Federal Housing Finance Agency
Office of Inspector General

FHFA Cannot Assure that All Electronic Media Approved for Destruction in October 2018 Was Destroyed, and it Continues to Lack Adequate Controls over Electronic Media Targeted for Disposal

Audit Report • AUD-2020-009 • March 30, 2020

AUD-2020-009

March 30, 2020

Executive Summary

The Federal Housing Finance Agency (FHFA or Agency), established by the Housing and Economic Recovery Act of 2008, is responsible for the supervision, regulation, and housing mission oversight of Fannie Mae and Freddie Mac (together, the Enterprises), and the Federal Home Loan Bank System (FHLBanks) (collectively, the regulated entities), and the FHLBanks' fiscal agent, the Office of Finance. Since 2008, FHFA has served as conservator of the Enterprises.

FHFA information is generally stored on different types of electronic media, such as hard disk drives and mobile devices. If the electronic media fails or when the system to which it is connected reaches the end of its service life, the media is disposed. When electronic media is disposed, FHFA has policies and procedures for employees to follow to protect the stored Agency information. In October 2018, FHFA's Chief Information Officer (CIO) approved a staff recommendation to destroy electronic media that had accumulated over 19 years. To carry out this destruction, FHFA amended a contract for paper shredding to include the shredding of electronic media and transferred electronic media to the contractor for shredding in January 2019.

We performed this audit to determine FHFA's controls over the disposal of electronic media and assess whether those controls were operating effectively.

We found that FHFA lacked meaningful controls over electronic media approved for shredding in October 2018 and collected by its contractor in January 2019. First, it failed to maintain accountability over the electronic media approved for shredding in October 2018 and transferred to its contractor in January 2019. FHFA provided to us five unreconciled counts of the electronic media approved for disposal and was unable to report the actual number of laptop and server hard drives, tapes, iPhones, and BlackBerrys collected for disposal by its contractor.

Second, we determined that FHFA failed to follow its existing procedures which required: (1) the hard drives and tapes scheduled for disposal to be degaussed (a method of purging data) and (2) some number of the iPhones scheduled for disposal to be "wiped" (returned to a factory setting with all data removed). In the event that some volume of this electronic media was not destroyed by the contractor, FHFA's failure to sanitize this media created the risk that FHFA data could be exposed.

According to FHFA, further disposal of equipment targeted for destruction is suspended until it revises its current procedures. We found that FHFA's current procedures were deficient because they did not require hard drives

AUD-2020-009

March 30, 2020

removed from computers to be accounted for because such hard drives were not included in regular physical inventories nor recorded in and reconciled to the information in its system of record used to account for computers.

We make one recommendation to address the shortcomings in the Agency's controls over its disposition of electronic media. In a written response, FHFA agreed with our recommendation.

This report was prepared by Jackie Dang, Audit Director; Dan Jensen, Auditor-in-Charge; and with assistance from Bob Taylor, Senior Advisor. We appreciate the cooperation of FHFA staff, as well as the assistance of all those who contributed to the preparation of this report.

This report has been distributed to Congress, the Office of Management and Budget, and others and will be posted on our website, www.fhfaoig.gov and www.oversight.gov.

Marla A. Freedman, Deputy Inspector General for Audits /s/

TABLE OF CONTENTS

ABBREVIATIONS

CIO	Chief Information Officer
CMDB	Configuration Management Database
CTO	Chief Technology Officer
FHFA or Agency	Federal Housing Finance Agency
FISMA	Federal Information Security Modernization Act of 2014
GAO	Government Accountability Office
Green Book	GAO-14-704G, *Standards for Internal Control in the Federal Government*
HD	Hard drives
NIST	National Institute of Standards and Technology
NIST SP 800-88	NIST Special Publication, Revision 1, *Guidelines for Media Sanitization*
OIG	Federal Housing Finance Agency Office of Inspector General
OGC	Federal Housing Finance Agency Office of General Counsel
OTIM	Federal Housing Finance Agency Office of Technology and Information Management
RAID	Redundant Array of Independent Disks

BACKGROUND

FHFA's Network and Systems

FHFA's network and systems process and host data and information such as financial reports, data from the Enterprises, examinations and analyses of the regulated entities, and personally identifiable information of employees. The Office of Technology and Information Management (OTIM), within FHFA, works with its mission and support offices to promote the effective and secure use of information and systems. FHFA has determined that the potential impact to the Agency and individuals if there is a security breach of its information and information systems is *moderate*.[1]

FHFA information is generally stored on different types of electronic media, such as: hard disk drives (both magnetic and solid state), removable media drives (e.g., Universal Serial Bus, optical media, etc.), mobile devices (e.g., iPhones, iPads, tablets, BlackBerrys, etc.), and tape drives. If the electronic media fails or when the system to which it is connected reaches the end of its service life, the media is disposed. Similarly, when systems are reallocated, such as reassigning a workstation or mobile device to a different user, old data on the associated electronic media must be removed prior to reassignment/reuse. When electronic media is disposed of or reused, FHFA has policies and procedures for employees to follow to protect the stored Agency information.

