December 9, 2015

Performance Audit

Printer/Copier Security

Citywide

Report No. 15-104

CITY OF ALBUQUERQUE
OFFICE OF INTERNAL AUDIT

PERFORMANCE AUDIT REPORT
PRINTER/COPIER SECURITY
CITYWIDE
REPORT NO. 15-104

TABLE OF CONTENTS

City of Albuquerque - Office of Internal Audit

Printer/Copier Security

Performance Audit **12/9/2015** Audit #15-104

The purpose of this audit was to review the Department of Technology and Innovation (DTI) policies and procedures governing the security of networked printer/copiers and to ascertain whether these devices were secured in conformance with recommended practices. The audit was included in the fiscal year (FY) 2015 audit plan.

Executive Summary

Printers and copiers are standard office equipment in all City departments. Today's printer/copiers are sophisticated multifunction devices that can send emails, scan and save documents, and send faxes. To manage these tasks, the devices have onboard computer operating systems and hard drives, and are connected to the City's network to process multiuser requests.

While enhancing productivity, these devices introduce risks to a networked computing environment. Documents processed by the devices are saved on the hard drive. If not programmed to erase these files, there is a risk that documents containing sensitive data can be retrieved and reprinted by an unauthorized party at a later time.

DTI has issued a procedure for securing networked printer/copiers, but awareness of the procedure has not been communicated effectively to City departments. Many Citywide printer/copiers have security features that have not been activated, increasing the risk of unauthorized use or release of confidential information. No evidence of any data breach related to printer/copiers came to our attention during the audit.

DTI agrees with the recommendations and will work with City Departments to enhance security of Citywide printer/copiers, develop an inventory of networked printers/copiers, and to strengthen communication of IT security standards.

Recommendations & Benefits

• • •

By following the recommendations in this report, DTI will:

- Enhance security of networked printer/copiers against misuse,
- Improve management of printer/copiers with a master listing of devices,
- Enhance consistency in purchases, leases, and maintenance contracts for printer/copiers,
- Improve communication of IT security policies, and
- Enhance security of networked printer/copiers and other multifunction devices.

City of Albuquerque

Office of Internal Audit

December 9, 2015

Accountability in Government Oversight Committee
P.O. Box 1293
Albuquerque, New Mexico 87103

Audit: Performance
Printer/Copier Security – Citywide
Audit No. 15-104

FINAL

INTRODUCTION

The Office of Internal Audit (OIA) conducted a performance audit of internal controls over Printer/Copier Security. The audit was included in OIA's fiscal year (FY) 2015 audit plan. The audit objectives, scope, and methodology can be found in **Appendix A**.

The audit only considered printer/copiers connected to the City's computer network, which is managed by the Department of Technology and Innovation (DTI). DTI is responsible for developing security policy for the computer network and other centrally-managed technology assets. Non-networked printer/copiers were outside the scope of this audit.

This performance audit considered risks associated with storage of sensitive documents on printer/copiers containing hard drives. Although the audit considered controls designed to prevent risks associated with data breaches, no evidence of any data breach related to printer/copiers came to our attention during the audit.

BACKROUND

Printers and copiers are standard office equipment in all City of Albuquerque (City) departments. Today's printer/copiers are sophisticated multifunction devices which are shared by entire offices. Beyond simply printing or copying documents, these devices can send emails, scan and save documents, send faxes, and produce complex print jobs. To accomplish these tasks, the printer/copiers have onboard computer operating systems capable of accepting, managing, and sequencing simultaneous requests from multiple users. Although feature-rich, these devices also

present security risks in a networked environment. Security features are available, but activation of the features is strictly the customer's responsibility.

Since 2002, most multifunction printer/copiers contain hard drives, which are similar to those on a personal computer. When a print or copy request is sent to a multifunction printer/copier, an image of the document is saved to the device's hard drive. The saved image is then used to generate printed copies of the document, or send the image in an email or fax.

Unless securely erased, a multifunction printer/copier hard drive may retain images of all documents processed by the device for months or years after the print or scan request. Without proper erasure of multifunction printer/copier hard drives, confidential or sensitive information processed by City multifunction printer/copiers may be reprinted by an unauthorized party at a later time, which could make the City liable for fines or legal penalties, or harm the City's reputation.

