Los Angeles County
Metropolitan Transportation Authority
Office of the Inspector General

Follow-Up Review of Department Information Security

Management has taken adequate corrective actions to implement the recommendations in the prior OIG audit report.

Report No. 12-AUD-12 **April 27, 2012**

Metro™

TABLE OF CONTENTS

Metro

Los Angeles County
Metropolitan Transportation Authority

Office of the Inspector General
818 West 7th Street, Suite 500
Los Angeles, CA 90017

213.244.7300 Tel
213.244.7343 Fax

DATE: April 27, 2012

TO: Board of Directors
Chief Executive Officer

Jack Shigetomi

FROM: Jack Shigetomi
Deputy Inspector General - Audits

SUBJECT: **Follow-Up Review of Department Information Security (Report No. 12-AUD-12)**

INTRODUCTION

The Office of the Inspector General (OIG) performed a follow-up review on four recommendations in our prior audit report on *Department Information Security* (Report No. 08-AUD-15, dated February 24, 2009). This follow-up review was performed to determine whether Metro management had implemented the recommendations to correct deficiencies noted in the prior audit report. This review was conducted as part of our ongoing program to assist the Los Angeles County Metropolitan Transportation Authority (Metro) in implementing an effective control program, and deterring fraud, waste and abuse. Overall, we found that management had taken adequate actions to implement the recommendations in our prior audit report.

OBJECTIVE AND SCOPE OF FOLLOW-UP REVIEW

The objective of the follow-up review was to determine whether management had implemented the recommendations in the prior OIG audit report *Department Information Security*. To achieve the objective, we:

- Reviewed Metro General Management Records Management (GEN 8) issued on August 17, 2010, which establishes the responsibilities and requirements for managing Metro records and ensures compliance with the California Public Records Act and other applicable state laws and regulations.

- Reviewed Metro Information Technology Information Security Policy (IT 1) issued on August 16, 2010, which defines general principles, roles and responsibilities for authorized access, storage, use, and disposition of Metro's data and information resources.

- Reviewed 6 new Information Technology Services Standard Operating Procedures (SOPs) issued between June and October of 2011 (see Attachment A).

- Discussed the issues with staff from the Information Technology Services, Research and Records Information (formerly Records Management), and the Organizational Development and Training Departments.

Our review was performed in accordance with Generally Accepted Government Auditing Standards for staff qualifications, independence, and due professional care and included such tests of procedures and records, as we considered necessary. Our conclusions are limited to our examination of the documents submitted by Metro Management.

BACKGROUND

Metro Data

The Information Technology Services (ITS) Department maintains Metro's computer network and major information systems. Authorized staff at user departments have access to the centralized databases. Information from the central databases can be copied and put on portable storage media or laptop computers. Since media and laptop computers can easily be taken out of Metro worksites, it is important to include these devices in information security policies.

Some of this information is private, sensitive, or business proprietary data that could be copied and removed from Metro worksites. Metro's central network system includes personal information such as names, social security numbers, bank account numbers, addresses, birth dates, and driver license numbers. The network system also contains confidential information such as procurement records and vendor information.

Legal Requirements

California State Law requires businesses to protect personal information.[1] Businesses are required to disclose any breach in security of the system following discovery or notification of the breach to any resident of California whose unencrypted personal information was, or is reasonably believed to have been acquired by an unauthorized person.

Prior OIG Audit

[1] California Civil Code 1798.80 and 1798.81.

Our prior audit report on *Department Information Security* found that Metro departments/business units had not implemented Metro policy requirements concerning information security; specifically, improvements were needed in the following areas:

- Departments had not validated and assessed business and information security risks.
- Departments had not developed written SOPs on information security.
- Some departments did not have procedures to control and/or secure information on portable storage media.
- Some departments did not have policies pertaining to taking removable storage media containing Metro data outside Metro worksites.
- Some departments did not keep records of sensitive or confidential data being taken out of the Metro facility.
- Some departments did not have procedures for encrypting data, password protecting removable storage media, or securing data when it is taken outside Metro worksites.