Standards for Electronic Media Disposal

The Federal Information Security Modernization Act of 2014 (FISMA) requires agencies, including FHFA, to develop, document, and implement agency-wide programs to provide information security for the information and information systems that support the operations and assets of the agency. Pursuant to FISMA, the National Institute of Standards and Technology (NIST) is responsible for developing information security standards and guidelines, including minimum requirements for federal information systems.

---

[1] The National Institute of Standards and Technology's Federal Information Processing Standards Publication 199, *Standards for Security Categorization of Federal Information and Information Systems* (Feb. 2004) establishes three security categories of potential impact for information and information systems: *low*, *moderate*, and *high*. The potential impact is *moderate* if the loss of confidentiality, integrity, or availability of the information or information system could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals. According to this publication, a serious adverse effect means that, for example, the loss of confidentiality, integrity, or availability might: (i) cause a significant degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is significantly reduced; (ii) result in significant damage to organizational assets; (iii) result in significant financial loss; or (iv) result in significant harm to individuals that does not involve loss of life or serious life threatening injuries.

NIST Special Publication 800-88, Revision 1, *Guidelines for Media Sanitization* (NIST SP 800-88), charges organizations with properly safeguarding used electronic media because NIST has concluded that improperly sanitized electronic media is an "often rich source of illicit information collection." NIST lists three methods to sanitize electronic media: clearing (e.g., overwriting sensitive information with non-sensitive data or resetting the device to the factory state), purging (e.g., applying a large magnetic force to magnetic media), and destroying (e.g., shredding the media). NIST SP 800-88 places the responsibility for ensuring that organizational sanitization requirements meet its guidelines on an agency's Chief Information Officer. Agencies are also required by the Government Accountability Office's (GAO) *Standards for Internal Control in the Federal Government* (the Green Book) to establish physical control over vulnerable assets.[2] According to the Green Book, an example of a physical control to secure and safeguard vulnerable assets is security for and limited access to the assets. Additionally, management should periodically count and compare such assets to control records.

FHFA's media disposal policies and procedures are found in its Information Security Media Sanitization Procedures and Property Management Standard Operating Procedure.

In October 2018, FHFA's Chief Information Officer Authorized the Disposal/ Destruction of Electronic Media that Had Accumulated over 19 Years at FHFA and its Predecessor Agencies

In 2012, FHFA consolidated its headquarters operations into a single location from what had been three separate Washington, DC locations. Prior to that consolidation, OTIM was directed by FHFA's Office of General Counsel (OGC) to retain certain electronic media related to litigation holds.[3] OTIM leadership decided to take the extra step of preserving all electronic media, including electronic media dating back to 1999, which included FHFA's predecessor agencies, the Office of Federal Housing Enterprise Oversight and the Federal Housing Finance Board. In 2018, OGC released several litigation holds, which permitted the destruction of the electronic media that was being held.

In September 2018, OTIM staff prepared a Staff Analysis memorandum (OTIM Staff Analysis) that recommended that "all hard drives, tape drives, and mobile devices referenced in [the] Staff Analysis and collected from excessed equipment between 1999 and February 2018, be securely shredded and recycled to prevent the unauthorized disclosure of Agency

[2] GAO-14-704G (Sept. 2014).

[3] A litigation hold is a notification from an organization's legal team to employees instructing them not to delete or destroy electronically stored information or discard paper documents that may be relevant to a new or imminent legal case.

data…" The OTIM Staff Analysis further recommended "acquiring the services of a secure shredding service to perform on-site shredding while observed by an OTIM employee."

In October 2018, FHFA's CIO approved the OTIM Staff Analysis recommendation to securely shred and recycle the electronic media listed in the document. Since OTIM determined it was not feasible to perform the shredding in-house, FHFA modified its existing contract used for paper shredding on November 30, 2018, to provide for off-site shredding of the electronic media.[4]

FHFA provided us with a PowerPoint presentation that it received from the contractor before it modified the contract for off-site shredding of electronic media. That presentation explained the contractor's controls over the destruction of customer materials. These controls included locked containers, scanning of the containers when picked up by the contractor at the customer's location and upon arrival at the contractor's facility, the destruction of the materials witnessed by the contractor, and camera monitoring of the contractor's facility. According to the presentation, the customer is provided a "Full [Contractor] Certificate of Destruction following each service."

On January 10, 2019, the contractor sent a truck to pick up the electronic media at FHFA's headquarters building for off-site shredding.

FACTS AND ANALYSIS

To implement NIST SP 800-88 and the Green Book requirements, FHFA adopted Information Security Media Sanitization Procedures and Property Management Standard Operating Procedure, both of which were in effect when the disposal of electronic media that is the subject of this audit took place in January 2019.