Due to the concerns noted, manufacturers of printers, copiers, and other multifunction devices have introduced security features intended to protect the devices from potential attack and reduce the risk that images stored on printer/copier hard drives can be reprinted at a later time. However, these features are only turned on if the customer requests that they be activated and there is frequently additional cost to activate the features.

There are numerous printer/copiers connected to the City's network. Some are owned by the City and others are leased from local vendors. The printer/copiers vary in their data storage capacity and security features.

FINDINGS

The following findings concern areas that OIA believes could be improved by the implementation of the related recommendations.

1. DTI SHOULD DEVELOP A WRITTEN PLAN TO ACTIVATE SECURITY SETTINGS ON NETWORKED PRINTER/COPIERS.

   Printer/copiers on the City's network have not been optimally secured against unauthorized access. Although the department published a Citywide Security Procedure, *Information Technology Protection – Guide to Securing Networked Printers, Scanners, Copiers, and Faxes* on July 1, 2014, compliance with the procedure is voluntary and not enforced.

   New printers, copiers, scanners, faxes, and other multifunction devices are generally

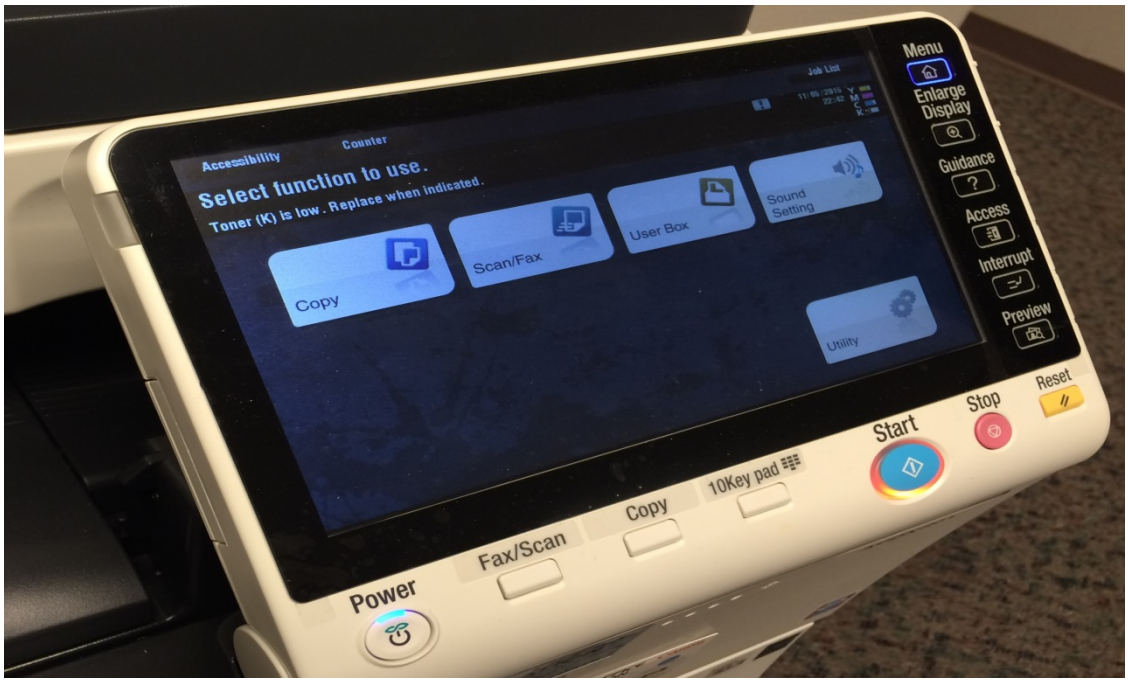
delivered to the requesting department and setup by vendors. There often is no interaction with DTI during the initial setup phase. Priority is given to getting the device up and running.

Since department personnel are often not aware of the security risks posed by modern printer/copiers, security considerations are often overlooked. Not activating a device's onboard security features puts the City at risk:

- The device may be accessed by an unauthorized party,
- Normal printing and copying functions may be disrupted, or
- Sensitive information being processed by the device may be exposed.

