



|                            |
|----------------------------|
| Issue Date<br>May 03, 2012 |
|----------------------------|

|                                     |
|-------------------------------------|
| Audit Report Number<br>2012-KC-0002 |
|-------------------------------------|

TO: Karen Newton Cole, Acting Chief Human Capital Officer, A

//signed//

FROM: Ronald J. Hosking, Regional Inspector General for Audit, 7AGA

SUBJECT: HUD Did Not Implement Adequate Policies and Procedures for Sanitizing Media in Its Multifunction Devices

## **HIGHLIGHTS**

### **What We Audited and Why**

We audited the U.S. Department of Housing and Urban Development's (HUD) Office of the Chief Human Capital Officer based on concerns about security risks of hard drives in multifunction devices. Our objective was to determine whether HUD had documented and implemented procedures to effectively remove sensitive data from the hard drives of multifunction devices before disposing of them.

### **What We Found**

HUD did not monitor or test the overwrite process for multifunction devices to ensure that the process effectively sanitized data from multifunction device hard drives. It also did not have a detailed plan in place to ensure proper sanitization of the devices' hard drives before disposal.

## **What We Recommend**

We recommend that the Chief Human Capital Officer develop and implement a plan to monitor and test HUD's overwrite process for hard drives on its multifunction devices to ensure that the process is effective. We also recommend that the Chief Human Capital Officer develop and implement a plan to ensure that all sensitive data are effectively sanitized from the hard drives of its multifunction devices before they are disposed of.

For each recommendation without a management decision, please respond and provide status reports in accordance with HUD Handbook 2000.06, REV-4. Please furnish us copies of any correspondence or directives issued because of the audit.

## **Auditee's Response**

HUD agreed with our finding and recommendations. We provided the draft report to HUD on March 7, 2012 and requested a response by April 6, 2012. It provided written comments on May 2, 2012.

The complete text of the auditee's response can be found in appendix A of this report.

# TABLE OF CONTENTS

---

|   |    |
|---|----|
| Background and Objective  | 4  |
| Results of Audit  |    |
| Finding : HUD Did Not Implement Adequate Policies and Procedures for<br>Sanitizing Media in Its Multifunction Devices | 5  |
| Scope and Methodology   | 8  |
| Internal Controls   | 9  |
| Appendix  |    |
| A. Auditee Comments   | 10 |
| B. Criteria   | 12 |

## **BACKGROUND AND OBJECTIVE**

---

The Office of the Chief Information Officer at the U.S. Department of Housing and Urban Development (HUD) was established on December 1, 1998. HUD's Chief Information Officer reports to the Office of the HUD Secretary or Deputy Secretary and advises the Secretary, Deputy Secretary, and other HUD senior managers on the strategic use of information technology to support core business processes and achieve mission-critical goals. One of the Office of the Chief Information Officer's primary responsibilities is to develop and implement information technology policy.

The Office of the Chief Human Capital Officer is led by the Chief Human Capital Officer. The Chief Human Capital Officer is assisted by the Deputy Chief Human Capital Officer. They provide overall policy and strategic direction for the Office, which is comprised of several components. One of these is the Office of Facilities Management Services.

The Office of Facilities Management Services provides a diverse array of key support services to headquarters and the field, including real and personal property management, fleet management, building operations, energy and environmental management, headquarters transportation services, lock and key services, parking management, telecommunications management, safety and health program management, records management, mail distribution and management, printing and graphics services, and development and issuance of departmental policy for administrative services. It is responsible for carrying out the Office of the Chief Information Officer's information technology policies and procedures with regard to printing equipment.

HUD headquarters is under a 5-year contract with Xerox for more than 300 multifunction devices, which expires in March 2013. There are several different contracts for multifunction devices in HUD's field offices, not all of which involve Xerox machines. HUD staff told us that no multifunction machines had been disposed of.

Our audit objective was to determine whether HUD had documented and implemented procedures to effectively remove sensitive data from the hard drives of multifunction devices before disposing of them.

## RESULTS OF AUDIT

---

### Finding: HUD Did Not Implement Adequate Policies and Procedures for Sanitizing Media in Its Multifunction Devices

HUD did not monitor or test the overwrite process for its multifunction devices and did not have a detailed plan in place to ensure proper sanitization of the devices' hard drives before disposal. This condition occurred because HUD staff in the Office of the Chief Human Capital Officer disagreed with the Office of the Chief Information Officer over which office was responsible for ensuring its hard drives were properly sanitized. As a result, HUD could not be assured that its overwrite process effectively removed data from the hard drives, and sensitive data could be at risk.