FHFA's Summary Count of Electronic Media in the OTIM Staff Analysis Did Not Align with its Detailed Inventory Attached to the OTIM Staff Analysis

The OTIM Staff Analysis included an overview of the types of electronic media to be shredded and a summary count of items in each category. Also attached to the OTIM Staff Analysis was a detailed inventory for each type of electronic media. For example, the

[4] On November 9, 2018, the OTIM specialist who oversaw the electronic media targeted for destruction sought and received approval from OTIM's Chief Technology Officer (CTO) and the OTIM Records Officer to allow the contractor to shred the electronic media at the contractor's facility without FHFA observation. The CTO's approval noted that the risk to FHFA was low as "user computer drives are encrypted, and the servers are RAID [Redundant Array of Independent Disks]" so it "would be difficult to get any meaningful data off of them." (In a RAID, data is broken into segments that are sent to the various disks in the array.)

inventory for the laptop hard drives included the FHFA barcodes of the computers from which the hard drives were removed and dates they were removed. Our review of the OTIM Staff Analysis and its attached detailed inventory found differences between the summary counts and the detailed inventory; those differences are shown in Figure 2.

FIGURE 2. DIFFERENCES BETWEEN SUMMARY INVENTORY COUNT IN THE OTIM STAFF ANALYSIS AND COUNT IN THE DETAILED INVENTORY ATTACHED

Type of Electronic Media Targeted for Destruction	Summary Count in the OTIM Staff Analysis	Count in the Detailed Inventory Attached to the OTIM Staff Analysis	Differences
Laptop hard drive (HD)	2,288	1,836	452
Server HD	856	857	(1)
Tape cartridge	95	95	0
iPhone	547	574	(27)[1]
BlackBerry	73	73	0
Totals	**3,859**	**3,435**	**424**

Source: OTIM Staff Analysis and OIG analysis.

[1] In its technical comments to a draft of this report, FHFA advised that 574 was the correct count for iPhones and that the difference was due to a transposition error.

FHFA Failed to Maintain Accountability over the Electronic Media Approved for Shredding in October 2018 and Transferred to the Shredding Contractor in January 2019

Conflicting Counts of the Electronic Media Approved for Disposal and the Electronic Media that Was Picked up for Shredding Were Never Reconciled or Resolved

As discussed above and illustrated in Figure 1, the OTIM Staff Analysis was internally inconsistent on the number of different items in two types of electronic media approved for shredding by the CIO: laptop hard drives and server hard drives.

On January 9, 2019, we observed the area in FHFA's building where the electronic media to be picked up for shredding by the contractor was gathered. (Our observation was conducted the day before the electronic media was collected by the contractor.) The OTIM specialist responsible for overseeing the contracted shredding of the electronic media provided us with another written version of the inventory of electronic media to be shredded (separate from the one in the OTIM Staff Analysis). This version of the inventory was labeled "FINAL HD Count by Location 09Nov2018," and had less detail than the inventory attached to the OTIM Staff Analysis. Figure 3 below illustrates the differences between the summary inventory count in the OTIM Staff Analysis, the count provided in the detailed inventory attached to the

OTIM Staff Analysis, and the count in the inventory labeled "FINAL HD Count by Location 09Nov2018" provided by the OTIM specialist.

FIGURE 3. DIFFERENCES BETWEEN THE INVENTORY COUNTS IN THE OTIM STAFF ANALYSIS, THE DETAILED INVENTORY ATTACHED TO THE OTIM STAFF ANALYSIS, AND THE INVENTORY LABELED "FINAL HD COUNT BY LOCATION 09NOV2018"

Type of Electronic Media Targeted for Destruction	Counts		
	Summary in the OTIM Staff Analysis	Detailed Inventory Attached to the OTIM Staff Analysis	Inventory Labeled "FINAL HD Count by Location 09Nov2018"
Laptop HD	2,288	1,836	2,274
Server HD	856	857	1,163
Tape cartridge	95	95	Not Provided
iPhone[1]	547	574	547
BlackBerry	73	73	73

Source: OTIM Staff Analysis, the Inventory Labeled "FINAL HD Count by Location 09Nov2018," and OIG Analysis.

[1] In its technical comments to a draft of this report, FHFA advised that 574 was the correct count for iPhones and that the difference was due to a transposition error.

We noted to the OTIM specialist that the OTIM Staff Analysis contained different counts of electronic media than the inventory attached to it, and that those two sets of numbers differed from the inventory labeled "FINAL HD Count by Location 09Nov2018." The OTIM specialist responded that the numbers in the inventory labeled "FINAL HD Count by Location 09Nov2018," were estimates, not actual counts. We cannot credit that explanation in light of the precision of the numbers in both the OTIM Staff Analysis and the attached inventory as well as the inventory labeled "FINAL HD Count by Location 09Nov2018."