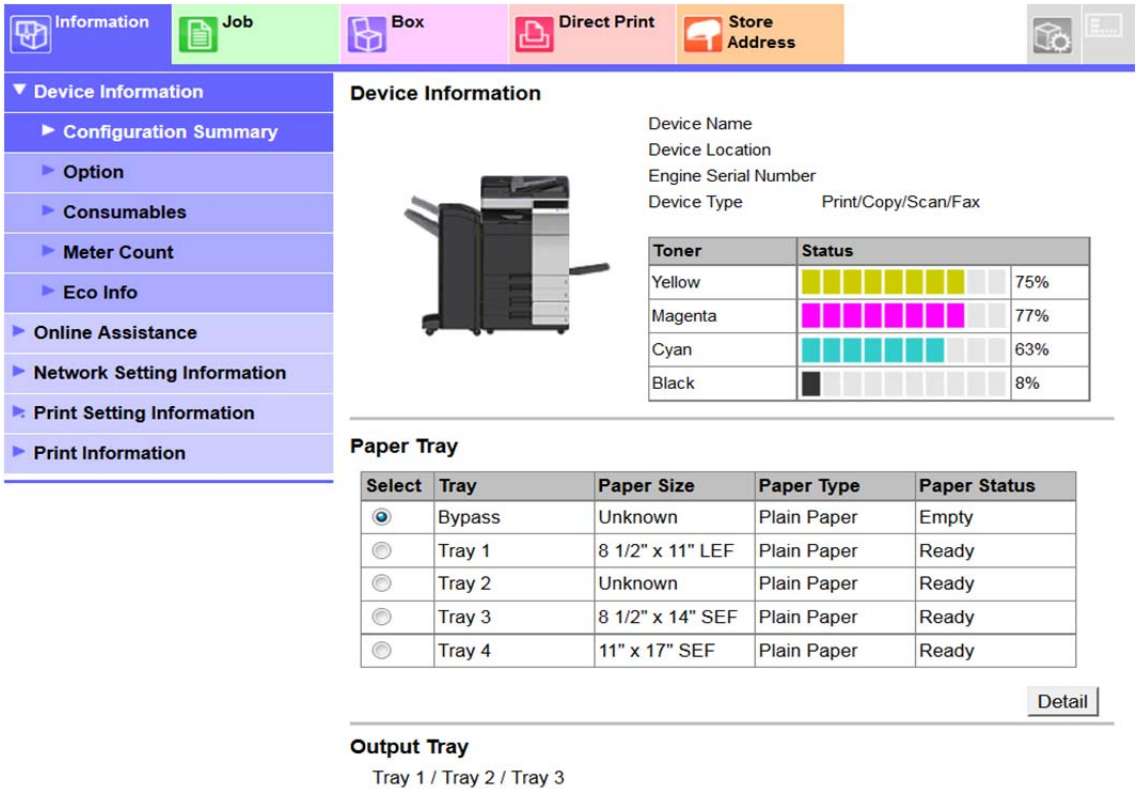
Today's printer/copiers have numerous features designed to improve office productivity. Users can manage these features through a touch screen on the device.

Figure 1 - Example of a copier touch control panel.



Additionally, networked devices can be accessed through a user-friendly web console accessible on any personal computer attached to the network. This access makes it possible to view extensive information about the device and the network. Web access makes it possible to control the printer/copier remotely, without having physical access to the device. For example, a user on the City network can use this method to access a printer/copier in a different department, floor, or building.

Figure 2 - Example of a printer/copier web console



Default administrator passwords have not been changed.

The first line of defense against misuse of remote access to printer/copiers is to establish a strong administrator password on the device. Printer/copiers ship with a default administrator password; the passwords are often published in the operator's manual for the device, or can be found on the manufacturer's website. If the default administrator password is not changed, any user on the City's network can potentially sign on as the printer/copier's administrator and make unauthorized changes to device settings or issue a command that disrupts printing or copying activities.

Changing the administrator password is recommended by printer/copier manufacturers and by the City's DTI security procedure *Information Technology Protection – Guide to Securing Networked Printers, Scanners, Copiers, and Faxes*. Changing the default administrator password is equivalent to locking an office door. However, in a sample of 27 Citywide printer/copiers supporting this feature, default administrator passwords had not been changed on 26 printer/copiers (93%). Implementing a strong administrator

password can significantly reduce the risk that a user inside the City's network can make unauthorized changes to the printer/copier's settings or deny use of the printer/copier.

