# *City of Albuquerque*

## Office of Internal Audit

FOLLOW-UP OF THE
DEPARTMENT OF TECHNOLOGY AND INNOVATION AUDIT
PRINTER / COPIER SECURITY
Report #20-15-104F
February 27, 2020

***INTRODUCTION***

The Office of Internal Audit (OIA) performed a follow-up of Performance Audit No.15-104, Department of Technology and Innovation (DTI) Printer/Copier Security during fiscal year (FY) 2015. The purpose of this follow-up is to report on the progress made by DTI in addressing the audit's findings and recommendations. Our follow-up procedures rely on the department providing the status of the recommendations.

A follow-up is substantially less in scope than an audit. The objective is to report on the status of corrective action regarding the audit's findings and recommendations.

We limited our scope to actions taken to address our audit recommendations from the final audit report dated December 9, 2015 through the submission of actions on December 12, 2019.

***BACKGROUND***

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.

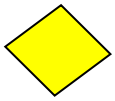
Follow-Up
Department of Technology and Innovation #20-15-104F
Printer/Copier Security
February 27, 2020

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.

## ***SUMMARY***

Of the five recommendations addressed in the original audit report, five are in process.

The status of the recommendations is identified by the symbols in the following legend:

 Fully Implemented  In Process  Not implemented

**Recommendation #1**
DTI should:

- 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.***

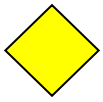
***"DTI will develop a plan to work with City Department IT/TRC liaisons to ensure all current networked printer/copiers are in compliance with the Printer Policy Security Standards.***

***"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."*

**Status Reported by DTI:**
"Complete. Here is the link to the written guide that is on our ewebsite:"

Guide to Securing Network Printers



**In Process**

https://eweb.cabq.gov/DTI_PoliciesProcedures/Procedures/Security/Guide%20to%20Securing%20Networked%20Printers.pdf

DTI has published the policies and procedures for City employees to activate security features on existing citywide owned and leased networked printer/copiers. However, no checklist was provided to ensure consistent activation of security features for employees setting up new owned and leased networked printer/copiers. No written plan to activate security features on existing City owned or leased network equipment.

**Recommendation #2**
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**

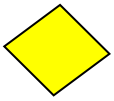
***"DTI will develop a plan to work with City Department IT/TRC liaisons to ensure all current networked printer/copiers are inventoried and stored in Service Now with as much information as possible concerning that asset item."***

**ESTIMATED COMPLETION DATE**
"***December 31, 2016."***

**Status Reported by DTI:**

A list of printers resides in the following applications:

- Windows Print Server
- KACE
- ServiceNow



**In Process**

DTI stated a list of printers resides in the following applications: Windows Print Server, KACE, and ServiceNow. However, the complete list of leased and City owned devices were not included, with the information requested above. The Configuration Management System listing of the inventory of printer/copiers was not provided. The multifunction printer/copier resources as last approved July 1, 2014.

**Recommendation #3**
DTI should:

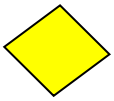
Enhance Technical Review Committee procedures to ensure that:

- 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."***

**Status Reported by DTI:**
No response was given.

 In Process

DTI did not provide support to ensure the set-up of new printer/copiers, leased or purchased be requested through a DTI Service Now ticket. The security procedures noted at *Information Technology Protection – Guide to Securing Networked Printers, Scanners, Copiers, and Faxes* do not mandate the individual department to work with or utilize the policies set by DTI, which is overseen by the Technical Review Committee.

**Recommendation #4**
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:***

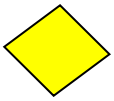
- ***DTI has communicated security related DTI policies, Standards, and Procedures using current communication methods available in CoA.***
- ***DTI has offered security training and URLs to be presented at NEO for new employees and will continue to work with HR to incorporate this training.***
- ***DTI 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."***

**Status Reported by DTI:**

No response was given.

 In Process

DTI has published the policies and procedures for City employees. However, no support was provided to ensure the City Directors are aware of the current security-related IT policies, standards and procedures. Also, no documentation was provided displaying formal communication related to responsibilities of the IT liaisons.

**Recommendation #5**

DTI should:

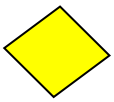
Consider adding additional recommendations to the next revision of the security procedure *Information Technology Protection – Guide to Securing Networked Printers, Scanners, Copiers, and Faxes:*

- 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.

**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."***

**Status Reported by DTI:**
Ongoing. As security standards evolve and new security/network equipment gets implemented we will revise the Guide.


In Process

DTI has published the policies and procedures for City employees to activate security features on existing citywide owned and leased networked printer/copiers. However, no support has been provided which verify the recommendations to enhance or require the recommendations as a first line defense of cyber security,

SUBMITTED:

_____
Connie Barros-Montoya, Staff Auditor,
Office of Internal Audit

REVIEWED & APPROVED:

_____
Ken Bramlett, Interim City Auditor,
Office of Internal Audit

APPROVED FOR PUBLICATION**:**

_____
Edmund E. Perea, Chairperson,
Accountability in Government
Oversight Committee