# Audit of NARA's Photocopier Security

## OIG Audit Report No. 11-07

## March 22, 2011

# Table of Contents

# Executive Summary

The National Archives and Records Administration (NARA) Office of the Inspector General (OIG) performed an audit of NARA's Photocopier Security. The objective of the audit was to determine if appropriate security measures were in place to safeguard and prevent inappropriate release of sensitive information and Personally Identifiable Information (PII) residing on NARA photocopiers that contain hard drives. Specifically our review focused on whether (1) NARA used photocopiers that contained hard drives capable of retaining sensitive information and (2) actions taken by NARA to mitigate risks posed by the potential exposure of this sensitive information were adequate.

An April 2010, CBS investigative news report exposed the potential privacy risks arising from sensitive and PII information left on the hard drives of excessed photocopiers that were not sanitized prior to disposal. When multiple copies of a document are made, using a photocopier that has a hard drive, the document is scanned once and copies are made from the file that has been saved on the hard drive. The residual data on the hard drive can be accessed, potentially exposing sensitive or PII which could lead to identity theft or fraudulent use of the information. The CBS news investigation found that hard drives of disposed photocopiers contained a plethora of sensitive, confidential, and PII data that was easily retrievable from the photocopier's hard drives.

Our audit found that opportunities exist to strengthen controls to ensure photocopier hard drives are protected from potential exposure. Specifically, we found the following weaknesses.

- NARA lacks appropriate controls to ensure all photocopiers across the agency are accounted for and that any hard drives residing on these machines are tracked and properly sanitized or destroyed prior to disposal.

- There are no policies documenting security measures to be taken for photocopiers utilized for general use nor are there procedures to ensure photocopier hard drives are sanitized or destroyed prior to disposal or at the end of the lease term.

- Photocopier lease agreements and contracts do not include a "keep disk"[1] or similar clause as required by NARA's *IT Security Methodology for Media Protection Policy* version 5.1.

During the entrance conference for this review, management informed the OIG that they were aware of the potential risks posed by not properly sanitizing photocopier hard drives prior to disposal and had initiated action to address the risks. Specifically, in May 2010, NARA's Office of General Council (NGC) began efforts to identify photocopier

[1] "Keep Disk" clause is language within a contract that allows retention of a hard drive should it fail and need to be replaced.

contracts and agreements across the agency in order to update them to include appropriate security language. Photocopier contracts (whether they have a hard drive or not) are being modified to contain a "keep your hard drive" clause in accordance with section 6 of NARA's *IT Security Methodology for Media Protection Policy* version 5.1. However, at the end of our fieldwork, NGC reported only 15 of the 79 agreements identified by management have been modified.

This report contains seven recommendations for addressing our findings. The recommendations in this report, upon adoption, will assist NARA in providing appropriate administrative, technical, and physical safeguards over sensitive information and PII as required by the Privacy Act.

# Background

An April 2010, CBS investigative news report brought attention to the potential privacy risks arising from the fact that photocopiers can store digital images of items copied on internal hard drives. The investigation found disposed photocopiers contained a plethora of sensitive, confidential, and PII data that was able to be retrieved from photocopier's hard drives.

Since 2002, many photocopiers have been manufactured to contain a hard drive with the capability of electronically storing images of documents copied, scanned, or emailed. Usually when several copies of a document are made, the document is scanned just once and the copies are made from the file that has been saved on the hard drive. The residual data can be accessed by removing the hard drive from the photocopier and connecting it to a PC. The hard drive requires special sanitization in order to mitigate the risk of unauthorized disclosure of information and to ensure its confidentiality. NARA's *IT Security Methodology for Media Protection Policy* version 5.1 states that information system media, which includes hard drives, must be sanitized prior to disposal or release. Sanitization techniques including clearing, purging, and destroying media information would prevent the disclosure of NARA sensitive information when the hard drive is reused or disposed.

Safeguarding PII is important to protect individuals, maintain public trust and confidence in an organization, and protect the reputation and any legal liability of an organization. For Federal government agencies the Privacy Act of 1974 requires them to establish appropriate administrative, technical and physical safeguards to ensure the security and confidentiality of records and to protect against any anticipated threats or hazards to their security or integrity which could result in substantial harm, embarrassment, inconvenience, or unfairness to any individual on whom information is maintained. NARA has responsibility to appropriately safeguard sensitive data and PII, including PII on hard drives of photocopiers. PII retained on unprotected hard drives could potentially be exposed and lead to identity theft or fraudulent use of the information. In May 2010, NARA's Office of General Council (NGC) began efforts to identify photocopier contracts and agreements across the agency in order to update them to include appropriate security language. Photocopier contracts (whether they have a hard drive or not) are being modified to contain a "keep your hard drive" clause in accordance with section 6 of NARA's *IT Security Methodology for Media Protection Policy* version 5.1.