Printer/copier hard drives have not been optimally secured.

Printer/copier hard drives have large storage capacities enabling the devices to temporarily save documents for sequential printing. However, unless the device is told to delete documents after printing or copying, document images may remain on printer/copier hard drives for months or years after a print job is completed. This creates a risk that an unauthorized party may view or reprint the document at a later time.

To prevent these risks, manufacturers often provide security features such as hard drive encryption or auto erase capabilities. Encryption "scrambles" the data on the hard drive, reducing the risk that the hard drive could be removed and accessed at a later time for information. Periodic erasure removes documents temporarily stored on the device, either immediately after a print/copy job completes, or at a regularly scheduled time, such as overnight, when the device is not being used. These features significantly reduce the risk that saved documents on the printer/copier hard drive could be retrieved by an unauthorized user. These security features are the customer's responsibility to activate. However the City is not consistently activating the features.

- Out of 16 printer/copiers in our sample that supported encryption, the feature was not enabled on 1 printer/copier (6%).
- Out of 15 printer/copiers in our sample that supported periodic hard drive erasure, 5 had not activated the feature (33%).

Activating these features significantly reduces the risk that previously printed or copied documents remain intact on the devices' hard drives.

Unnecessary network services have not been turned off.

Multifunction printer/copiers are designed to be used in a variety of environments and communicate with various computer networks. By default, new devices generally ship with most network services enabled. Depending on the customer's environment, most of these services are unnecessary. The presence of unnecessary services increases the means by which a printer/copier can be attacked.

Information security best practices and the City's DTI security procedure *Information Technology Protection – Guide to Securing Networked Printers, Scanners, Copiers, and Faxes* both suggest turning off unnecessary services. However, the City does not consistently turn these services off.

- On 25 of 25 printer/copiers in our sample that supported Internet Protocol filtering

(100%), devices had not been enabled to block traffic from outside the City network.

- On 20 of 25 printer/copiers (80%), File Transfer Protocol (FTP) had not been disabled.
- On 8 of 9 printer/copiers (89%), the Telnet protocol had not been turned off.
- On 10 of 23 printer/copiers (43%), Appletalk had not been disabled.
- On 1 out of 24 printer/copiers (4%), Netware had not been disabled.

Additional security of printer/copiers on the City's network can be achieved by simply activating recommended security settings.

RECOMMENDATIONS

- DTI should develop a written plan to activate security features on existing Citywide owned and leased networked printer/copiers to ensure conformance with the security procedure *Information Technology Protection – Guide to Securing Networked Printers, Scanners, Copiers, and Faxes*. In particular, the plan should ensure
  - Activation of strong administrator passwords,
  - Hard drive encryption and/or erasure when available, and
  - Disabling of unnecessary services.

- DTI should also develop a checklist for Service Desk personnel to ensure consistent activation of security features when adding printer/copiers and other multifunction devices to the City's network.

RESPONSE FROM DTI

"DTI will develop a plan to include the Printer Policy Security Standards into the purchase/lease printer copier agreements so that vendors are required to enable the security standards for printers and copiers upon being purchased and installed by City Departments.

"DTI will develop a plan to work with City Department IT/TRC liaisons to ensure all current networked printer/copiers are in compliance with the Printer Policy Security Standards.

"Note on Activation of Strong Admin passwords – this is not possible on many devices as they use pin numbers only, in these cases the default password will be changed."

ESTIMATED COMPLETION DATE

"December 31, 2015."

2. DTI SHOULD DEVELOP AND MAINTAIN A MASTER LISTING OF ALL PRINTER/COPIERS ON THE CITY'S NETWORK.

DTI does not have a complete listing of printer/copiers connected to the City's network. DTI has a partial listing of devices, but this listing does include key data elements, such as City department, physical location/room number, and whether or not the device has a hard drive. The partial listing provided by DTI contained 367 devices; however, DTI estimates that there are between 600 and 700 printer/copiers on the network.

Without a complete listing of Citywide printer/copiers with advanced features such as hard drives, DTI lacks the ability to implement sufficient safeguards to protect printer/copier devices and the network from potential insider attack and to ensure that hard drives are properly accounted for at the end of printer/copier lifecycles.