On January 9, 2019, we observed the organization of the electronic media that was to be picked up the next day by the contractor. We found that the electronic media collected for the contractor was haphazardly stored in ripped and opened boxes, as shown in the photos on the next page:

Source: OIG, photos taken January 9, 2019, of some of the electronic media approved for shredding, which was the day before the contractor sent a truck to FHFA's headquarters building to pick up the electronic media for off-site shredding.

FHFA Failed to Reconcile and Resolve Differences in Counts of Electronic Media between FHFA's Chain of Custody Form Transferring the Media to the Contractor for Shredding, the Contractor's Certificate of Destruction of the Media, and the Contractor's Invoice for the Shredding of the Media

According to the OTIM specialist who was present on January 10, 2019, when the electronic media items identified for shredding were picked up by the contractor at FHFA, the contractor's driver counted the laptop hard drives and the server hard drives as he put the items into contractor-supplied containers. He recorded his counts – 1,845 laptop hard drives (different from any of the FHFA OTIM counts) and 1,205 server hard drives (different from any of the FHFA OTIM counts), for a total of 3,050 hard drives – on an attachment to an FHFA Chain of Custody Form. The OTIM specialist also said he observed the driver counting the tape cartridges before he placed them into two contractor-supplied containers, but the driver did not record the number of tapes on the FHFA Chain of Custody Form. Also, according to the OTIM specialist, the contractor's driver did not count the number of iPhones or BlackBerrys before he placed the iPhones and BlackBerrys together in another contractor-supplied container. The driver recorded a count of "three" "Qtz [sic] of 95g Containers of Cell Phones/Tapes" on the FHFA Chain of Custody Form attachment. The Chain of Custody Form was signed by the OTIM specialist and the driver with a date and time of January 10, 2019, at

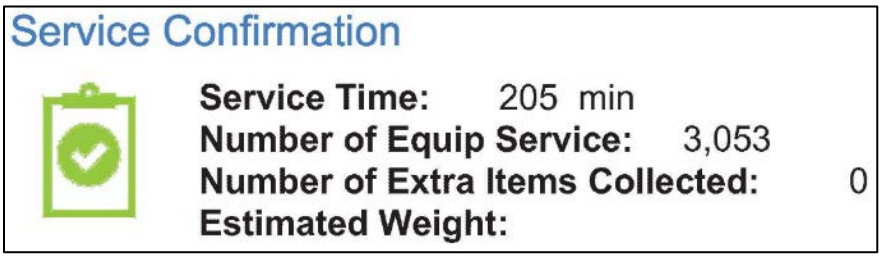
12:30 pm. The driver subsequently scanned the bins and left FHFA with the containers. (See Figure 4 below.)

FIGURE 4. ATTACHMENT TO THE FHFA CHAIN OF CUSTODY FORM SIGNED BY THE OTIM SPECIALIST AND THE CONTRACTOR'S DRIVER

Qty of Hard Drives After 1st 10	Price per Hard Drive	Subtotal Hard Drives	Qtz of 95g Containers of Cell Phones/Tapes	Price per 95g Container	Subtotal 95g Containers	Qty of Servers
2265	$ 4.00	$ 9,060.00	12	$ 35.00	$ 420.00	1170
1845		$ -			$ -	1205
		$ -	3		$ -	
		$ -			$ -	

By email dated January 15, 2019, the contractor provided the OTIM specialist with a Certificate of Destruction. That certificate showed 3,053 equipment items as serviced. See Figure 5.

FIGURE 5. PAGE ONE, CONTRACTOR'S CERTIFICATE OF DESTRUCTION



As discussed earlier, the contractor's driver counted, on January 10, 2019, a total of 1,845 laptop hard drives and 1,205 server hard drives (for a total of 3,050) hard drives. The OTIM specialist explained that the difference of three in the count between the January 10, 2019, inventory count of 3,050 hard drives and the 3,053 on the Certificate of Destruction was due to human error; because it was a small difference, he was not concerned about the discrepancy. Another explanation could be that the 3,053 count consisted of the counted hard drives (3,050) plus the 3 containers, but that was not considered by the OTIM specialist.[5]

[5] In a technical comment to a draft of this report, FHFA took issue with our speculation that the 3,053 count could consist of the counted hard drives (3,050) plus the 3 containers and provided an email exchange between the OTIM specialist and the contractor's representative. In response to the question from OTIM, "So what does the 3,053 represent?," the contractor's representative answered:

> It *looks* like the 3,053 is strictly Hard Drives, the tapes and phones are not individually counted as we used our 96g containers for those (Since only hard drives are billed out individually those

The second page of the Certificate of Destruction included a description of the electronic media supposedly "serviced": laptop hard drives (no quantity provided), media servers (no quantity provided), a container of cell phones (no quantity provided, see arrow), and a container of media tapes (no quantity provided). See Figure 6 below. The OTIM specialist confirmed that this description was only of the types of electronic media "serviced" and not quantities of the media.