The Acquisitions Services Division (NAA) within the Office of Administration (NA) maintains responsibility for procuring and managing of general photocopiers across NARA. According the Director of NAA, the Office of Presidential Libraries (NL) and the Office of Regional Records Services (NR) have the authority to procure and manage their own photocopiers.

# Objectives, Scope, Methodology

The objective of this audit was to determine whether the appropriate security measures were in place to safeguard sensitive information and PII residing on photocopier hard drives upon disposal or while in possession of an outside vendor. Specifically our review focused on whether (1) NARA used photocopiers that contain hard drives capable of retaining sensitive information and (2) that actions taken by NARA to mitigate risks posed by the potential exposure of this sensitive information were adequate. The audit included photocopiers across all NARA offices. However, all audit work was performed at Archives II in College Park, MD.

We examined applicable laws, regulations, and NARA guidance including (a) The Privacy Act of 1974; (b) The Federal Information Security Management Act (FISMA) of 2002; (c) National Institute of Standards and Technology (NIST) Special Publication 800-88, *Guidelines for Media Sanitization*; (d) NARA Directive 1608 *Protection of Personally Identifiable Information (PII*); (e) NARA's IT Security Methodology for Media Protection; (f) Supplement to NARA 202, *Classified Information Security Program Handbook*; (g) Transmission of Electronic Media to NARA sites; (h) Asset Management Team Media Tracking and Disposal Plan; (i) Supplement to NARA 241, *NARA Personal Property Operating Guide*; and (j) NARA 236-1, *Inventory of Government Accountable and Sensitive Property*.

To accomplish our objectives we did the following:

- Judgmentally selected a sample of NARA owned photocopiers and performed research to determine if a hard drive was installed;
- Reviewed disposal and excess property documents from 2005 through 2010 and made inquiries with vendors to determine if the model had the capability of having a hard drive;
- Reviewed controls over classified photocopiers;
- Reviewed photocopier contracts;
- Held discussions with NARA employees and officials within the Office of General Council (NGC), Office of Administration (NA), Office of Acquisition Services (NAA), Facilities and Personal Property Management Division (NAF), Office of Information Services (NH), and the Office of Regional Records Services (NR);
- Reviewed all network printers to identify those with hard drives.

Our audit work was performed between July 2010 and October 2010. 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 objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

# Audit Results

## 1. Accountability and controls over photocopier inventory and disposals require improvement

NARA lacks appropriate accountability and adequate management controls to ensure all photocopiers across the agency are accounted for and that any hard drives residing on these machines are tracked and properly sanitized or destroyed prior to disposal. Specifically our audit disclosed: (1) no complete agency-wide inventory of copiers exist, (2) copiers containing hard drives have not been identified, (3) copier purpose and use have not been identified, and (4) disposal protocols were not adequate. These conditions exist because no group has been assigned responsibility for tracking all photocopiers across the agency and ensuring that any photocopiers containing hard drives are properly sanitized prior to disposal. According to NARA's *IT Security Methodology for Media Protection Policy* version 5.1, NARA must sanitize or destroy information system media before disposal or release for reuse. In addition, NARA Directive 1608 *Protection of Personally Identifiable Information (PII*) defines the rules to protect PII from unauthorized disclosure and emphasizes the role of NARA users in ensuring appropriate safeguards are in place to protect all NARA systems containing PII. Furthermore, according to NARA 236-1 *Inventory of Government Accountable and Sensitive Property* and NARA 241 *NARA Personal Property Operating Guide*, accountable property includes borrowed or leased property as well as property having a unit cost of $3,000 or more. Accountable property must be tracked and accounted for in the NARA Personal Property Management System. As a result of the lack of accountability and controls, NARA is at risk of inappropriate release of sensitive information and PII data.

During the course of our review, we interviewed management to determine who was responsible for accounting for, tracking, and disposing of all photocopiers across the agency. No one office claimed responsibility. The Acting Assistant Archivist of NA stated that a complete listing of all photocopiers and related hard drives is just not maintained. A property management officer within NAF stated that leased photocopiers are not considered accountable property and therefore they are not tracked and that hard drive information was also not tracked by NAF. The Director of NAA indicated that NAA did not have a complete listing of all photocopiers across the agency because some offices procure photocopiers without going through NAA. He also stated that NAA would not be responsible for maintaining such a list. The Acting Chief Information Officer stated that since photocopiers are not considered computer equipment, they were not responsible for the disposition of them. However, he stated that NH's disposition policies for hard drives may apply. NGC also stated that they are not responsible for tracking this information. Although, NGC has recently taken on efforts to ensure photocopier contracts include the appropriate security language, they have not attempted to identify individual photocopiers with hard drives to ensure the correct procedures are followed when disposing of them.