The prior audit report recommended that:

1. Information Technology Services should notify and reinforce to departments/business units the requirement in Metro's Information Technology Policy IT 1 that business units are required to (a) validate and assess the information security risk, and (b) implement written Standard Operating Procedures.

2. Information Technology Services and Records Management should provide additional direction and assistance to departments/business units on information security requirements.

3. Information Technology Services and Records Management should provide additional guidance to departments/business units as to areas that should be covered by department SOPs such as:

   a. Process to assess business and information system security risks.

   b. Define all data resources under department control including the sensitivity and privacy considerations.

   c. Identify the scope and access of appropriate staff.

d. Define the circumstances, methods, and approvals for taking data from Metro worksites.

e. Specify the data security requirements when data is taken from Metro worksites.

4. Records Management should complete its revision of General Policy 8 and include guidance on control and monitoring data in areas such as:

    a. Encryption and/or password protection for portable storage media.

    b. Controls such as authorization or logs for sensitive data files taken outside of Metro worksites.

    c. Attaching Metro data files to e-mails.

    d. Opening and/or saving Metro data files on employee's personal computers.

RESULTS OF FOLLOW-UP REVIEW

We found that Metro management had taken adequate corrective actions to implement the recommendations noted in the prior audit report on *Department Information Security*. Specifically Metro management completed the following actions:

- Metro-wide General Management Policy GEN 8, revised August 17, 2010, resolved all matters that the prior audit found with the previous policy.

- Information Security Policy IT 1, was revised on August 16, 2010. The new policy resolved all matters concerning the previous policy.

- ITS implemented several new standard operating procedures (SOPs), available on their webpage through the link "Policies." The relevant policies are as follows (see Attachment A for details of each SOP):

    - MIT-02 Data Management Roles & Responsibilities Standard, October 3, 2011
    - MIT-03 Password Standard, June 23, 2011
    - MIT-04 Data Classification and Control Standard, September 30, 2011
    - MIT-07 Acceptable use of IT Computing Devices, September 30, 2011
    - MIT-10 Security Standard For Email, September 30, 2011

- MIT-11 Security Controls Modification Standard, September 30, 2011

- The new ITS SOPs were incorporated into the Management Orientation Program (MOP) through the class titled "Record Management and Information Security." The MOP involves 9 mandatory courses and is offered quarterly to managers and supervisors to provide training on specific Metro policies and procedures. "Records Management and Information Security" is a mandatory class for the MOP, as well as for all supervisors and managers who have not yet taken the most up-to-date version of it. Supervisors and managers are required to take this course periodically based on when procedures are revised. This class is instructed by staff from the Research and Records Information Department and includes a presentation from an ITS representative.

- The Records Management Center has conducted, and continues to perform, periodic inspections and audits of department records (Records Inventory Evaluations) every 2 years. Thirty six inspections have been made since the revision of GEN 8. The dates of when a department is due for a Records Inventory Evaluation and the last evaluation are listed on a Sharepoint spreadsheet. Records Management also files the comprehensive report on their share drive.

- ITS staff have identified about 160 computer applications owned by about 25 departments. ITS is in the process of developing an information security template to identify these applications and the staff responsible. ITS security staff have begun working with the owners to assure user staff are knowledgeable of security procedures and follow them. Since this process is still ongoing, we might consider reviewing this area in a future audit. ITS staff also participate in the MOP training described above and answer questions from attendees.

We believe that the positive corrective actions taken by management should improve controls and procedures over department information security. See Attachment B for additional details of the status of implemented corrective actions.

Attachment A

ITS Standard Operating Procedures Reviewed

We reviewed the following 6 new Information Technology Services Standard Operating Procedures (SOPs) issued between June and October of 2011:

- Information Technology Services Data Management Roles & Responsibilities Standard (MIT-02) issued on October 3, 2011, establishes Information Technology Security “Roles and Responsibilities” with “Terms and Definitions” to identify shared responsibilities for assuring that Metro systems and applications have confidentiality, integrity, and availability, and efficiently serves the needs of the Agency.

