UNITED STATES GOVERNMENT
FEDERAL COMMUNICATIONS COMMISSION
OFFICE OF INSPECTOR GENERAL

MEMORANDUM

DATE: October 31, 2011

TO: Managing Director

FROM: Inspector General

SUBJECT: Report on Inspection of FCC Digital Printers, Copiers and Scanners

The Office of Inspector General (OIG) has completed an inspection of the Federal Communications Commission's (FCC) policies and procedures for ensuring that digital copiers, printers or scanners, when going off lease or being de-accessioned, contain no sensitive, confidential, or personal data.

Our inspection found that the FCC has implemented some policies and processes to ensure that digital copiers, printers or scanners, when going off lease or being de-accessioned, contain no FCC or corporate sensitive data, or personally identifiable information (PII), however, these procedures need to be formalized and finalized.

The results of this inspection were discussed with FCC management and staff knowledgeable with the FCC digital copiers and their comments have been incorporated them into this report. The comments received were in agreement with the report's conclusions. This report is being issued in final and no response is required.

If you have any questions, please contact me at (202) 418-1522 or William Garay, Assistant Inspector General for Audit at (202) 418-7899.

cc: Chief of Staff
Chief Information Security Officer
Performance Evaluation and Records Management (PERM)

FEDERAL COMMUNICATIONS COMMISSION

OFFICE OF INSPECTOR GENERAL

INSPECTION REPORT
DIGITAL PRINTER, COPIER, AND SCANNER INSPECTION

Report No. 11-EVAL-02-01
September 9, 2011

TABLE OF CONTENTS

Summary

This report presents our findings and recommendations based on our inspection of the Federal Communications Commission's (Commission, or FCC) policies and procedures for ensuring that digital copiers, printers or scanners, when going off lease or being de-accessioned, contain no sensitive, confidential, or personal data.

We conducted our inspection under the authority of the *Inspector General Act of 1978*, as amended, and according to "Quality Standards for Inspection and Evaluation," January 2011, issued by the Council of the Inspectors General on Integrity and Efficiency.

A draft copy of this inspection report was provided to FCC management and staff knowledgeable with the FCC digital copiers for their comments. We received comments and incorporated them into the report. The comments received were in agreement with the report's conclusions.

Objective, Scope, and Methodology

The objective of our inspection was to determine whether the Commission had established and implemented policies and procedures to ensure that digital copiers, printers or scanners, when going off lease or being de-accessioned, contained no FCC or corporate sensitive data, or personally identifiable information (PII).

The scope of our inspection was applicable FCC policies and procedures that address digital copiers, printers or scanners. The methodology included discussion with staff and management, review of current FCC policies and procedures, review of the current FCC copier Statement of Work (SOW), review of Xerox security webpages and documents, and the observation of Xerox multifunction peripheral (MFP) devices and network printers along with their configuration settings.

There were no prior inspections or audits of this area performed.

Criteria

The criteria for this inspection included:

NIST Special Publication 800-53 Revision 3, *Recommended Security Controls for Federal Information Systems*, states:

> MP-1 MEDIA PROTECTION POLICY AND PROCEDURES
>
> Control: The organization develops, disseminates, and reviews/updates [*Assignment: organization-defined frequency*]:

a. A formal, documented media protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

b. Formal, documented procedures to facilitate the implementation of the media protection policy and associated media protection controls.

MP-6 MEDIA SANITIZATION

Control: The organization sanitizes information system media, both digital and non-digital, prior to disposal, release out of organizational control, or release for reuse.[1]

Conclusion

We found that the FCC had not formally documented the FCC baseline secure configuration for the Xerox MFP devices.

The FCC has issued the Interim Cyber Security Policy, which, in paragraph 2.12 *Contracting*, addresses digital copiers. However, even though this policy proactively addresses security in the procurement process, this interim policy does not address policy and procedures for the baseline secure configuration of digital copiers before they are connected to the production network.

The FCC has implemented informal processes which ensure that digital copiers, printers or scanners, when going off lease or being de-accessioned, contain no FCC or corporate sensitive data, or personally identifiable information (PII).

We make recommendations at the end of this report that address these conclusions.