Additionally, we also discussed the condition noted above with General Counsel and the Acting Assistant Archivist for NA. Both agreed that the weaknesses cited represent security vulnerabilities that needed management's attention to ensure appropriate controls are identified and put in place to mitigate the risk of potential exposure.

Without adequate accountability and controls, there is an increased risk of exposure of PII or sensitive information that could leave NARA vulnerable.

**No complete agency-wide inventory of photocopiers exist**

There is no complete accurate inventory of photocopiers across the agency and no one office is assigned responsibility to maintain and track such an inventory. The OIG attempted to get a complete photocopier listing containing all photocopiers across the agency (owned and leased) from NAF and NAA and was not able to obtain a complete accurate list. NAF maintains a list of 144 leased photocopiers located within the Archives I, Archives II, St Louis, and Suitland offices and a list of 119 owned photocopiers across the agency. However, these lists do not represent a complete inventory of all photocopiers (leased and owned) across the agency.

When we asked whether a list of leased photocopiers in all offices existed, we were told that leased copiers are not accountable property and therefore not inventoried or in the property management system. However, according to NARA 236-1 *Inventory of Government Accountable and Sensitive Property* and NARA 241 *Personal Property Operating Guide*, accountable property includes borrowed or leased property as well as property having a unit cost of $3,000 or more. Accountable property must be tracked and accounted for in the NARA Personal Property Management System. We discussed this with the property management officer within NAF who agreed that leased photocopiers should be tracked.

NAF management maintains a list of 119 owned photocopiers across the agency in the PPMS system. However, through discussions and contact with various NARA personnel and offices we identified at least six additional NARA owned photocopiers that were not on the NAF list (see below). All six machines had an acquisition cost of $3,000 or more and according to NARA 236-1 and 241 they should have been tracked and accounted for in the NARA Personal Property Management System.

| Copier Make | Serial Number | Location | Acquisition Cost |
|---|---|---|---|
| Cannon IR5000 | MPL62529 | Morrow | $3,286.56 |
| Cannon IR5000 | MPL09414 | Morrow | $3,000.00 |
| Cannon IR3300 | MRJ03267 | Atlanta Federal Records Center | $3,166.68 |
| Cannon IR4570 | SKU1895 | Atlanta Federal Records Center | $3,868.32 |

| | | | |
|---|---|---|---|
| Canon IR 3300G | MRJ02983 | Carter Library | $6,709.43 |
| Konica/Minolta bizhub C550 | A00J011000421 | Bush Library | $11,364.30 |

**Photocopiers containing hard drives have not been identified**

Neither the list of owned photocopiers nor the list of leased photocopiers obtained from NAF identified photocopiers with hard drives. We requested this information from NAF and were told this information was not known because no one was keeping track of it. To identify whether any of the photocopiers had a hard drive installed, we took a sample of 69 photocopiers from the list of 119 owned photocopiers acquired since 2005. We made inquiries with the photocopier manufacturers to determine if the photocopiers had hard drives. We gave the manufacturers the make, model, and serial number to identify if the specific model had a hard drive installed on it. In addition, we obtained information from the NARA regional and library offices on leased or owned photocopiers with hard drives. Our analysis revealed a total of 34 photocopiers currently at NARA (both leased and owned) that have a hard drive installed on them. One of the 34 photocopiers identified as having a hard drive is used for classified reproduction (See appendix A). We could not be reasonably sure that this is a complete listing of all photocopiers across the agency that contains hard drives since there is no tracking of all photocopiers across the agency.

Without having a complete list of all photocopiers across the agency and whether they contain a hard drive, NARA is lacking the administrative safeguards to protect PII that may reside on photocopiers hard drives.

**Photocopier purpose and use have not been identified**

The lists of owned and leased photocopiers we obtained from NAF did not indicate whether the photocopiers were used for classified or general copying. This would be of importance to NAS since they are responsible for tracking classified information. The lists did not document where classified photocopiers were located and who was responsible for them. There are additional controls and security measures that are to be in place for classified photocopiers. Specifically the following additional controls and security measures are required.

- Classified reproduction equipment must be located in a secure area or, access must be restricted while copying is in progress.
- All machines used for classified reproduction should incorporate as many security design features as possible (e.g., lock, copy counter, removable hard drives, encryption of data prior to being stored in memory and on hard drive, all memory automatically cleared after copy).
- Photocopiers located outside of secure areas that are authorized for classified reproduction must not have hard drives or the capacity to retain memory or images.