Information Technology Infrastructure Library (ITIL) guidance for Information Technology (IT) Service Management classifies hardware assets, such as printer/copiers, as *configuration items*. Inventories of configuration items and their attributes should be recorded in a configuration management database.

RECOMMENDATIONS

- DTI should develop and maintain a master listing of printer/copiers and other multifunctional devices on the City's network, including both leased and City-owned devices. The process should begin with a mandatory survey of all City departments requesting information about all departmental multifunction printer/copiers connected to the City's network.

- Specific information about each multifunction device should be collected, including:
  - Make of Printer/Copier
  - Model of Printer/Copier
  - Serial Number
  - Hard drive (yes/no)
  - Administrator password
  - Department
  - Division

- Purpose and use of machine
- Physical location
- Internet Protocol (IP) address
- Date in service
- Maintenance vendor
- Maintenance vendor contact information
- Lessor information (if leased)
- Lease expiration date (if leased)

- Once complete, the inventory of printer/copiers and other networked multifunction devices should be added to the Configuration Management System. Additions, deletions, or movement of devices should be captured through Service Now tickets.

RESPONSE FROM DTI

"DTI will develop a plan to work with City Department IT/TRC liaisons to ensure all current networked printer/copiers are inventoried and stored in Service Now with as much information as possible concerning that asset item."

ESTIMATED COMPLETION DATE

"December 31, 2016."

3. DTI SHOULD ENHANCE TECHNICAL REVIEW COMMITTEE PROCEDURES GOVERNING ACQUISITION AND MAINTENANCE OF NETWORKED PRINTER/COPIERS.

The City's Technical Review Committee must approve all requests for printer/copiers below $25,000. The review considers technical sufficiency and compliance with standards. Because printer/copiers are considered standard commodities, they generally do not require in-depth analysis, and may be approved directly by the Chief Information Officer. Current processes, however, do not ensure that leased or purchased printer/copiers will conform to DTI Security Policies, Standards, and Procedures.

The Technical Review Committee requires that a maintenance contract accompany any new purchase of a multifunction printer/copier. However, there is no process to ensure that maintenance vendors are aware of DTI Security Policies, Standards, and Procedures. There is no requirement to request DTI's assistance when setting up a new device. There is also an expectation that maintenance vendors will apply software updates and patches to

the printer/copiers, yet this expectation is not explicitly communicated to maintenance vendors.

There are inconsistent processes for removing printer/copier hard drives from service. City-owned devices are sent to the City's warehouse for erasure. However, a similar process does not exist for hard drives on leased devices. As a result, there is a risk that leased printer/copiers will be returned to the lessor without first erasing their hard drives.

RECOMMENDATIONS

DTI should enhance Technical Review Committee procedures to ensure that:

- Setup of new printer/copiers, whether leased or purchased, be requested through a DTI Service Now ticket.
- Printer/copiers connected to the City's network conform to DTI policies and standards, including, but not limited to, the security procedure *Information Technology Protection – Guide to Securing Networked Printers, Scanners, Copiers, and Faxes*.
- When available, hard drive encryption and/or auto-erasure features are activated.
- All printer/copier hard drives, whether leased or owned, are securely erased when multifunction devices are retired from service or when the hard drive is replaced.
- Related maintenance agreements are reviewed for proper security requirements by a specialist prior to approving purchase or lease of a printer or copier.
- Printer/copier maintenance contracts require vendors to apply patches and security updates to networked printer/copiers.

RESPONSE FROM DTI

"Purchasing will add the IT Guide to securing printers, scanners, copiers, and faxes to the purchase/lease agreements with the vendors as an installation setup requirement task. Once the vendor has completed the installation, the service desk will audit the security parameters."

ESTIMATED COMPLETION DATE

"June 30, 2016."

4. DTI SHOULD INCREASE COMMUNICATION OF INFORMATION TECHNOLOGY SECURITY POLICIES.

DTI Policies, Procedures, and Standards addressing information security have not been effectively communicated. DTI Policies, Procedures, and Standards are distributed through the Technical Review Committee, IT Liaisons, and through posting on the City's website. There is an expectation that Technical Review Committee members and IT Liaisons are the first lines of communication to City departments for technical information. However, these methods do not ensure that all departments and divisions are informed. Without effective internal communication of security policies, City departments may not be aware of information technology risks.

