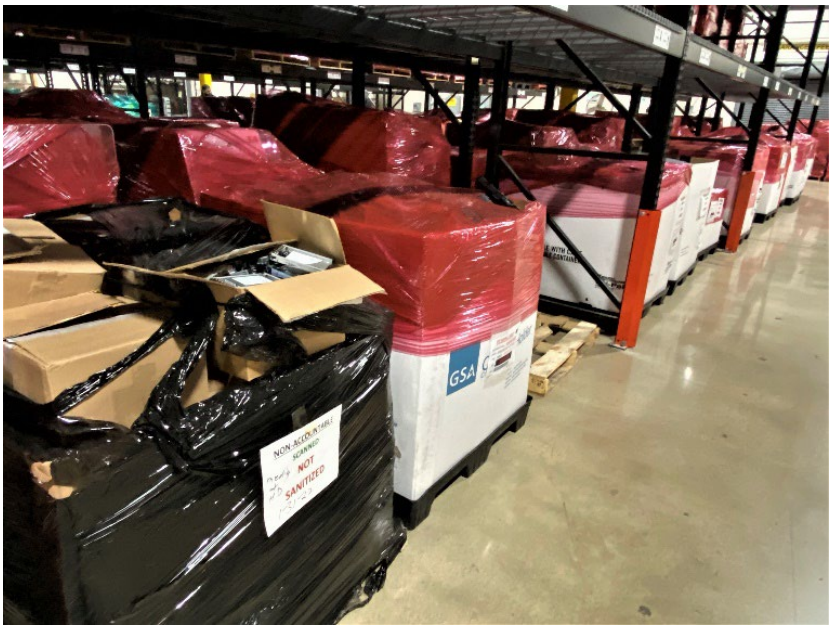
Figure 2

Pallet with Open (or Broken) Wrapping in the Facility Shelving Area

View 1 – Electronic storage media exposed

Source: OIG, date October 23, 2023

View 2 – Compromised pallet in the open aisles of the Facility



Source: OIG, date October 23, 2023

As shown in Figure 2, during the same site visit we also observed, on the floor of the Facility storage area, a container with a label dated January 2022 that identified its contents as "non-accountable." Notably, the container's shrink wrapping was torn, and boxes inside were visibly open and contained hard drives marked Secret. We brought this to the attention of FBI personnel and the pallet was promptly secured with additional shrink wrap. AMU considers extracted electronic storage media as non-accountable assets and stores them in specific pallets of extracted media. Because AMU does not prioritize destruction of non-accountable assets, pallets of hard drives are shelved for an extended period (up to 21 months based on our observation) before destruction. The FBI PTI supervisor and contractor confirmed that they would not be aware if someone was to take hard drives from the pallets because these assets are not counted or otherwise tracked.

The Facility is shared with other FBI operations, such as logistics, mail, and information technology equipment fulfilment. Based on an access list the FBI provided in May 2024, there were 395 persons with active access to the Facility, which included 28 task force officers and 63 contractors from at least 17 companies. There is no physical barrier preventing FBI and non-FBI personnel and contractors from other Facility operations from accessing PTI's work area and the pallets of unsanitized assets in the Facility shelving space. Although there is a metal roll-up door to the MDT's work area as seen in Figure 3, the FBI supervisor and MDT contractor did not explain why they do not lower the closure to secure the space at the end of the day to prevent non-AMU personnel access to the media sanitization and destruction areas. Compounding this issue is the non-functioning camera in Figure 3 and the absence of camera coverage in other relevant areas, which further hinders the FBI's ability to monitor and address any security incidents or inventory discrepancies.

Figure 3

Metal Roll-Up Door to the MDT's Workspace and Non-functioning Camera

Source: OIG, date October 23, 2023

In response to our concerns, the FBI stated that the Facility was operating as an open storage secure area for classified material up to the Secret classification level, specifically including fixed magnetic media (hard drives).[5] We requested evidence of the open storage accreditation and determined that an interim accreditation was granted in 2015 but had expired in March 2016. Following our observations, the FBI performed a site visit in November 2023 to confirm the remediation of the security enhancements required from a 2015 open storage inspection checklist. The FBI granted the Facility its final open storage accreditation in January 2024. The FBI stated that the lack of final accreditation was an administrative oversight and that enhancements had been completed in the interim. However, the FBI could not provide evidence of when the required enhancements were completed.