- Classified photocopiers must be sanitized before allowing maintenance personnel access to the machine. Copier maintenance personnel must be escorted and closely monitored by appropriately cleared NARA staff whenever they service equipment authorized for classified reproduction.

Without this information, management cannot perform appropriate oversight to properly track photocopiers and ensure that appropriate controls are being implemented over them.

**Disposal protocols for photocopiers were not adequate**

Photocopier disposals are not adequately tracked and documented and NARA did not ensure that hard drives on excessed photocopiers were sanitized prior to disposal. Based on our audit work, we identified that photocopiers have been disposed of in the last five years which had the potential of having a hard drive installed on them.

The OIG obtained 17 excess property and destruction reports from the requested period of 2005 through 2010 to determine if any photocopiers disposed contained a hard drive. Excess property and destruction reports were not filed in one central location or sequentially. Some were filed in boxes and some online using the Standard Form 120. Additionally these forms in some cases were either filled out inaccurately or were incomplete. None of the forms indicated whether the photocopier being excessed contained a hard drive and whether the hard drive was sanitized. Therefore, we concluded that photocopier disposals are not adequately tracked and we could not be reasonably certain that we obtained a complete listing of all photocopier disposals within the last five years.

We made inquiries with the photocopier manufacturers to determine if any of the photocopiers listed on those excess reports had a hard drive. We gave them the make and model to identify if the specific model had the capability of having a hard drive installed on it. Of the 39 photocopiers that were disposed of during this time frame by the agency, there were 19 photocopiers with the potential of having a hard drive installed on them (see below). There was no documentation available to ascertain whether hard drives were in fact installed on these machines or that hard drives were removed and sanitized or destroyed prior to disposal.

| SF 120 Report Number | Disposition date | Make/Model | Quantity |
|---|---|---|---|
| 473067-5119 | 5/3/2005 | Cannon 1150 | 1 |
| 473067-6047-0001 | 2/16/2006 | Xerox 230DC | 14 |
| 473067-6047-0001 | 2/16/2006 | Xerox 220DC | 1 |
| 473067-6348 | 12/15/2006 | Xerox 220DC | 1 |
| 473067-6356 | 1/8/2007 | Xerox 220DC | 1 |
| 883101-8212-0080 | 7/25/2008 | Cannon IR400S | 1 |
| | | **Total** | **19** |

Additionally, excess property reports were not always filled out properly. In seven instances the photocopier make and/or model information was not documented on the form, in two instances the model identified was not a photocopier, and in two instances the make and model were recorded incorrectly and the vendor was not able to locate the information needed to perform the audit test.

According to NARA's *IT Security Methodology for Media Protection Policy* version 5.1, NARA must sanitize or destroy information system media before disposal or release for reuse.

NARA Directive 1608 *Protection of Personally Identifiable Information (PII*) defines the rules to protect PII from unauthorized disclosure and emphasizes the role of NARA users in ensuring that the appropriate safeguards are in place to protect all NARA systems containing PII. This directive applies to PII in any form or format which would cover PII residing on a hard drive or memory of a photocopier. Physical and technical safeguards that must be in place according to this directive include the following listed below.

- Encryption of data on external hard drives and properly protected when being transmitted outside the agency.

- Destruction of materials containing PII by shredding, burning, deleting, or other authorized destruction method that ensures the data or record is unreadable or unrecoverable.

Without proper protocols to identify photocopiers with hard drives and ensuring that those hard drives are properly sanitized prior to disposal, there is the risk that hard drives containing PII or classified information could have been exposed leaving NARA vulnerable.

**Recommendation 1**

The Assistant Archivist for Administration should improve the inventory over photocopiers to:

a) Include all photocopiers across the agency (owned and leased); and
b) Identify those photocopiers with hard drives, whether they are used for general or classified copying, and when they are disposed.

**Recommendation 2**

The Assistant Archivist for Administration should assign responsibility to one group to oversee management, tracking, and disposal of photocopiers.

In addition, Assistant Archivist for Administration should assign NAA to consolidate the acquisition of photocopiers into one or few contracts to ensure better management of them and to potentially reduce costs,

**Recommendation 3**

The Assistant Archivist for Administration should ensure that documentation of photocopier disposals include accurate information on the make and model and also identify whether the unit had a hard drive. If a hard drive is present, documentation should include the method of sanitization. In addition, this information should be kept in a central location.

**Recommendation 4**

The Assistant Archivist for Administration should implement a policy that photocopier acquisitions do not include hard drives unless a valid business case is presented specifying the need to have one.

**Management Response**

Management concurred with the recommendations.