- Information Technology Services Information Technology Password Standard (MIT-03) issued on June 23, 2011, provides guidelines for creating, protecting, changing, and deleting passwords which are strong, complex, and protected.

- Information Technology Services Information Technology Data Classification and Control Standard (MIT-04) issued on September 30, 2011, provides guidelines to Metro System Owners, Data Owners and Data Custodians for assessing business information systems and determining the sensitivity of the data within the applications.

- Information Technology Services Acceptable Use of IT Computing Devices (MIT-07) issued on September 30, 2011, establishes a standard for acceptable and non-acceptable usage of IT resources at Metro.

- Information Technology Services Information Technology Security Standard for Email (MIT-10) issued on September 30, 2011, provides security controls to protect the transmission of sensitive data through email services that will reduce risks to Metro’s information systems.

- Information Technology Services Security Controls Modification Standard (MIT-11) issued on September 30, 2011, provides guidelines to modify the security access of a Data User in the event of a role or status change.

Status of Implementation of Corrective Actions
Follow-up Review of Department Information Security

Recommendation 1

OIG Recommendation	Management Response	Current Actions Taken
a. Validate and assess the information security risk	The Information technology Service Department will develop a new Information Security training module that will be offered through the OD&T Management Orientation Program (MOP). The training module will be conducted by ITS in conjunction with the Records Management Training course.	The Management Orientation Program (MOP) involves 9 mandatory classes and 14 regular classes. It is offered once a quarter to managers and supervisors in order to provide training on specific Metro policies and procedures. The additional class offered is titled "Record Management and Information Security." It is a mandatory class for this program, and also mandatory for all supervisors and above. It is instructed by Records Services. An ITS representative also makes a presentation during this class.
b. Implement Written Standard Operating Procedures	The ITS Department, Records Management Center (RCM), and County Counsel will collaborate and develop an agency-wide Information Security Standard Operating Procedures (SOPs) that Metro business units will implement and utilize to accomplish and maintain uniformity and consistency of procedures used to validate and assess information security risks. The completion date for development of the SOPs will be twelve (12) months following Board approval of the revision to the Records Management (GEN 8) Policy. The Information Security (IT 1) Policy will also be revised to reiterate and refer the business units to the SOPs for direction and guidance.	ITS has implemented several new standards, which are available on their webpage through the link "Policies." The policies are as follows: MIT-02 Data Management Roles & Responsibilities Standard (10/03/11), MIT-03 Password Standard (06/23/11) MIT-04 Data Classification And Control Standard (9/30/11), MIT-07 Acceptable use of IT Computing Devices (09/30/11), MIT-10 Security Standard For Email (9/30/11), MIT-11 Security Controls Modification Standard (09/30/11). In addition, IT 1 was revised effective 8/16/2010. Paragraph 1.1 states "SBU's are responsible for ensuring information security is implemented within their departments, following guidelines established by ITS and RMC. We might consider reviewing the effectiveness of this action in a future audit.

Status of Implementation of Corrective Actions
Follow-up Review of Department Information Security

Recommendation 2

OIG Recommendation	Management Response	Current Actions Taken
Information Technology Service and Records Management should provide additional direction and assistance to departments/business units on information security requirements	The additional direction and guidance will be addressed in the new information security training module in conjunction with the Records Management Training course and the Information Security SOPs. In addition, information security awareness sessions will be conducted to facilitate the implementation of the Information Security SOPs.	• The Management Orientation Program (MOP) involves 9 mandatory classes and 14 regular classes. It is offered quarterly to managers and supervisors to provide training on specific Metro policies and procedures. The additional class offered is titled "Record Management and Information Security." It is a mandatory class for this program, and also mandatory for all supervisors and above. It is instructed by Records Services. An ITS representative also makes a presentation during this class. • ITS has implemented several new standards, available on their webpage through the link "Policies." The policies are MIT-02, MIT-03, MIT-04, MIT-07, MIT-10, and MIT-11. • ITS has identified the Metro applications and the departments that own that data. Staff is also developing a template for owners to use in controlling this data and have begun working with the owners to assure that data is protected at the department level.