FIGURE 6. PAGE TWO, CONTRACTOR'S CERTIFICATE OF DESTRUCTION

We observed to the OTIM specialist that the FHFA Chain of Custody Form listed three containers of tape cartridges and cell phones but the Certificate of Destruction identified only "Lg Tote" for these two categories of electronic media. He responded that he thought that the Certificate of Destruction only identified the types of media (i.e., tapes, phones, and drives), not the quantity. However, his response is not supported by the information recorded on the Certificate of Destruction, which reflects that the collected tapes and cell phones were in "Lg Tote[s]."

The inventory of FHFA electronic media that was picked up and shredded by the contractor is further muddled by the contractor's invoice submitted for the service and paid by FHFA. That invoice, dated January 31, 2019, billed for the off-site "purge" of 1,845 hard drives (the same count on the Chain of Custody Form), 1,205 large media units (the same count on the Chain of Custody Form), and 12 95-gallon bins (although only 3 such containers were identified on the Chain of Custody Form and only 2 on the Certificate of Destruction). See Figure 7.

---

are the only [ones] we scan and count). For the containers, there was a total of 12 96g containers filled with the tapes and phones! (emphasis added)

Later that day, the contractor representative, in the same email chain, stated that 3,053 was the "confirmed final count of hard drives," which was different from the 3,050 hard drives that the contractor's driver logged on the Chain of Custody form.

If FHFA's position were accepted as accurate, and 3,053 hard drives were collected and destroyed by the contractor, the contractor's Certificate of Destruction would be inaccurate because the total would not include the containers filled with tapes, iPhones, and BlackBerrys on FHFA's Chain of Custody form.

FIGURE 7. CONTRACTOR'S INVOICE DATED JANUARY 31, 2019

ACR CIN#	SERVICE TYPE	SHRED-SIZE	QTY	UNIT OF MEASURE	MINIMUM STOPCHRG	UNIT PRICE	TOTAL
'FA DC OBFM, 400 7th St SW, Washington, DC, 20024-2585, US							
	OFF-SITE PURGE -MEDIA		1,845	Hard Drive		4.00	$7,380.00
	OFF-SITE PURGE -MEDIA		1,205	Large Media Unit		6.00	$7,230.00
	OFF-SITE PURGE -MEDIA		12	95 Gallon Bin		35.00	$420.00

We asked FHFA to explain the discrepancy between the number of containers billed (12) and the number on the Certificate of Destruction (2). FHFA had no explanation and never challenged the number of containers for which it was billed.

FHFA Did Not Follow its Sanitization Procedures for the Hard Drives, Tapes, and iPhones that Were Approved for Shredding in October 2018 and Transferred to the Shredding Contractor in January 2019

At the time of the January 2019 disposal, FHFA's Information Security Media Sanitization Procedures stated that tapes should be degaussed and required that hard drives "must be removed and degaussed or undergo Secure Erase," and disposal must occur through shredding.[6] The procedures also required that iPhones be "purged through a local or remote wipe which consists of erasing all content and settings" prior to destruction.[7]

We were told that none of the hard drives and tapes approved for destruction in October 2018 were degaussed after the litigation holds were lifted.[8] OTIM officials also reported to us that some unknown number of the 574 iPhones were not "wiped" (e.g., returned to a factory setting with all data removed as required by FHFA policy) during a "tech refresh" in March

[6] Degaussing is a process of exposing magnetic media such as hard drives and magnetic tape to a strong magnetic field to disrupt the recorded data. Secure Erase is a command that completely erases all data, amounting to electronic data shredding.

[7] The version of the Information Security Media Sanitization Procedures in effect in January 2019 (Revision 1.3, dated February 2018) did not mention sanitization procedures for BlackBerrys. An earlier version, Revision 1.2 dated May 2016, prescribed wipe as the sanitization method for BlackBerrys. We did not inquire as part of this audit whether the BlackBerrys targeted and approved for destruction were wiped.

[8] In a technical comment to a draft of this report, FHFA explained that the hard drives and tapes were not sanitized (degaussed or Secure Erased) at the time they were removed from servers or computers because of the litigation holds. Once the litigation holds were subsequently lifted, we found that FHFA failed to follow its sanitation policy for the hard drives approved for destruction, which FHFA does not dispute.

2017. OTIM provided several reasons why these iPhones were not wiped, including the claim it would have taken thousands of hours to manually reset all the iPhones individually (which we do not credit because of the ease in restoring iPhone factory settings)[9] and that FHFA lacked the necessary number of software licenses to manage its tech refresh. According to OTIM, the licenses for returned iPhones were reassigned to new iPhones before the old iPhones were wiped.