Further, according to the FBI, its internal policy on the Destruction of Classified and Sensitive Material did not specify timeframes for destruction. Thus, the FBI stated that AMU's practice of storing the pallets of hard drives on the Facility floor does not violate its internal policies and that the Facility had received accreditation for open storage of fixed magnetic media. However, as we discussed, the FBI accreditation for open storage was only officially granted in January 2024. According to the FBI's Construction and Approval

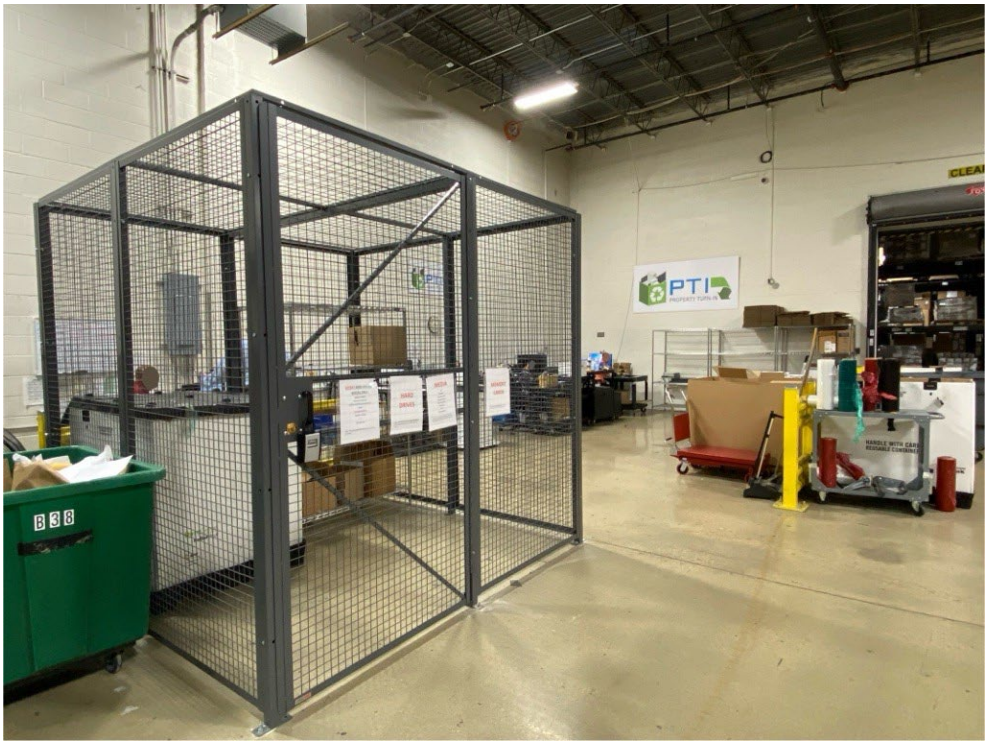
[5] An open-storage secure area is a space with reinforced construction in which classified materials, up to and including at the Secret collateral level, may be stored outside of GSA-approved security containers.

of Open-Storage Secure Areas, Closed-Storage Secure Areas, and Controlled Unclassified Areas Policy Guide (1264PG), FBI personnel must maintain a clean desk policy within open-storage secure areas and take all measures to respect the need-to-know requirement for access to classified information. The policy continues to state that to ensure a clean desk, FBI personnel must store classified material at the end of the day in closed containers (e.g., desks or file cabinets).

FBI personnel stated that to better secure the electronic storage media, PTI will store unsanitized and unwrapped hard drives and solid-state drives in a secure cage until the pallet is filled and ready for wrapping. Figure 4 shows the cage the FBI installed in PTI's workspace to secure media that it receives.

Figure 4

Cage Installed in PTI Workspace to Secure Media



Source: OIG, date February 28, 2024 (OIG obscured the faces of FBI personnel in the photo)

Finally, the FBI also stated in December 2023 that it is in the process of installing a new camera system at the Facility. However, during our follow-up visit to the Facility in February 2024, FBI personnel stated that the installation of the new camera system had not been completed. The FBI explained in June 2024 that it is actively working on obtaining a waiver for it to install a video surveillance system. We believe that the combination of the FBI's lack of accountability of the electronic storage media, lack of internal physical access control, and lack of sufficient video surveillance compounds the risk of media, potentially with sensitive and classified information, being lost or stolen without detection. We recommend that the FBI strengthen the controls and practices for the physical security of its electronic storage media at the Facility to prevent loss or theft.