## 2. There are no policy and procedures describing security measures to be taken for general use photocopiers and disposal of photocopiers containing a hard drive

There are no documented policies describing security measures to be taken for photocopiers utilized for general use, nor are there procedures to ensure that photocopier hard drives are sanitized or destroyed prior to disposal or at the end of the lease term. Management has not developed policies and procedures in these areas because accountability for this area has not been assigned to any office. In addition, security concerns over photocopier hard drives have recently emerged and management had not made this a priority. Furthermore, NARA has focused on ensuring photocopier contract language is updated rather than ensuring day to day procedures for photocopier use are created and implemented. The Government Accountability Office (GAO) requires managers to develop detailed policies and procedures, and to ensure the policies and procedures are an integral part of agency operations. In addition, the Privacy Act requires each agency to establish administrative and technical safeguards to insure the security and confidentiality of records and to protect against any anticipated threats. Lack of effective policies and procedures increase the risk that photocopier hard drives are not adequately secured and safeguarded and increase the risk of exposure of PII or classified information.

There are no documented procedures or policies in place for photocopiers for general use. NARA does have a policy containing guidelines for copying classified information which provides guidance including security measures for photocopiers used for the reproduction of classified material. However, no guidance has been developed for photocopiers used for general use. Thus, there is no restriction on copying items containing sensitive information such as PII on these photocopiers. Most Human Resources forms, initial travel forms, and background investigation forms contain a social security number and other PII information. Many times these forms are photocopied on a general use photocopier prior to submission to the appropriate department. Additionally, the receiving departments also make copies of these documents using a general use photocopier.

NARA also has guidance addressing the disposal of personal property and the disposal of hard drives regardless of the source. However, there are no procedures specifically addressing how to (1) dispose of photocopiers, (2) remove the hard drives, or (3) ensure that photocopier hard drives are sanitized or destroyed prior to disposal or at the end of the lease term. As a result, confusion exists regarding what to do when a photocopier is ready for disposal. We interviewed several employees who stated that they were unsure of what to do with photocopiers at the end of their useful life. For example one employee in NAF stated that there were 2 copiers in the warehouse "cage" ready to be excessed and he was not sure if there were hard drives in them. In addition, he was not sure how to retrieve the hard drive, what to do with it if there was one, and who was responsible for destroying the hard drive. In another example, an employee in the Center for Legislative Archives (NWL) was not sure how to dispose of an old classified

photocopier properly. There is no guidance to direct NARA employees on how to properly dispose of these items. These examples further validate the need for procedures to be documented and communicated to all NARA employees.

We interviewed the Acting Assistant Archivist of NA and the General Counsel in NGC and both agreed that procedures need to be developed in these areas to ensure that the proper steps are taken to protect PII, classified, or other sensitive information residing on photocopier hard drives.

GAO's *Standards for Internal Control in the Federal Government* states, management is responsible for developing the detailed policies, procedures, and practices to fit their agency's operations and to ensure that they are built into and an integral part of operations. Information should be recorded and communicated to management and others within the entity, who need it, and in a form and within a time frame, which enables them to carry out their internal control and other responsibilities.

Lack of policies and procedures increase the risk that vulnerable assets are not adequately secured and safeguarded and increase the risk of exposure of PII or classified information.

**Recommendation 5**

The Assistant Archivist of Administration should create a policy for security measures to be taken for all photocopiers across the agency similar to the policy used for classified photocopiers.

**Recommendation 6**

The Assistant Archivist of Administration should create a procedure for the disposal of photocopiers that will dovetail into NH's ***Asset Management Team Media Tracking and Disposal Plan.*** The following items should be included in the procedures:

- How the photocopier hard drive should be removed or who to contact to get it removed;
- Where and how to send the hard drive;
- Evidence should be kept to document when it was removed, where it was sent, who received it, when it was destroyed and method of destruction;
- Who maintains responsibility for ensuring this procedure is implemented

This procedure should be reviewed by NA program offices as well as NH. Finally updated procedures should be posted on-line for easy reference by NARA staff.

**Management Response**

Management concurred with the recommendations.

## 3. Security language missing from photocopier contracts

Photocopier lease agreements and contracts do not include a "keep disk" or similar clause as required by NARA's *IT Security Methodology for Media Protection Policy* version 5.1. NARA did not comply with its own policy to mitigate the risks posed by potential exposure of sensitive information in the event a photocopier is in the possession of a vendor or is being replaced, disposed, or turned in after the expiration of the lease term. NARA's *IT Security Methodology for Media Protection Policy* version 5.1 "Media Sanitization" states that contracts are required to include a "keep disk" clause or similar option in order to protect NARA from the risk of PII contained on hard drives from being exposed. While there have been no known security breaches, there is the risk of exposing sensitive information to unauthorized individuals.