Background

Investigative news reports have revealed instances where companies and government agencies have returned leased copiers that still contained sensitive data. The objective of this inspection was to determine whether the Commission had established policies and procedures to ensure that digital copiers, printers or scanners, when going off lease or being de-accessioned, contain no FCC or corporate sensitive data, or PII.

[1] Pursuant to the Federal Information Security Management Act of 2002 (“FISMA”), federal agencies are required to follow the recommendations in NIST Special Publication 800-53 Revision 3, *Recommended Security Controls for Federal Information Systems*, August 2009, by the Federal Information Processing Standards Publication 200, *Minimum Security Requirements for Federal Information and Information Systems*, March 2006 (“FIPS PUB 200”).

Current FCC Processes

The FCC took action regarding digital copier security in May 2010 and enabled data protection regarding MFP devices, which are digital copiers, scanners, and printers.

These informal procedures included:

1) Daily image overwrite (3X) of all image data from disk or other non-volatile storage, including any pending jobs.

> FCC has configured these MFP devices to automatically and immediately overwrite the data as soon as printing is complete. This overwrite also occurs every 24 hours. Pending jobs refer to print jobs that have been spooled to the MFP device using the Secure Print option. Until the person who spooled this Secure Print job comes to the MFP device and enters his or her user name and PIN to print the job, it is a pending job. If a Secure Print job is not printed within 24 hours of having been spooled, it is overwritten.

2) Encryption on all FCC MFP devices to ensure all FCC users are protected.

> Xerox also provides a data encryption feature that, when enabled, encrypts all stored data with an AES 128-bit encryption algorithm.

3) When Xerox MFP devices are due for return, the hard drives are removed (by the vendor) before the MFP device leaves FCC facilities. These hard drives are then given to IT, stored for proper disposal, and then destroyed. The FCC contracts for MFP devices with removable hard drives, specifically, so that at the end of the lease term these hard drives can be removed and then destroyed.

When the Xerox MFP device configuration was first defined by a workgroup, no formal documentation of the Xerox MFP device configuration was issued.

The procedures for configuring the Xerox MFP devices are not documented by the FCC because the procedures describing how to securely configure the Xerox MFP devices are in the Xerox MFP device manuals.

Formally documenting the FCC standard secure configuration for the Xerox MFP devices has not been performed. Specifically, there is no list of what changes are made to the default settings. For example, the default email function is turned off.

During the course of this inspection, we determined that only the Xerox MFP devices contain hard drives.

When FCC Information Technology Center (ITC) staff was interviewed, they stated that FCC network printers do not have hard drives. The result of a random selection of 12 network printers' configuration files showed that none of the sampled network printers had hard drives. While making these observations, we noted that within FCC headquarters, the most common MFP devices are the Xerox 4110 and the Xerox Workcentre 7655. The most common network printer is the Xerox Phaser 4500.

Copier Contract and Statement of Work (SOW)

The current Xerox contract (FCC-RFQ-11000012) has various contract clauses/sections that reflect hard drive removal and data overwrite.

The current copier SOW contains copier specification clauses that require

> "Secure Print, Image Overwrite up to 3 times, Data Encryption (SSL/TLS), Removable Hard Disk Drive, Disk Overwrite, IPV6 compliant, IP filtering"

This clause reflects data sanitization and/or hard drive removal requirements.

Currently, the FCC is transitioning from the old copier contract to a new copier contract. Normally, based on ITC feedback, the vendor provides one of the new MFP devices one week in advance of the delivery of all the others, so that the ITC can define and securely configure that one. All the other MFP devices are then securely configured the same as the first one. Currently, the ITC does not formally document this baseline secure configuration. Thoroughly documenting it would prevent baseline inconsistencies.

FCC Cyber Security Program, Interim Cyber Security Policy

In July 2011, the FCC Cyber Security Program issued the Interim Cyber Security Policy, Version 2.0, effective date July 15, 2011, which addresses contracting for leased computers, printers, or copiers. This interim policy contains language addressing the digital copier security issue. Specifically:

> **2.12 Contracting**
>
> FCC relies on contractor support for administrative, technical and subject matter expertise. Additionally, FCC contracts purchase and leases of computer and other electronic equipment such as printers, scanners, and copiers. As solicitations for contracts are released, they should include, at a minimum:
>
> ....
>
> - For leased computers and printers or copiers with hard drives, contract clause should state that all hard drives and removable media remain the property of FCC at lease end, or that all data to be removed by FCC personnel prior to lease termination.