We recognize that NIST SP 800-88 does not require degaussing prior to shredding of hard drives and tapes if meaningful controls exist over these categories of electronic media. NIST also does not require wiping of iPhones or other cell phones if they are destroyed by shredding. However, FHFA lacked meaningful controls over the electronic media approved for shredding in October 2018 and collected by its contractor in January 2019, for the following reasons:

- FHFA lacked an accurate inventory of the electronic media approved for shredding by the CIO in October 2018;
- It failed to identify and reconcile the discrepancies between the summary count in the OTIM Staff Analysis and the attached detailed inventory;
- It failed to identify and reconcile the discrepancies between the detailed inventory attached to the OTIM Staff Analysis, the summary count in the OTIM Staff Analysis, and the inventory labeled "FINAL HD Count by Location 09Nov2018;"
- It failed to identify and reconcile the discrepancies between the inventory labeled "FINAL HD Count by Location 09Nov2018" and the inventory listed on FHFA's Chain of Custody Form, completed at the time of pick-up on January 10, 2019; and
- It failed to identify and reconcile discrepancies between the inventory listed on FHFA's Chain of Custody Form and the contractor's invoice.

Figure 8 below shows the differing counts and units of measure that were never reconciled for the electronic media that was targeted and, in January 2019, destroyed.

[9] In technical comments to a draft of this report, FHFA maintained that it lacked sufficient resources needed to manually wipe each iPhone, and its May 2019 updated policy permitted it to send unwiped iPhones to a contractor for destruction. This audit looked at FHFA's controls over electronic media approved for shredding in October 2018 and transferred to its contractor in January 2019, so the May 2019 updated policy, whatever it may authorize, has no relevance. FHFA has provided no explanation why it would elect to wipe one phone at a time rather than wipe a large number at the same time.

FIGURE 8. THE SUMMARY COUNT OF ELECTRONIC MEDIA TARGETED FOR DESTRUCTION IN THE OTIM STAFF ANALYSIS, THE COUNT IN THE DETAILED INVENTORY ATTACHED TO THE OTIM STAFF ANALYSIS, THE INVENTORY LABELED "FINAL HD COUNT BY LOCATION 09NOV2018," THE COUNT IN THE ATTACHMENT TO FHFA CHAIN OF CUSTODY FORM SIGNED JANUARY 10, 2019, AND THE COUNT IN THE CONTRACTOR'S INVOICE DATED JANUARY 31, 2019

Type of Electronic Media Targeted for Destruction	Counts				
	Summary in the OTIM Staff Analysis	Detailed Inventory Attached to the OTIM Staff Analysis	Inventory Labeled "FINAL HD Count by Location 09Nov2018"	Attachment to FHFA Chain of Custody Signed January 10, 2019[1]	Contractor's Invoice Dated January 31, 2019
Laptop HD	2,288	1,836	2,274	1,845	1,845
Server HD	856	857	1,163	1,205	1,205
Tape cartridge	95	95	Not provided	Three 95-gallon bins of cell phones/ tapes	Unknown – contractor billed for 12 95-gallon bins
iPhone[2]	547	574	547		
BlackBerry	73	73	73		

[1] As discussed above, page one of the contractor's Certificate of Destruction showed that 3,053 equipment items were serviced (which is consistent with the count of 1,845 laptop hard drives, 1,205 server hard drives, and 3 95-gallon bins) (see Figure 4). The second page of the Certificate of Destruction included a description of the electronic media supposedly "serviced": laptop hard drives (no quantity provided), media servers (no quantity provided), a container of cell phones (no quantity provided), and a container of media tapes (no quantity provided) (see Figure 5).

[2] In its technical comments to a draft of this report, FHFA advised that 574 was the correct count for iPhones and that the difference was due to a transposition error.

According to the CTO, FHFA did not need tight controls over the hard drives and arrayed server drives because those drives were encrypted and the risk of a security breach of the information on them was low. That assertion, however, is at odds with FHFA's Information Security Media Sanitization Procedures and NIST SP 800-88. Additionally, some number of the 574 iPhones that were approved for destruction retained their FHFA data when they were picked up by the contractor. In the event that these iPhones were not destroyed pursuant to the contract, there is a risk that FHFA data could have been accessed.

FHFA Has Not Disposed of Any Electronic Media Since January 2019 and Further Disposals of Electronic Media Have Been on Hold Since October 2019

By email dated October 23, 2019, FHFA's CIO instructed OTIM management and security staff:

> Until further notice, all destruction of excess FHFA equipment is hereby suspended. Any already collected equipment, or subsequently collected equipment, should be stored securely and inventoried. Additional guidance

will be provided shortly. This suspension will be in effect until I notify you otherwise and I do not anticipate any exceptions being granted.

According to an OTIM official, the hold on disposal of the excess equipment was put in place until FHFA's disposal procedures are redone. As of February 2020, there was no anticipated date for completion of the revised procedures.

