METROPOLITAN GOVERNMENT OF NASHVILLE AND DAVIDSON COUNTY

OFFICE OF INTERNAL AUDIT

Professional Audit and Advisory Service

FINAL REPORT

Audit of the Acceptable Use of Information Technology Assets – Office of Emergency Management

Date Issued: November 29, 2012

Office Location and Phone Number

222 3rd Avenue North, Suite 401
Nashville, Tennessee 37201
615-862-6110

The Metropolitan Nashville Office of Internal Audit is an independent audit agency reporting directly to the Metropolitan Nashville Audit Committee

EXECUTIVE SUMMARY

November 29, 2012

Results in Brief

An audit of the *Acceptable Use of Information Technology Assets Policy* for the Office of Emergency Management was chosen along with two other entities to determine progress in meeting management’s goal to enhance the overall information security posture for the Metropolitan Nashville Government. This report contains the results for the Office of Emergency Management.

Audit Objectives

- *Were users storing sensitive Metro Nashville information on authorized storage devices?*

  Yes. It was determined that sensitive data, which includes confidential data, was stored according to the Acceptable Use Policy and best security standards.

- *Were employees knowledgeable of Acceptable Use of Information Technology Assets Policy and related Data Classification Policy provisions?*

  Generally yes. While not specifically aware of all parts of the policy, the group was generally following the policy.

- *Were prohibited acts, outlined in the Acceptable Use Policy, being carried out on Metro Nashville equipment?*

  Generally no. Employee personal use accounted for minimal time on the internet and negligible computer workstations resources.

Background and Recommendations

A new *Acceptable Use of Information Technology Assets Policy* was distributed in May 2011 and went into effect in November 2011. The purpose of the policy was to improve information security management within the Metropolitan Nashville Government.

Information Classifications

Public – No risk such as reports meant for public distribution.

Internal – Lowest risk such as staff phone numbers.

Confidential – High risk such as social security and credit card numbers.

Restricted– Highest risk where loss of life could occur, such as witness protection information.

Recommendations

Key recommendations of this report include:

- Reemphasize with staff of the lack of expectation of privacy.
- Monitor website filter reports for excessive access to blocked websites and were necessary, inform staff of websites that are blocked.
- Disable and/or delete un-necessary computer accounts that are not needed.
- Train staff on the use of the Information Classification Policy.

TABLE OF CONTENTS

INTRODUCTION

Audit Initiation

The audit of the Office of Emergency Management was conducted as part of the approved 2012 Audit Work Plan. The Office of Emergency Management was chosen along with two other entities to determine progress in meeting management's goal to enhance the overall information security posture for the Metropolitan Nashville Government

Background

The Acceptable Use of Information Technology Assets Policy (hereinafter referred to as "Acceptable Use Policy") was generated from the effort established by Executive Order Number Five, Security Awareness, and Executive Order Number 38, Information Security Management Policy and Steering Committee Authorization. A team made up of representatives from all major departments collaborated to create a set of security policies and plans to improve information security management.

The purpose of this policy was to define good practices for the acceptable use of information and assets associated with information processing and information processing facilities to ensure that the Metropolitan Nashville Government achieves and maintains appropriate protection of its information technology assets.

The Office of Emergency Management has 11 employees and two contractors, of which all have computer access. Each of the 13 personnel had their own computer and network account and was aware of and had signed the Acceptable Use policy.

Organizational Structure

The interim Director of the Nashville Fire Department is also the interim Director of the Office of Emergency Management. Reporting to interim Director of the Nashville Fire Department is an Assistant Nashville Fire Department Chief, who is responsible for carrying out operations duties and to provide resources for operation. The Director of Water Services is in the span of control due to his position in handling of Metro Nashville emergency situations.

Information Systems

The following information systems are used by the Office of Emergency Management staff:

- Computer-aided Dispatch call management/dispatch system
- Web EOC-Web based package to display data in the Emergency Operation Center ("War Room") on four large panels
- LeoGov.com-Replacement system for Web EOC
- Enterprise Business Systems, Accounting
- XM Radios
- CAD Software

- Office of Emergency Management Asset List package (for grant funded items)

- Dragon Speech to test conversion package

- Air-card Sprint package

There were 13 computers assigned to the Office of Emergency Management staff and 18 user accounts in the Active Directory database.