In May 2010, NGC began efforts to identify photocopier contracts and agreements across the agency in order to update them to include appropriate security language. According to NGC, photocopier contracts (whether they have a hard drive or not) are being modified to contain a "keep disk" clause in accordance with section 6 of NARA's *IT Security Methodology for Media Protection Policy* version 5.1. NGC developed language for a "keep disk" clause to be included in these agreements and contracts. The clause states:

> *"In accordance with NARA policy, NARA will take title to all electronic storage devices, including but not limited to hard drives that may contain Personally Identifiable Information (PII). NARA will not allow the removal of any electronic storage device that may contain PII data from its facilities by a contractor, including individuals performing maintenance on equipment, devices or systems. This provision applies even in the event the equipment is leased. NARA will handle the destruction of this hardware internally. This provision must flow down to all subcontracts, including those for maintenance.*
>
> *If the Vendor comes into possession of an electronic storage device that may contain PII, the Vendor will immediately notify the Contracting Officer and return the electronic storage device to NARA. Vendor will protect the confidentiality of the electronic storage device and will not access, disclose, release, disseminate, or publish any of the information on the electronic storage device."*

NGC identified and is maintaining a list of 79 lease agreements and purchase documents obtained from a PRISM[2] search as well as by contacting regional and library offices. As of the end of our fieldwork, only 15 of the 79 lease agreements and purchase documents have been modified. This is due to management waiting on vendors to respond to the request to update the contracts and management not having all pertinent information needed to get contracts updated. Of the 79 lease agreements and purchase documents, 15 are for photocopiers that do not have hard drives. So this leaves 49 contracts that have yet to be modified which leaves the agency at risk for exposure of PII or

[2] PRISM is the automated procurement system. NAA uses this application to administer contract awards and maintain purchase information. The application is accessed via the NARANET network.

classified information if hard drives remain the property of the vendor. Furthermore, no action has been initiated on 26 of the 79 agreements because NGC is not aware of who the contract officer is for most of these agreements. Per conversation with NGC, these contracts may not be active and they would need the assistance of NAA in order to determine the status and who would be responsible for updating the contract. Since there is no tracking of all photocopiers in a central location, management cannot be reasonably certain that they have a complete listing of all photocopier leases and contracts, and therefore cannot be sure all photocopier contracts and lease agreements will be updated.

**Recommendation 7**

The Assistant Archivist of NA with assistance from the General Counsel should

a) Work with NAA and NAF to get a complete list of all photocopier contracts and agreements to ensure all get updated to include the appropriate security language;
b) Continue to review and update all photocopier agreements and contracts to include the proper security clause; and
c) Work with NAA to determine the status of the 26 agreements and initiate action to get them modified if necessary.