Conclusion

The lack of inventory controls over the FBI's electronic storage media increases the FBI's risks of having thumb drives, disk drives, and hard drives or solid-state drives lost or stolen after they have been extracted from the larger electronic component, such as a laptop or a server. Also, the FBI does not mark these electronic media to identify the level of classification of the information contained in the storage device. The lack of accountability over these media, as well as the lack of internal physical access control and adequate camera coverage at relevant areas at the Facility, unnecessarily places electronic storage media at risk of loss or theft without possibility of detection.

Although our related audit of the FBI's contract is ongoing, we are providing this memorandum to the FBI now so that it may promptly act to ensure its electronic storage media is properly accounted for, appropriately marked, and adequately safeguarded to avoid any loss.

Recommendations

We recommend that the FBI:

1. Revise its procedures to ensure all electronic storage media containing sensitive or classified information, including hard drives that are extracted from computers slated for destruction, are appropriately accounted for, tracked, timely sanitized, and destroyed.

2. Implement controls to ensure its electronic storage media are marked with the appropriate NSI classification level markings, in accordance with applicable policies and guidelines.

3. Strengthen the control and practices for the physical security of its electronic storage media at the Facility to prevent loss or theft.

The OIG provided a draft of this memorandum to the FBI and the FBI's response is incorporated as Appendix 1. Appendix 2 provided the OIG's analysis of the FBI's response and a summary of the action necessary to close the recommendation in this memorandum. The OIG requests that the FBI provide an update on the status of its response to the recommendation within 90 days of the issuance of this memorandum. If you have any questions or would like to discuss the information in this memorandum, please contact me at (202) 514-3435 or Jason R. Malmstrom, Assistant Inspector General for Audit, at (202) 616-4633.

cc: Thomas G. Seiler
Section Chief
External Analysis and Evaluation Section
Inspection Division
Federal Bureau of Investigation

Jonathan F. Lenzner
Chief of Staff
Federal Bureau of Investigation

William M. Miller
Deputy Chief of Staff
Federal Bureau of Investigation

Jay Greenberg
Assistant Director
Inspection Division
Federal Bureau of Investigation

P.J. O'Brien
Deputy Assistant Director
Inspection Division
Federal Bureau of Investigation

Danielle Washington
Acting Unit Chief, External Analysis Unit
Inspection Division
Federal Bureau of Investigation

Louise Duhamel
Assistant Director, Audit Liaison Group
Internal Review and Evaluation Office
Justice Management Division

Bradley Weinsheimer
Associate Deputy Attorney General

Mitchell Reich
Chief of Staff and Deputy Associate Attorney General
Office of the Associate Attorney General

Dahlia Mignouna
Deputy Chief of Staff
Office of the Associate Attorney General

APPENDIX 1: THE FEDERAL BUREAU OF INVESTIGATION'S RESPONSE TO THE DRAFT MANAGEMENT ADVISORY MEMORANDUM

U.S. Department of Justice

Federal Bureau of Investigation

Washington, D. C. 20535-0001

August 6, 2024

The Honorable Michael E. Horowitz
Inspector General
Office of the Inspector General
U.S. Department of Justice
950 Pennsylvania Avenue, N.W.
Washington, DC 20530

Dear Mr. Horowitz:

The Federal Bureau of Investigation (FBI) appreciates the opportunity to review and respond to your office's report entitled, Audit of The FBI's Media Destruction Services Contract Awarded to Articus Solutions, LLC.

We look forward to working with the Office of the Inspector General to address the concerns and recommendations provided in the report. The FBI recognizes the importance of addressing the immediate concerns regarding inventory management and disposition procedures of electronic storage media. The FBI will take corrective action and make necessary improvements. We appreciate your feedback as we continue this effort.

Should you have any questions, feel free to contact me. We greatly appreciate the professionalism of your audit staff throughout this matter.