For fiscal year 2012, information technology related budgeted expense was $196,470.

OBJECTIVES AND CONCLUSIONS

1. *Were users storing sensitive Metro Nashville information on authorized storage devices?*

   Yes. By interviewing and studying the data flows of the Office of Emergency Management operations, it was determined that sensitive data, which includes confidential data, was stored according to the Acceptable Use Policy and best security standards. The sensitive data, in paper form, was in locked file cabinets and the computer aided dispatch data was electronically stored.

   The computer-aided dispatch system may store restricted data. In addition to secure login, the building was monitored by 24-hour guard system with card access required for entry.

2. *Were employees knowledgeable of the Acceptable Use Policy and related Data Classification Policy provisions?*

   - *Were users aware of password requirements?*
   - *Were user's email and internet access primarily for Metro Nashville business purposes?*
   - *Were user's mobile phones authorized by Metro Nashville and connected to an approved mobile device server?*
   - *Were user's expectations of privacy, when using Metro Nashville devices, valid?*
   - *Were users accessing the Metro Nashville network from an external site utilizing an approved virtual private network connection?*

   Generally yes. In the short time the Office of Emergency Management had been exposed to the Acceptable Use of Information Technology Assets policy, employees were aware of and signed-off on the Acceptable Use of Information Technology Assets Policy. While not specifically aware of all parts of the policy, the group was generally following the policy.

   However, there was no one in our sample who was aware of the Information Classification Policy, 13 users in total.

   Furthermore the following security practices were observed:

   - Passwords and logical locks were applied according to the Acceptable Use Policy.
   - There was no evidence that email was being used for non-business purposes based on interviews and direct observation of email content.
   - Users were aware of the internet access requirements.

- Metro Nashville approved cell phones, personal digital assistant or smart phones were being used.
- Users expected their data to be private versus the policy which states it is not for five (38 percent) of 13 users (see Observation A).
- Users with remote access privileges agreed with the active directory security group members list.

3. *Were prohibited acts, outlined in the Acceptable Use Policy, being carried out on Metro Nashville equipment?*

    - *Excessive personal use*
    - *Viewing or storing inappropriate material*
    - *Illegal duplication of software*
    - *Unauthorized system access*
    - *Unauthorized distribution of information on the internet*

    Generally no. Employee personal use accounted for minimal time on the internet and negligible computer workstations resources. Intellectual property rights for four programs were installed on department workstations, two of which were identified as personal.

    Office of Emergency Management internet access was tested over a ten day period. Approximately 25 percent was assigned the blocked website category, “Bandwidth: Personal Network Storage and Backup”, with the greatest occurrence of access to www.dropbox.com, a cloud storage and file sharing website. The Office of Emergency Management used the website for a government related project until November 2011. Due to demand on the Metro network, the website was blocked (in the website filter software) by Information Technology Services in late June 2012.

    The Office of Emergency Management staff continued to attempt to access the site which was recorded in the internet log sample conducted in late July and early August. (see Observation A).

OBSERVATIONS AND RECOMMENDATIONS

A - Acceptable Use of Information Technology Assets Policy

Information security practices could be improved to minimize the risk of unauthorized access or processing of Metro Nashville information assets. The following areas of concern were observed:

- Staff indicated they had an expectation of privacy when sending and receiving data or email. This was the case for five (38 percent) out of 13 Office of Emergency Management users. The remaining personnel did not expect privacy in those instances, because, data could be sent anywhere, seen by anyone or requested through e-discovery by the Department of Law or open records requests.
- Intellectual property rights for four programs installed on department workstations. Two were identified as personal.
- In the Office of Emergency Management Active Directory report, five generic ID's were listed. Upon reconciliation of those five, one account was found active but no longer needed.
- There were an unusually large number of access attempts to dropbox.com and related IP addresses approximately 30 days after the website was blocked. The Office of Emergency Management used this website for a government related project until November 2011. Access to this website was blocked by Information Technology Services in late June 2012 due to bandwidth considerations and was unrelated to the Office of Emergency Management usage. The sample was conducted in late July and early August, where a large number of blocked access attempts were recorded to this site

Criteria:

- *Acceptable Use of Information Technology Assets Policy*, 7.1.3, effective November 1, 2011
- ISO 27002, Part 11.1, Access control rules should take account of policies for information dissemination and authorization.