Controls Over Retired Electronic Media Continued to Fall Short of Ensuring Accountability

As part of our audit, we sought to determine what physical controls were in place over the electronic media that had been retired since October 2018, the approval date of the OTIM Staff Analysis. FHFA's Property Management Standard Operating Procedure requires:

- Retired property must be held in a designated secure room within FHFA.
- Hard drives must be removed from retired computers, including laptops, and clearly marked.
- The Help Desk must maintain an index, or inventory, of each removed hard drive, identified by its serial number, the barcode of the computer from which it was removed, the type and model of the computer, the name of the user to whom the computer was assigned, the date the hard drive was removed and the reason for the removal, and the box where the hard drive would be stored.[10]

The procedure also calls for the Help Desk contractor to perform a monthly physical inventory of all "accountable" property and reconcile the inventory results to OTIM's inventory system of record, the Configuration Management Database (CMDB). However, hard drives removed from retired computers were not considered accountable property and were not recorded in or reconciled to the CMDB nor were they part of a regular physical inventory. In our view, this procedure does not meet Green Book requirements: electronic media removed from computers is not accounted for in OTIM's inventory system of record (control record) and such media is not included in regular physical inventories.

On January 17, 2020, we observed a sealed box containing hard drives that had been reportedly removed from retired computers in the designated secured room for retired IT assets. We requested and observed an OTIM Help Desk contractor employee verify that the drives in the box matched the index (inventory) maintained by the Help Desk. The contractor

[10] The computers and mobile devices (e.g., iPhones, tablets) and their status (e.g., Issued, Returned, Retired) were tracked within OTIM's inventory system of record. The spreadsheet index of hard drives was maintained outside that system.

unsealed the box, counted the hard drives therein, and compared the count and information on each hard drive to the number and information on the index. Based on our observation, we found that the contents of the box matched the information on the index, without exception.[11]

We did not, as part of our observation, attempt to determine whether the index matched any other control record, such as the computers in the CMDB with the status of retired, as there are no FHFA procedures calling for such a match. While FHFA's sealed box of hard drives matched the index maintained by the Help Desk on January 17, 2020, our observation provides no assurance that FHFA can account for all hard drives removed from computers because such hard drives were not included in its regular physical inventory nor recorded in and reconciled to the CMDB.

FINDINGS

1. **FHFA Lacked Adequate Controls over the Electronic Media Approved for Destruction**
2. **FHFA Did Not Follow its Electronic Media Sanitization Procedures**
3. **FHFA's Controls over Retired Electronic Media Did Not Ensure Accountability**

CONCLUSION

FHFA lacked an accurate count of the volume of electronic media – laptop and server hard drives, tapes, iPhones, and BlackBerrys, accrued over 19 years, approved by FHFA's CIO for destruction in October 2018 and destroyed in January 2019, in violation of NIST SP 800-88, the Green Book, and its internal guidance. In connection with its efforts to collect and send out hard drives, tapes, iPhones, and BlackBerrys for destruction, we found that FHFA failed to follow its own sanitation procedures. In the event that these electronic media were not destroyed pursuant to the contract, there is a risk that FHFA data could have been accessed.

FHFA's current Property Management Standard Operating Procedure for electronic media targeted for disposal does not meet Green Book requirements: electronic media removed from computers is not accounted for in OTIM's inventory system of record (control record) and such media is not included in regular physical inventories. FHFA has suspended further disposal of electronic media targeted for destruction, pending revisions to its disposal

[11] There were 103 hard drives in the box as of January 17, 2020.

procedures. Revision of FHFA's current procedures should meet the requirements imposed by NIST and the Green Book.

RECOMMENDATION

We recommend that FHFA:

1. Review, revise, and implement its procedures for disposal of electronic media targeted for destruction, consistent with NIST and Green Book requirements. Those revised procedures should:

    - Prescribe the expectations for sanitization of the targeted electronic media consistent with NIST guidance;
    - Provide for tracking the targeted electronic media in an inventory system of record;
    - Provide for regular physical inventory of the targeted electronic media and reconciliation to the control record(s) through destruction; and
    - Provide for accountability of the targeted electronic media from the time the media is taken out of service through its destruction, with reconciliations of any count differences that may arise as the media is transferred within FHFA, and from FHFA to other parties used to destroy the media.

Should FHFA decline to accept this recommendation, we expect that FHFA will propose an alternative management decision with actions to address the deficiencies identified in this report and a timetable to fully implement those actions. When FHFA proposes an alternative management decision, we expect that it will advise us of the controls it intends to put into place to remediate the identified deficiencies so that we can test their efficacy.

FHFA COMMENTS AND OIG RESPONSE

We provided FHFA an opportunity to respond to a draft of this audit report. FHFA provided technical comments on the draft report, and those comments were considered in finalizing this report. FHFA also provided a management response, which is included in the Appendix to this report. In its management response, FHFA agreed with our recommendation and plans to take corrective actions on or before December 15, 2020.

As its corrective actions, FHFA plans to (1) review and revise its Media Sanitization Procedure and (2) revise its Asset Management Procedures to ensure that all targeted electronic media is tracked in an inventory system of record; is physically inventoried and reconciled to inventory control records; and is accounted for from the time the targeted electronic media is taken out of service through its destruction. The revised procedures will provide for the reconciliation of any differences in counts that arise during the excess and destruction process. We consider FHFA's planned corrective actions responsive to our recommendation.