For example, the Technical Review Committee does not include members from all City departments and attendance at meetings is not mandatory. OIA reviewed Technical Review Committee participation for FY2015 and noted the following:

- Seven City departments did not have Technical Review Committee representation,
- One department and one division had Technical Review Committee representation, but did not attend a single meeting in FY2015, and
- Five departments attended less than 50 percent of the Technical Review Committee meetings in FY2015.

Although the City's Sensitive Data Policy charges each individual with access to sensitive data to safeguard the data, an anonymous survey of Technical Review Committee Members and Departmental IT Liaisons indicated that:

- Only 69 percent of respondents were aware of the DTI security procedure *Information Technology Protection – Guide to Securing Networked Printers, Scanners, Copiers, and Faxes*,
- Only 46 percent indicated that some of the recommended settings had been activated, and
- Only 54 percent indicated that hard drives had been configured to encrypt data or to automatically delete and periodically overwrite data.

The Committee of Sponsoring Organizations of the Treadway Commission's (COSO) internal control framework principle #14 emphasizes the importance of effective internal communication across a complex organization, such as a local government. Specifically, communication of information conveyed across the entity should include:

- "Policies and procedures that support personnel in performing their internal control responsibilities.

- Specified objectives.
- Importance, relevance and benefits of effective internal control.
- Roles and responsibilities of management and other personnel in performing controls.
- Expectations of the organization to communicate up, down and across the entity any matters of significance relating to internal control including instances of weakness, deterioration or non-adherence."

RECOMMENDATIONS

DTI should:

- Improve communication of security-related DTI Policies, Standards, and Procedures.
- Expand delivery methods to ensure that all users of the City's network are aware of relevant policies and procedures and their role and responsibilities related to information security.
- Include information security in new employee orientation; provide handouts containing intranet links to DTI Policies, Standards, and Procedures and Cyber Security Awareness Training.
- Distribute periodic information security emails to all employees on new and updated IT security policies and issues.
- Strengthen awareness through secondary communication channels, such as posting of flyers, articles on City's intranet, and through expansion of Cyber Security Awareness Training.
- Reinforce significant security-related IT issues through direct communication from the Chief Information Officer to key management personnel.
- Ensure that department directors are aware of security-related IT policies, standards, and procedures. Consider discussion of polices, standards, and procedures at the CAO's weekly Directors meeting.
- Clearly articulate security-related roles and responsibilities to IT Liaisons, and Technical Review Committee members.
- Update Technical Review Committee Policy to formalize communication-related responsibilities of members.

RESPONSE FROM DTI

"We will continue to strengthen the IT Security program with the following improvement items:

- ***DTI has communicated security related DTI policies, Standards, and Procedures using current communication methods available in CoA.***
- ***DTI has offered security training and URLs to be presented at NEO for new employees and will continue to work with HR to incorporate this training.***
- ***DTI currently uses secondary communication methods on eWeb, security web site, and through phishing testing and training.***
- ***The CIO has presented to the Directors and senior management on security related issues many times and will continue.***
- ***The CIO has presented Security related items on a regular basis at the weekly director meetings.***
- ***All security related items are presented to the TRC members as they are required to approve them prior to being published or revised. DTI also emails all new and revised policies and standards to IT liaisons.***
- ***We will update the TRC policy to require members to communicate with their departments."***

ESTIMATED COMPLETION DATE

"Ongoing."

5. DTI SHOULD ENHANCE ITS SECURITY GUIDANCE FOR NETWORKED PRINTER/COPIERS.

DTI'S information security procedure, *Information Technology Protection – Guide to Securing Networked Printers, Scanners, Copiers, and Faxes*, provides guidance on securing networked multifunction printer/copiers. The procedure was published July 1, 2014, and addresses the most significant risks associated with networked printer/copiers.

The City's procedure was compared to recommendations by the SANS Institute, a trusted source for information security training. While the City's procedure addresses a majority of the items identified by SANS, the procedure was silent on several SANS recommendations. DTI should consider adding these recommendations to the next update of its security procedure.