Risk:
Unauthorized access or processing of Metro Nashville information may occur resulting in financial loss or compromise of public trust.

Recommendation:
Management of the Office of Emergency Management should:

1. Reemphasize with staff of the lack of expectation of privacy, intellectual property rights, and email retention practices when using Metro Nashville technology assets.

2. Monitor website filter reports for excessive access to blocked websites and were necessary, inform staff of websites that are blocked.
3. Disable and/or delete un-necessary computer accounts that are not needed.
4. Train staff on the use of the Information Classification Policy.

GENERAL AUDIT INFORMATION

Statement of Compliance with GAGAS

This audit was conducted from July 2012 to August 2012, 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 observations and conclusions based on our audit objectives.

We believe that the evidence obtained provides a reasonable basis for our observations and conclusions based on our audit objectives.

Scope and Methodology

The audit period focused primarily on the period November 1, 2011, through June 30, 2012. The methodology employed throughout this audit was one of objectively reviewing various forms of documentation, conducting interviews and surveys, observations, procedures, and other relevant data.

Criteria

In conducting this audit, the existing processes were evaluated for compliance with:

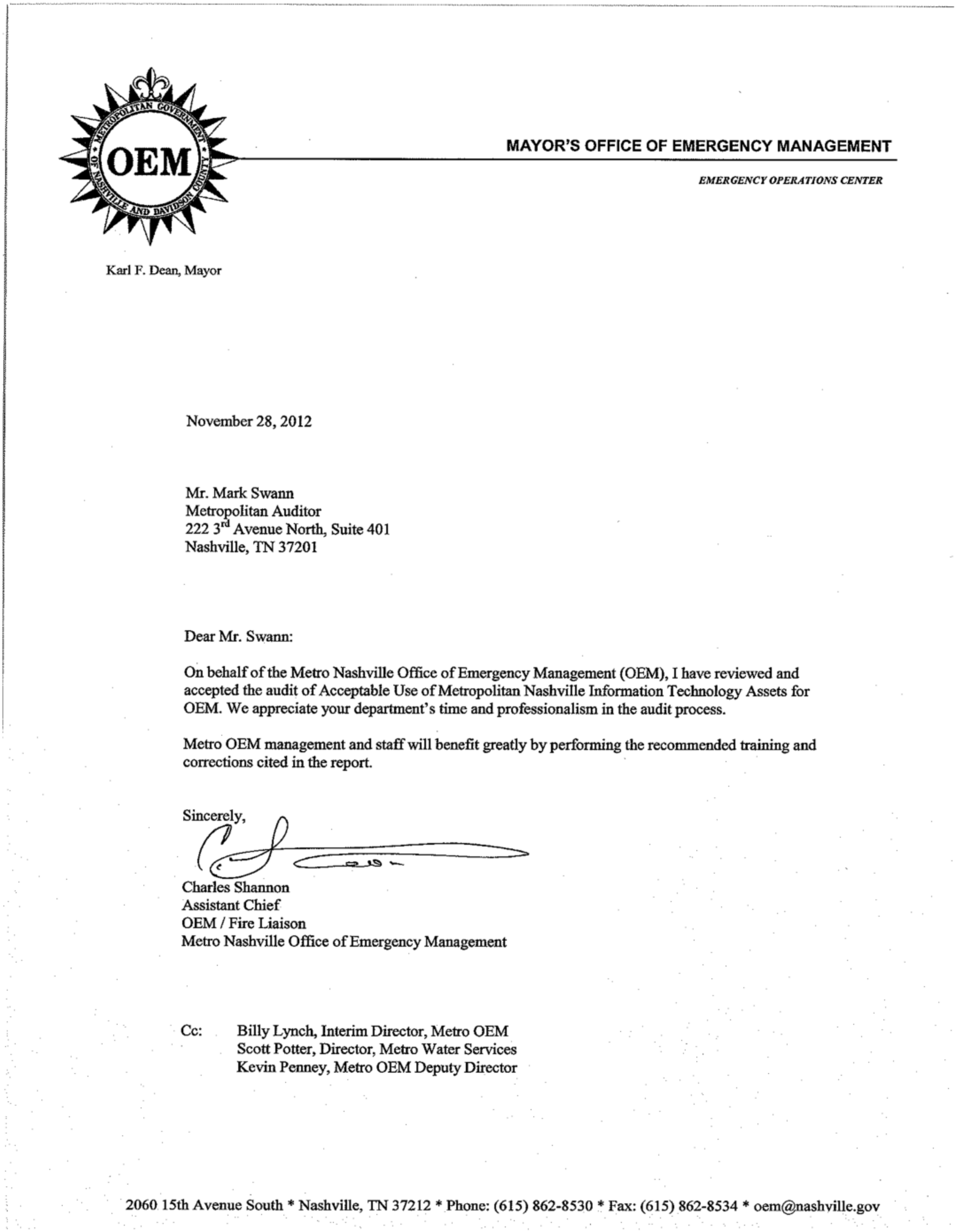
- *Acceptable Use of Information Technology Assets Policy*, 7.1.3, effective November 1, 2011
- *Information Classification Polic*y, 7.2,1, effective November 1, 2011
- *International Standards Organization 27001/27002*, Part 7