OBJECTIVE, SCOPE, AND METHODOLOGY .....

We conducted this audit to determine FHFA's controls over the disposal of electronic media and assess whether those controls were operating effectively.

To accomplish our objective,

- We reviewed:
    - NIST standards and guidelines: Federal Information Processing Standards Publication 199, *Standards for Security Categorization of Federal Information and Information Systems* (February 2004) and NIST Special Publication 800-88, Revision 1, *Guidelines for Media Sanitization* (December 2014) for electronic media sanitization.
    - GAO's *Standards for Internal Control in the Federal Government* (September 2014). We determined that the category of control activities applicable to this audit was "Physical control over vulnerable assets."
    - FHFA procedures: Information Security Media Sanitization Procedures (February 2018 and May 2016 versions) and Property Management Standard Operating Procedure (May 2018).
- We reviewed and analyzed:
    - An OTIM Staff Analysis entitled "Disposal of FHFA Hard Drives," approved by FHFA's CIO on October 24, 2018. Attached to this memorandum was a detailed inventory of electronic media targeted for disposal.
    - Contract documents pertaining to FHFA's modification in November 2018 of an existing contract for paper-shredding services to include shredding services

for electronic media. We also interviewed FHFA contracting staff about these documents.

  - Other FHFA documentation related to the electronic media shredding. This documentation included: an inventory labeled "FINAL HD Count by Location 09Nov2018"; an FHFA Chain of Custody Form transferring electronic media to the contractor signed by FHFA and a driver for the contractor on January 10, 2019; the contractor's Certificate of Destruction for electronic media provided to FHFA by the contractor on January 15, 2019; and the contractor's invoice for the electronic media shredding service dated January 31, 2019.

- We interviewed FHFA OTIM officials and staff and OTIM Help Desk contractor employees regarding their roles in the electronic media disposal process. Among those interviewed was the OTIM senior IT specialist most involved with the electronic media disposal approved by the CIO in October 2018.

- We observed a physical inventory by an OTIM Help Desk contractor employee of electronic media that had been reportedly removed from retired computers. That physical inventory was performed at our request on January 17, 2020.

We conducted this performance audit between October 2018 and March 2020 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 objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objective.

APPENDIX: FHFA MANAGEMENT RESPONSE.....

Federal Housing Finance Agency

MEMORANDUM

TO: Marla Freedman, Deputy Inspector General for Audits

FROM: R. Kevin Winkler, Chief Information Officer RKW

SUBJECT: Draft Audit Report: *FHFA Cannot Assure that All Electronic Media Approved for Destruction in October 2018 Was Destroyed, and it Continues to Lack Adequate Controls over Electronic Media Targeted for Disposal*

DATE: March 27, 2020

Thank you for the opportunity to respond to the above-referenced draft audit report by the Office of Inspector General. This memorandum provides the Federal Housing Finance Agency's (FHFA) management response to the single recommendation contained in the draft audit report.

Recommendation 1: *Review, revise, and implement its procedures for disposal of electronic media targeted for destruction, consistent with NIST and Green Book requirements. Those revised procedures should:*

- *Prescribe the expectations for sanitization of the targeted electronic media consistent with NIST guidance;*
- *Provide for the tracking of the targeted electronic media in an inventory system of record;*
- *Provide for regular physical inventory of the targeted electronic media and reconciliation to the control record(s) through destruction; and*
- *Provide for accountability of the targeted electronic media from the time the media is taken out of service through its destruction, with reconciliations of any count differences that may arise as the media is transferred within FHFA, and from FHFA to other parties used to destroy the media.*

Management Response: FHFA agrees with the recommendation and will take the following actions.

a. Review and revise its Media Sanitization Procedure by December 15, 2020; and
b. Revise its Asset Management Procedures by December 15, 2020, to ensure that all targeted electronic media:
    - Is tracked in an inventory system of record;
    - Is physically inventoried and reconciled to inventory control records;

- Is accounted for from the time the targeted electronic media is taken out of service through its destruction. The revised procedures will provide for the reconciliation of any differences in counts that arise during the excess and destruction processes.

If you have any questions, please feel free to contact Stuart Levy at (202) 649-3610 or e-mail, Stuart.Levy@fhfa.gov.

CC: Chris Bosland
Larry Stauffer
Craig Sherman
Ralph Mosios
Jim Vercellone
Jason Donaldson
John Major

ADDITIONAL INFORMATION AND COPIES.....

For additional copies of this report:

Call: 202-730-0880

Fax: 202-318-0239

Visit: www.fhfaoig.gov

To report potential fraud, waste, abuse, mismanagement, or any other kind of criminal or noncriminal misconduct relative to FHFA's programs or operations:

Call: 1-800-793-7724

Fax: 202-318-0358

Visit: www.fhfaoig.gov/ReportFraud

Write:

FHFA Office of Inspector General
Attn: Office of Investigations – Hotline
400 Seventh Street SW
Washington, DC 20219