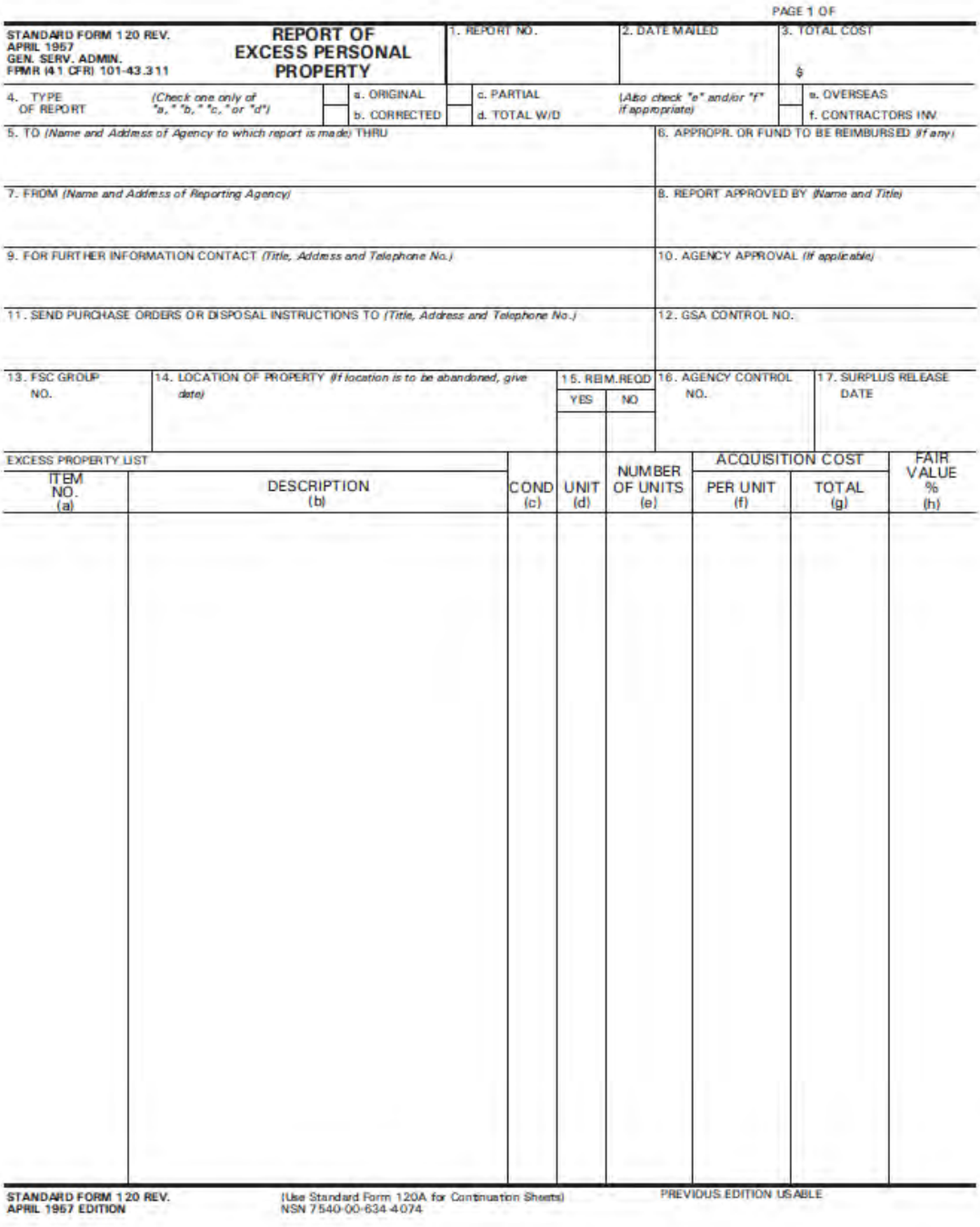
Management Response

Management concurred with the recommendation.

# Appendix A – Photocopiers With Hard Drives

| # | Copier Make | Serial Number | Location | Own or Lease | |
|---|---|---|---|---|---|
| 1 | Xerox WCP35 | MYP-002285 | Clinton Library | Own | |
| 2 | Xerox WCP32/40 | KMM-002591 | Clinton Library | Own | |
| 3 | Xerox CC/WCP35 | MYP-002649 | Clinton Library | Own | |
| 4 | Xerox Bookmark 40 | LBD001186N | Kennedy Library | Own | |
| 5 | KYOCERA KM3060 | UYE8600040 | Military Record Center | Own | |
| 6 | KYOCERA KM3060 | UYE8600038 | ST Louis | Own | |
| 7 | RICOH AFICO 1035G | H7720401218 | Morrow | Own | |
| 8 | KYOCERA KM3050 | UPV7300055 | Military Record Center | Own | |
| 9 | KYOCERA KM3050 | UPV7300062 | Military Record Center | Own | |
| 10 | KYOCERA KM3050 | UPV7200034 | Military Record Center | Own | |
| 11 | KYOCERA KM3050 | UPV7300076 | Military Record Center | Own | |
| 12 | KYOCERA KM3050 | UPV7300054 | Military Record Center | Own | |
| 13 | Panasonic DPC262 | DEG44H00028 | Eisenhower Library | Own | |
| 14 | KYOCERA KM3035 | AJK3016350 | Military Record Center | Own | |
| 15 | KYOCERA KM4035 | AJL3016677 | Military Record Center | Own | |
| 16 | Cannon IR5000 | MPL62529 | Morrow | Lease | |
| 17 | Cannon IR5000 | MPL09414 | Morrow | Lease | |
| 18 | Cannon IR5020 | JCT18197 | Atlanta Federal Records Center | Own | |
| 19 | Cannon IR5020 | JCT18112 | Atlanta Federal Records Center | Own | |
| 20 | Cannon IR3300 | MRJ02070 | Atlanta Federal Records Center | Own | |
| 21 | Cannon IR3300 | MRJ03267 | Atlanta Federal Records Center | Own | |
| 22 | Cannon IR4570 | SKU1895 | Atlanta Federal Records Center | Own | |
| 23 | Ricoh Aficio 1035G | H7011200327 | Morrow | Own | |
| 24 | OCE digital Copier 3165 | 166061658 | Atlanta Federal Records Center | Own | |
| 25 | Konica Minolta 500/501, machine 13468 | A0R5011004757 | Philadelphia | Lease | |
| 26 | Konica Minolta 200/350, machine 13469; ( | 31139718 | Philadelphia | Lease | |
| 27 | Konica Minolat 200/350, machine 13467; ( | 31139684 | Philadelphia | Lease | |
| 28 | Canon Image Runner 3300G | MRJ02983 | Carter Library | Own | |
| 29 | Canon Image Runner 3300G | MPH66494 | Carter Library | Own | |
| 30 | Xerox CC232HG | URT158166 | Carter Library | Lease | Classified |
| 31 | Sharp MX-2700N | 90000472 | Carter Library | Lease | |
| 32 | Sharp AR-M620N | 4AB00381 | Reagan Library | Lease | |
| 33 | Konica Minolta CF3102 | 3129216 | Philadelphia | Own | |
| 34 | OCE 3165 | 1660603319 | Philadelphia | Own | |