However, even though this policy proactively addresses security in the procurement process, this interim policy does not address policy and procedures for the baseline secure configuration of digital copiers before they are connected to the production network.

Xerox Product Security Features

As a result of this inspection, we determined that some of the product security features that Xerox offers include:

Disk Encryption – Uses AES 128-bit encryption (or AES 256-bit depending on model) to secure data at rest.

On Demand Image Overwrite – Executed prior to removal or as needed to remove all image data from disk or other non-volatile storage.

Immediate Image Overwrite – Automatically executed immediately after jobs are completed to remove image data from disk or other non-volatile storage.

Scheduled Image Overwrite – Automatic, daily overwrite of all image data from disk or other non-volatile storage including any pending jobs.

Hard Drive Retention Service – Xerox has what it calls the Hard Drive Retention Service. This service allows the customer, for a fee, to retain their hard drive(s) and sanitize or destroy them in a manner consistent with internal policies or regulatory standards.

We noted for some of the copiers and printers at FCC Headquarters, the following features were offered:

The WorkCentre 7655 uses a hard drive for all imaging functions. Image Overwrite and disk encryption are included as standard features.

The Xerox 4110 uses a hard drive for all imaging functions. An optional Security kit that includes Image Overwrite and Encryption features is available. An optional Removable Hard Drive kit may be available. Overwrite is not enabled by default. Encryption of image data in the print engine is not enabled by default.

The Phaser 4500 does not use a hard drive for printing, unless the optional hard drive has been installed. Image Overwrite is installed, but disabled by default. Disk Encryption is available, but the default state is no encryption.

Finally, attached as an appendix is a listing of security features offered on Xerox products.

Findings and Recommendations

1. Finding: The FCC has not formally documented the FCC baseline secure configuration for the Xerox MFP devices.

   Recommendation: The FCC should formally document the FCC baseline secure configuration for the Xerox MFP devices.

2. Finding: The FCC has issued the Interim Cyber Security Policy, which addresses digital copiers. However, even though this policy proactively addresses security in the procurement process, this interim policy does not address policy and procedures for the baseline secure configuration of digital copiers before they are connected to the production network.

   Recommendation: FCC should finalize the FCC Cyber Security Policy, and consider updating it to reflect policy and procedures for establishing, documenting, and implementing the baseline secure configuration of digital copiers before they are connected to the production network. Also, the FCC should consider including additional copier security features language, along with coordinating with the Contracts and Purchasing Center (CPC) for copier security requirements language for new procurements.

3. Finding: While the FCC has implemented informal processes, the FCC has not implemented and documented formal processes which ensure that digital copiers, printers or scanners, when going off lease or being de-accessioned, contained no FCC or corporate sensitive data, or PII.

   Recommendation: The FCC should formally document the processes which ensure that digital copiers, printers or scanners, when going off lease or being de-accessioned, contained no FCC or corporate sensitive data, or PII.

Appendix I – Xerox Product Security Features

Extract from Xerox Product Security Webpage

Source: http://www.xerox.com/information-security/product-security/enus.html

Specific security features on Xerox devices include:

Image Overwrite Option: The Image Overwrite security option electronically shreds information stored on the hard disk of devices as part of routine job processing. Electronic erasure can be performed automatically at job completion (Immediate), On Demand, and on some models Scheduled. The Xerox Image Overwrite security process implements a three-pass algorithm originally specified by the U.S. Department of Defense.

Data Encryption: All data in motion in and out of the device, as well as data stored within the device, is secured with state of the art encryption. Most Xerox devices support several different protocols for encrypting data in motion in and out of the device including SSL and IP Security (IPSec). Note that scanning, printing, and access to the Web/remote user interface can be secured with either SSL/TLS or IPSec.