Audit Project Staff

Joseph McGinley, CISSP, CISA - In Charge Auditor
Mark Swann, CPA (Texas), CIA, CISA – Quality Assurance

APPENDIX A. MANAGEMENT RESPONSE

Management’s Responses Starts on Next Page



OEM

METROPOLITAN GOVERNMENT OF NASHVILLE AND DAVIDSON COUNTY

MAYOR'S OFFICE OF EMERGENCY MANAGEMENT

EMERGENCY OPERATIONS CENTER

Karl F. Dean, Mayor

November 28, 2012

Mr. Mark Swann
Metropolitan Auditor
222 3rd Avenue North, Suite 401
Nashville, TN 37201

Dear Mr. Swann:

On behalf of the Metro Nashville Office of Emergency Management (OEM), I have reviewed and accepted the audit of Acceptable Use of Metropolitan Nashville Information Technology Assets for OEM. We appreciate your department's time and professionalism in the audit process.

Metro OEM management and staff will benefit greatly by performing the recommended training and corrections cited in the report.

Sincerely,

Charles Shannon
Assistant Chief
OEM / Fire Liaison
Metro Nashville Office of Emergency Management

Cc: Billy Lynch, Interim Director, Metro OEM
Scott Potter, Director, Metro Water Services
Kevin Penney, Metro OEM Deputy Director

2060 15th Avenue South * Nashville, TN 37212 * Phone: (615) 862-8530 * Fax: (615) 862-8534 * oem@nashville.gov

Audit of the Acceptable Use of Information Technology Assets Policy
Office of Emergency Management Response to Audit Recommendations

Audit Recommendation	Response to Recommendation/Action Plan	Assigned Responsibility	Estimated Completion
A.1 Management of the Office of Emergency Management should reemphasize with staff the lack of expectation of privacy, intellectual property rights, and email retention practices when using Metro Nashville technology assets.	**Accept.** Management of the Office of Emergency Management has instructed staff to re-emphasize there is no expectation of privacy and to continue proper email retention practices -- when using Metro Nashville technology assets.	Kevin Penney Charles Shannon	11-1-12
A.2 Management of the Office of Emergency Management should monitor website filter reports for excessive access to blocked websites and were necessary, inform staff of websites that are blocked.	**Accept.** Management of the Office of Emergency Management has instructed staff website filtering reports will be monitored regularly to ensure compliance with Metro's IT Proper Use Policy.	Kevin Penney Charles Shannon	On-going
A.3 Management of the Office of Emergency Management should disable and/or delete un-necessary computer accounts that are not needed.	**Accept.** Management of the Office of Emergency Management will disable or delete inactive or unnecessary computer accounts.	Kevin Penney Charles Shannon	11-2-12
A.4 Management of the Office of Emergency Management should train staff on the use of the Information Classification Policy.	**Accept.** Management of the Office of Emergency Management instructed staff to review again and be familiar with Metro's Information Classification Policy and continue to handle and secure data appropriately. Refresher training will also occur, as needed.	Kevin Penney Charles Shannon	11-1-12