# Appendix B - Standard Form 120- Excess Property Report



PAGE 1 OF

STANDARD FORM 120 REV.
APRIL 1957
GEN. SERV. ADMIN.
FPMR (41 CFR) 101-43.311

**REPORT OF EXCESS PERSONAL PROPERTY**

1. REPORT NO.
2. DATE MAILED
3. TOTAL COST
$

4. TYPE OF REPORT (Check one only of "a," "b," "c," or "d")
a. ORIGINAL
b. CORRECTED
c. PARTIAL
d. TOTAL W/D
(Also check "e" and/or "f" if appropriate)
e. OVERSEAS
f. CONTRACTORS INV.

5. TO (Name and Address of Agency to which report is made) THRU

6. APPROPR. OR FUND TO BE REIMBURSED (If any)

7. FROM (Name and Address of Reporting Agency)

8. REPORT APPROVED BY (Name and Title)

9. FOR FURTHER INFORMATION CONTACT (Title, Address and Telephone No.)

10. AGENCY APPROVAL (If applicable)

11. SEND PURCHASE ORDERS OR DISPOSAL INSTRUCTIONS TO (Title, Address and Telephone No.)

12. GSA CONTROL NO.

13. FSC GROUP NO.
14. LOCATION OF PROPERTY (If location is to be abandoned, give date)
15. REIM. REQD — YES / NO
16. AGENCY CONTROL NO.
17. SURPLUS RELEASE DATE

EXCESS PROPERTY LIST

| ITEM NO. (a) | DESCRIPTION (b) | COND (c) | UNIT (d) | NUMBER OF UNITS (e) | ACQUISITION COST PER UNIT (f) | ACQUISITION COST TOTAL (g) | FAIR VALUE % (h) |
|---|---|---|---|---|---|---|---|
| | | | | | | | |

STANDARD FORM 120 REV.
APRIL 1957 EDITION

(Use Standard Form 120A for Continuation Sheets)
NSN 7540-00-634-4074

PREVIOUS EDITION USABLE

# Appendix C - Acronyms and Abbreviations

| | |
|---|---|
| GAO | Government Accountability Office |
| NARA | National Archives and Records Administration |
| OIG | Office of Inspector General |
| PII | Personally Identifiable Information |
| NGC | Office of General Counsel |
| NA | Office of Administration |
| NAA | Acquisition Services Division |
| NL | Office of Presidential Libraries |
| NR | Office of Regional Records Services |
| NH | Office of Information Services |
| NHT | Information Technology Services Division |
| NAF | Facilities and Personal Property Management Division |
| NWL | Center for Legislative Archives |

# Appendix D - Management's Response to the Report

NATIONAL ARCHIVES

ARCHIVIST *of the* UNITED STATES

DAVID S. FERRIERO
T: 202.357.5900
F: 202.357.5901
*david.ferriero@nara.gov*

17 March 2011

To: Paul Brachfeld, Inspector General
From: David S. Ferriero, Archivist of the United States
Subject: Audit 11-07, Audit of NARA's Photocopier Security

Thank you for the opportunity to comment on this draft report. We appreciate the willingness of the auditor to meet and discuss corrections and changes to some of the language in the report. This report includes seven recommendations. We concur with all seven recommendations and have already begun working to contain some of the problems noted in the draft report.

If you have questions about these comments, please contact Mary Drak at mary.drak@nara.gov or by phone at 301-837-1668.

David S. Ferriero
Archivist of the United States

NATIONAL ARCHIVES *and* RECORDS ADMINISTRATION
700 PENNSYLVANIA AVENUE, NW
WASHINGTON, DC 20408-0001
*www.archives.gov*

# Appendix E - Report Distribution List

Archivist of the United States
Deputy Archivist of the United States
Assistant Archivist, Office of Administration (NA)
Chief of Staff
Management Control Liaison, Policy and Planning (NPOL)
Office of General Counsel (NGC)