Sincerely,

J. William Rivers
Assistant Director
Security Division

Department of Justice (DOJ) Office of the Inspector General (OIG)
FBI's Media Destruction Audit
Amended Draft Management Advisory Memo (MAM) Review and Recommendation Response

Recommendation 1. Revise its procedures to ensure all electronic storage media containing sensitive or classified information, including hard drives that are extracted from computers slated for destruction, are appropriately accounted for, tracked, timely sanitized, and destroyed.

FBI Response: Concur. Security Division (SecD), Finance and Facilities Division (FFD), Office of the Chief Information Officer (OCIO), and other technical security stakeholders created the *Physical Control and Destruction of Classified and Sensitive Electronic Devices and Material Policy Directive,* which will require marking and accountability as envisioned in the DOJ review. The policy is in the final editing stage in the FBI's Internal Policy Office.

Recommendation 2. Implement controls to ensure its electronic storage media are marked with the appropriate NSI classification level markings, in accordance with applicable policies and guidelines.

FBI Response: Concur. SecD, FFD, OCIO, and other technical security stakeholders created the *Physical Control and Destruction of Classified and Sensitive Electronic Devices and Material Policy Directive,* which will require marking and accountability as envisioned in the DOJ review. The policy is in the final editing stage in the FBI's Internal Policy Office.

Recommendation 3. Strengthen the control and practices for the physical security of its electronic storage media at the Facility to prevent loss or theft.

FBI Response: Concur. SecD has coordinated with FFD for the installation of "cages" to provide positive control, as well as the coordination of a waiver to permit specific video security system coverage of the "cages" and other sensitive areas (as appropriate).

APPENDIX 2: OFFICE OF THE INSPECTOR GENERAL ANALYSIS AND SUMMARY OF ACTIONS NECESSARY TO CLOSE THE RECOMMENDATIONS

The Office of the Inspector General (OIG) provided a draft of this memorandum to the Federal Bureau of Investigation (FBI). The FBI's response is incorporated as Appendix 1 of this final memorandum. The FBI concurred with each of the recommendations and, as a result, the recommendations are resolved. The following discussion provides the OIG analysis of the FBI's response and a summary of the actions necessary to close the recommendations. The OIG requests that the FBI provide an update on the status of its response to the recommendations within 90 days of the issuance of this memorandum.

Recommendations for the FBI:

1. **Revise its procedures to ensure all electronic storage media containing sensitive or classified information, including hard drives that are extracted from computers slated for destruction, are appropriately accounted for, tracked, timely sanitized, and destroyed.**

   Resolved. The FBI concurred with our recommendation and stated in its response that the Security Division (SecD), Finance and Facilities Division (FFD), Office of the Chief Information Officer (OCIO), and other technical security stakeholders created the Physical Control and Destruction of Classified and Sensitive Electronic Devices and Material Policy Directive, which will require marking and accountability. The FBI stated that this policy is in the final editing stage in the FBI's Internal Policy Office.

   This recommendation can be closed when we receive evidence that the FBI has revised its procedures to ensure all electronic storage media containing sensitive or classified information, including hard drives that are extracted from computers slated for destruction, are appropriately accounted for, tracked, timely sanitized, and destroyed.

2. **Implement controls to ensure its electronic storage media are marked with the appropriate National Security Information (NSI) classification level markings, in accordance with applicable policies and guidelines.**

   Resolved. The FBI concurred with our recommendation and stated that SecD, FFD, OCIO, and other technical security stakeholders created the Physical Control and Destruction of Classified and Sensitive Electronic Devices and Material Policy Directive, which will require marking and accountability. The FBI stated that this policy is in the final editing stage in the FBI's Internal Policy Office.

   This recommendation can be closed when we receive evidence that the FBI has implemented controls to ensure its electronic storage media are marked with the appropriate NSI classification level markings, in accordance with applicable policies and guidelines.

3. **Strengthen the control and practices for the physical security of its electronic storage media at the Facility to prevent loss or theft.**

   Resolved. The FBI concurred with our recommendation and stated that SecD has coordinated with FFD for the installation of "cages" to provide positive control, as well as the coordination of a waiver to permit specific video security system coverage of the "cages" and other sensitive areas, as appropriate.

   This recommendation can be closed when we receive evidence that the FBI has strengthened the control and practices for the physical security of its electronic storage media at the Facility to prevent loss and theft.