RECOMMENDATIONS

DTI should consider adding additional recommendations to the next revision of the security procedure *Information Technology Protection – Guide to Securing Networked Printers, Scanners, Copiers, and Faxes:*

- Assign printer/copiers to a static IP address.
- Use encrypted communication protocols.
- Enable event logging on the printer/copier.
- Ensure that device event logs are regularly monitored.
- Protect address books, mailboxes, and logs on printer/copiers by applying City password standards.
- For devices that print sensitive data, recommend that departments physically secure the devices, require identification of maintenance personnel, and supervise maintenance personnel when on site.
- Require users to authenticate when scanning, faxing, and copying from the device console.
- If the printer/copier has a removable hard drive, ensure that it is locked into the device.

RESPONSE FROM DTI

"DTI will revise the policy and Guide to securing network printers, scanners, Copiers, and Faxes with the recommendations identified."

ESTIMATED COMPLETION DATE

"June 30, 2016."

CONCLUSION

DTI should take additional steps to increase security on networked printer/copiers and other multifunction devices. Through development of a written plan and service desk checklist, existing networked printer/copiers can be brought into conformance with security best practices.

DTI should also take steps to increase awareness of information technology security policies and specific risks posed by networked printer/copiers. DTI should consider adding additional recommendations to its information security procedure, *Information Technology Protection – Guide to Securing Networked Printers, Scanners, Copiers, and Faxes*.

Enhancements should be made to processes for departmental purchasing, leasing, and maintenance of printer/copiers. Going forward, printer/copiers should not be connected to the network unless accompanied by a DTI Service Now request. All devices on the network should be documented in a master list, which identifies any devices with hard drives. Procedures should be enhanced to ensure that hard drives on leased printer/copiers are properly erased before being sent back to the vendor or being replaced.

Through implementation of the recommendations in this report, DTI can:

- Enhance security and management of networked printers, copiers, and other multifunction devices,
- Reduce the risk of unauthorized release of sensitive information, and
- Improve communication and awareness of IT security policies.

We greatly appreciate the assistance and cooperation of the Department of Technology and Innovation during the course of the audit.

_____
Senior Information Systems Auditor

REVIEWED:

_____
Internal Audit Manager

APPROVED:

_____
Debra Yoshimura, CPA, CIA, CGAP
Director, Office of Internal Audit

APPROVED FOR PUBLICATION**:**

_____
Chairperson, Accountability in
Government Oversight Committee

APPENDIX A

OBJECTIVES

The audit objectives are:

- Are policies and procedures adequate for governing the security of networked printer/copiers and other multifunction devices?
- Are information security best practices active on citywide printer/copiers and other multifunction devices?

SCOPE

Our audit did not include an examination of all functions and activities related to the City's management of networked printer/copiers, and other multifunction devices. Our scope was limited to the objectives above.

This report and its conclusions are based on information taken from a sample of transactions and do not represent an examination of all related transactions and activities. The audit report is based on our examination of activities through the completion of fieldwork on October 14, 2015 and does not reflect events or accounting entries after that date.

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.

METHODOLOGY

Methodologies used to accomplish the audit objectives include but are not limited to the following.

- Obtained an understanding of City procedures for purchasing and leasing printer/copiers and other multifunction devices.
- Interviewed DTI management to ascertain processes used to setup, maintain, and monitor networked printer/copiers and other multifunction devices.
- Inquired of DTI personnel regarding procedures for applying patches and firmware

updates to networked printer/copiers and other multifunction devices.

- Reviewed City Purchasing Ordinance requirements for disposition of City-owned surplus, salvage and scrap property.
- Met with City Warehouse staff to gain an understanding of processes for removing City-owned printer/copiers and multifunction devices from service.
- Researched best practices and other guidance related to security of networked multifunction devices.
- Reviewed audit reports addressing similar subject matter of other government entities.
- Reviewed vulnerability assessments performed on the City's network for identification of printer/copier vulnerabilities and related remediation efforts.
- Reviewed settings on a random sample of networked multifunction printer/copiers.
- Reviewed settings and physical security on a judgmentally-selected sample of multifunction printer/copiers in departments that routinely print and copy information of a sensitive nature.
- Surveyed departmental IT liaisons and Technology Review Committee members to assess general awareness of printer/copier security.
- Surveyed departmental IT liaisons and Technology Review Committee members to assess specific knowledge of DTI Security Procedure *Information Technology Protection – Guide to Securing Networked Printers, Scanners, Copiers, and Faxes*.