---

#### **HUD Did Not Monitor or Test the Overwrite Process**

HUD did not implement policies and procedures for media sanitization. It did not monitor or test the overwrite process for its multifunction devices to ensure that the process effectively sanitized data from its multifunction device hard drives. The Office of the Chief Information Officer had written policies and procedures stating that HUD was required to

- Sanitize all information system media before disposal or release for reuse;
- Track, document, and verify media sanitization actions; and
- Periodically test sanitization equipment and procedures to ensure correct performance.

HUD and information systems contractor staff told us that the hard drives in the multifunction devices were overwritten every night and that the overwrite process removed all of the data from the hard drives. The overwrite process was set up at the time the machines were installed, and each machine printed out a report every morning stating whether the overwrite process was successful. There was no process in place to use the reports for monitoring the overwrite process, and the machines were about to begin the last year of a 5-year contract that expires on March 6, 2013.

HUD's Xerox representative told us that to be most efficient, the machines should be set to immediately overwrite each job after it completes. The Xerox representative also told us that the machines can be overwritten on demand, using a menu on the machine but that HUD cannot wait until the day the leased machines go back to Xerox to perform this function. The overwrite process takes 20-30 minutes to complete and is not always successful the first time. Therefore

it could take twice that long to overwrite the machine, which is not feasible while machines are being switched out.

The Xerox representative gave an example of a customer with 147 machines, who tried to overwrite them as they left the facility. The Xerox representative said that the operation was a nightmare and ultimately unsuccessful because all of the machine hard drives were not overwritten. HUD has nearly 300 machines in headquarters on one contract.

HUD recently changed the settings on the machines as a result of our audit work. HUD's information technology contractor set the overwrite process to be performed after each job in addition to the nightly overwrite process. The immediate overwrite function was recommended by the Xerox representative; however, HUD had not tested the overwrite process and could not be assured that it effectively removed data from the hard drives.

### **HUD Did Not Have a Detailed Disposal Plan in Place**

HUD did not have a detailed plan in place to ensure proper sanitization of the devices' hard drives before disposal. HUD staff had researched what options were available and had discussed the options internally, but did not finalize a plan for disposing of the hard drives at the end of the lease. The HUD staff we spoke with generally agreed that the best way to secure the data on multifunction hard drives is to retain the hard drives at the end of the lease and have them physically destroyed by shredding them. However, no official decision had been made on how to handle the hard drives at the end of the lease.

Retaining the hard drives is the most expensive way to secure the data. Xerox officials told us that the hard drives cost about \$350 each and that a few of the more complex machines contained two hard drives. They said that this cost would be in addition to the cost of the contract. The cost of the shredding process is also not included in the contract. HUD staff told us that HUD did not have the proper equipment to shred the hard drives and a contractor would have to be hired to perform the function.

### **HUD Staff Disagreed Over Responsibilities**

HUD staff in the Office of the Chief Human Capital Officer disagreed with the Office of the Chief Information Officer over which office was responsible for monitoring, testing, and sanitation of data. One of the primary responsibilities of

the Office of the Chief Information Officer is to develop and implement information technology policy; however, it is up to the Office of the Chief Human Capital Officer to carry out the policy because it is responsible for managing the multifunction machines.

### **Sensitive Information Could Be at Risk**

HUD could not be assured that its overwrite process effectively removed data from its hard drives, and sensitive data could be at risk. HUD did not monitor the nightly overwrite process, but even if the process was successful, data could be on the devices the day they are taken out of service because print, fax, copy, and scan jobs may be performed the same day the machine is returned to Xerox. HUD needs to develop and implement a disposal plan for the machines to ensure that they are not returned with sensitive information on the hard drives.

### **Recommendations**

We recommend that the Chief Human Capital Officer work with the Chief Information Officer to

- 1A. Develop and implement a plan to monitor and test HUD's overwrite process for hard drives on its multifunction devices to ensure that the process is effective.
- 1B. Develop and implement a plan to ensure that all sensitive data are effectively removed from the hard drives of its multifunction devices before they are disposed of.

## SCOPE AND METHODOLOGY

---

Our review generally covered the period October 1, 2009, through September 30, 2011. We performed onsite work from November 2011 through January 2012 at HUD headquarters at 451 7<sup>th</sup> Street Southwest, Washington, DC.

To accomplish the audit objective, we

- Reviewed HUD's handbooks and information technology security procedures.
- Reviewed the National Institute of Standards and Technology's Recommended Security Controls for Federal Information Systems and Organizations.
- Reviewed the Code of Federal Regulations.
- Reviewed HUD's contract for multifunction devices.
- Conducted interviews with staff from HUD's Office of the Chief Information Officer, Office of the Chief Human Capital Officer, and information technology contractor and representatives from the Xerox Corporation.

We did not use or rely on computer-processed data to support our audit conclusions. In addition, we did not perform testing on the multifunction device hard drives.