Access Security Software Page: Unified ID System integrates your Xerox multifunction systems with your existing employee/student ID badge solution to provide a flexible and convenient authentication system. Users simply log-in with a swipe of their magnetic or proximity ID card for secure access to MFP system functions that need to be tracked for accounting or regulatory requirements.

Embedded Fax: While firewalls work at the network periphery to prevent unauthorized access to a customer's environment, unprotected fax connections in multifunction devices can be an open "back door" into the network. Xerox was the first manufacturer to offer a Common Criteria certified product that assures complete separation of the fax telephone line and the network connection, and continues to include that claim in all product certifications.

Xerox Standard Accounting: When enabled on Xerox office printers and multifunction devices, this feature monitors the print, copy, scan and fax pages produced and who produces them. Administrators can limit the number of print, copy, scan and fax jobs a user can perform, track activity at a user, group or department level, and manage access to color copying and printing.

User Authorization: Use of device functions (e.g., scan, e-mail and fax) can be restricted by user and by function according to access control lists set by the System Administrator.

Secure Print: When sending a job from a print driver or using the web print submission tool, the user selects the Secure Print method and enters a unique PIN number. Jobs are sent and safely stored at the device until the user enters that same unique PIN to release them. This controls unauthorized viewing of hard copy documents sent to the printer.

Extensible Interface Platform® (EIP): A labor saving feature for office and multifunction devices, this allows document-related software applications to be accessed on the user interface to improve workflow and minimize time at the device.

Removable Hard Disk Drive Accessory/Kit: Removable Hard Drive Kits are only supported on some Production High Volume systems which allow the System Administrator to quickly and easily remove hard drives and lock them up. This eliminates the risk of unauthorized access when the device is unattended or is powered off at end of day. This capability is helpful for customers who print data that is subject to legal regulations (e.g., HIPAA, PCI) or might have a Variable Input Printing database containing sensitive information.

Access Control: Most customers need to restrict access to a device to a limited set of authorized users and Operators. Xerox production devices include access control features such as:

> **Authentication Feature:** This feature ensures that only properly authorized users are permitted to use a Production device. Any type of interaction between a user and a Xerox production device is associated with a security account. The association, or logon session, is the basis for granting access to any user. Once the logon session is established, the user can interact with the printer or access customer data, subject to restrictions based on the user's Role.
>
> **Role Based Access Control (RBAC):** The RBAC feature ensures that authenticated users are assigned to a role of User, Operator, or Administrator. Each role has associated privileges with appropriate levels of access to features, jobs and print queue attributes.
>
> **Microsoft Active Directory Services:** The Microsoft Active Directory Services (ADS) feature enables the device to authenticate user accounts against a centralized user account database, instead of exclusively using the user account database that is managed locally at the device.

Network Security:

Many Xerox devices also include features to protect the printer from unauthorized remote access and to protect the confidentiality of “data in motion”, specifically customer jobs which are transmitted to the printer over a network. These features include:

IPFiltering: Internet Protocol (IP) Filtering capability enables a system administrator to restrict access to the device to a limited set of IP addresses. This provides a defense against remote attackers. Computers whose IP addresses are outside of the allowed set are not permitted to access the device.

IPSec: Internet Protocol (IP) Security enables the digital front end or printer device to authenticate remote users and requires these users to encrypt the data transmitted using legacy print protocols such as LPR and Port 9100. IPSec is supported by a variety of PC operating systems including all modern versions of Microsoft Windows.

Secure Socket Layer/Transport Layer Security (SSL/TLS): The SSL/TLS feature provides protection of customer confidential data transmitted over a network when using the HTTP protocol (e.g., Web Print client).

Digital Certificate: The Digital Certificate feature enables the system administrator to create a self-signed digital certificate, or import a digital certificate signed by a Certificate Authority (e.g., RSA, VeriSign). A digital certificate enables print clients to authenticate a printer/print server and to encrypt data using SSL/TLS.

Network Authentication: Access to device functions (e.g., scan, e-mail and fax) is restricted by validating network user names and passwords prior to use of these functions.

802.1x Device Authentication: Office devices implement the 802.1x standard. This allows the device to be authenticated on a network before the network will allow any network traffic to pass to or from the device. This stops rogue devices from infiltrating the network.