We conducted the audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objective. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objective.



# INTERNAL CONTROLS

---

Internal control is a process adopted by those charged with governance and management, designed to provide reasonable assurance about the achievement of the organization's mission, goals, and objectives with regard to

- Effectiveness and efficiency of operations,
- Reliability of financial reporting, and
- Compliance with applicable laws and regulations.

Internal controls comprise the plans, policies, methods, and procedures used to meet the organization's mission, goals, and objectives. Internal controls include the processes and procedures for planning, organizing, directing, and controlling program operations as well as the systems for measuring, reporting, and monitoring program performance.

---

## Relevant Internal Controls

We determined that the following internal controls were relevant to our audit objective:

- Controls to ensure compliance with the Office of the Chief Information Officer's policies and procedures for media sanitization.
- Controls for sanitizing sensitive data when disposing of multifunction devices.

We assessed the relevant controls identified above.

A deficiency in internal control exists when the design or operation of a control does not allow management or employees, in the normal course of performing their assigned functions, the reasonable opportunity to prevent, detect, or correct (1) impairments to effectiveness or efficiency of operations, (2) misstatements in financial or performance information, or (3) violations of laws and regulations on a timely basis.

## Significant Deficiencies

Based on our review, we believe that the following items are significant deficiencies:

- HUD did not have controls in place to ensure that it complied with testing and monitoring requirements for the overwrite process for its multifunction devices.
- HUD did not have controls in place to ensure that it had a sanitization plan for the multifunction devices before disposal.

# APPENDIXES

## Appendix A


### AUDITEE COMMENTS



U.S. DEPARTMENT OF HOUSING AND URBAN DEVELOPMENT  
WASHINGTON, DC 20410-3000

CHIEF HUMAN CAPITAL OFFICER

MAY - 1 2012

MEMORANDUM FOR: Ronald J. Hosking, Regional Inspector General for Audit, 7AGA  
FROM:   
Karen Newton Cole, Acting Chief Human Capital Officer, A  
SUBJECT: HUD Did Not Implement Adequate Policies and Procedures for  
Sanitizing Media in Its Multifunction Devices

The Office of the Inspector General (OIG) audited the U.S. Department of Housing and Urban Development's (HUD) Office of the Chief Human Capital Officer (OCHCO) concerning the security risks involving hard drives in multifunctional devices. Their objective was to determine whether HUD had documented and implemented procedures that incorporated the effective removal of sensitive data left on hard drives of multifunctional devices before disposal.

The OCHCO appreciates the opportunity to respond to the OIG's audit report on the plan for disposal of hardware drives in multifunctional devices.

The OIG recommends the OCHCO develop and implement a plan to monitor and test the hard drive overwrite process, currently utilized by HUD on its multifunctional devices, to ensure the process is effective. They also recommend the OCHCO develop and implement a plan to ensure that all sensitive data are effectively sanitized from the hard drives of its multifunctional devices before disposal of the devices.

The OCHCO is currently solidifying a plan to monitor and test the current overwrite process for hard drives on its multifunctional devices. OCHCO will request assistance from the Office of the Chief Information Officer (OCIO) to ensure this process is effective.

Office of the Chief Human Capital Officer's information security plan for multifunctional devices will include:

1. Procuring the services of the current vendor to sanitize the hard drives on each multifunctional device and certify that all machines have been wiped according to DOD 5220.22-M or better standards at the end of the current contract.
2. Login Security/HSPD12 Card Enablement – to protect all data by controlling who has access to use the device.
3. SSL/TLS Encryption of data – to protect the data while it moves through the machine.
4. Immediate and scheduled image overwrite DOD 5220.22-M or better – to ensure all data has been removed after each job and will include periodic random testing to ensure the process is effective.

[www.hud.gov](http://www.hud.gov)

[espanol.hud.gov](http://espanol.hud.gov)

These requirements will be placed in the new contracted lease beginning in 2013 and accordingly, the OCHCO in conjunction with the OCIO will ensure the settings are enacted as intended.

If you have any questions, please contact Michael Schimmenti, Director, Office of Facilities Management Services, at (202) 402-7325.

## Appendix B

### CRITERIA

---

HUD Handbook 2400.25, REV-2, CHG-1, section 4.7.6, states that HUD must:

- Sanitize information system media, both digital and non-digital, prior to disposal or release for reuse.
- Track, document, and verify media sanitization actions.
- Periodically test sanitization equipment and procedures to ensure correct performance.

HUD Handbook 2400.25, REV-2, CHG-1, section 4.7.6, also states that program offices and system owners shall ensure that any sensitive information stored on media that will be surplus or returned to the manufacturer shall be purged from the media before disposal.