Status of Implementation of Corrective Actions
Follow-up Review of Department Information Security

Recommendation 3

OIG Recommendation	Management Response	GEN 8 (8/17/2010) Applicability	SOP Applicability
a. Process to assess business and information system security risks	The Information Security SOPs will include direction and guidance for business units to follow to assess information security risks	N/A	MIT-04 paragraph 2.3 states "System Owners must periodically check to ensure that their business systems continue to be classified appropriately and that the security controls and safeguards remain valid and operative"
b. Define all data resources under department control including the sensitivity and privacy considerations	The requirement for business units to define all data resources under their control including sensitivity and privacy considerations will be included in the GEN 8 Policy, and guidelines to assist departments with meeting this requirement will be provided in the Information Security SOPs	Paragraph 1.0 states "Departments must define the data resources under their control"	MIT-04 paragraph 1.2 states "All data locations and classifications must be clearly identified"
c. Identify the scope and access of appropriate staff	The requirement for business units to identify the scope and access of appropriate staff will be included in the revised GEN 8 Policy, and guidelines to assist business units in meeting this requirement will be provided in the Information Security SOPs	Paragraph 1.0 states "Departments must define the data resources under their control and determine the appropriate access level of staff"	MIT-02 paragraph 3.0 states "Determine and authorize all levels of user access to support the business functionality"
d. Define the circumstances, methods, and approvals for taking data from Metro worksites	The revisions to the GEN 8 Policy will include guidelines for identifying and controlling all data/information taken outside of Metro worksites. More detailed procedures will be outlined in the Information Security SOPs that will be followed by all departments.	Paragraph 1.1 states "Sensitive documents may not be removed from LACMTA worksites unless for business use and the information content is properly logged and authorized by a department manager"	MIT-07 paragraph 1.5 states "Copying data to removable portable storage devices (example: USB thumb drives) requires prior approval by your management. Any data that is classified sensitive or personal can only be copied to an approved ITS secured storage device"
e. Specify the data security requirements when data is taken from metro worksites	The revision to the GEN 8 Policy will include guidelines for identifying and controlling all data/information taken outside of Metro worksites, which will include the use of encryption and/or password protection. Specific procedures will be outlined in the Information Security SOPs that must be followed by all business units.	Paragraph 1.1 states "Sensitive documents may not be removed from LACMTA worksites unless for business use and the information content is properly logged and authorized by a department manager. Use of encryption and/or password protection is required for access and use of LACMTA computers or other electronic devices storing electronic data files"	MIT-07 paragraph 1.5 states "Metro ITS department secures and maintains all computer (desktop/laptop) devices by providing security patches with the latest technology…When remote computing with a non-Metro issued device (such as a home computer), you must have updates security patches as well as a current Anti-Virus program installed" and "Copying data to removable portable storage devices (example: USB thumb drives) requires prior approval by your management. Any data that is classified sensitive or personal can only be copied to an approved ITS secured storage device."

Status of Implementation of Corrective Actions
Follow-up Review of Department Information Security

Recommendation 4

OIG Recommendation	Management Response	Original Policy (9/26/2002)	New Policy (8/17/2010)
a. Encryption and/or password protection for portable storage media	The revisions to the GEN 8 Policy will include guidelines for identifying and controlling all data/information taken outside of Metro worksites, which will include the use of encryption and/or password protection	Paragraph 1.5.3.3 states "If there is any need to copy electronic departmental records, they will advise the Records Coordinator. However, staff that as a regular part of their job duties develop records, regardless of form, may maintain such records in draft form on any MTA issued and owned electronic device"	Paragraph 1.1 states "Use of encryption and/or password protection is required for access and use of LACMTA computers or other electronic devices storing electronic data files"
b. Controls such as authorization or logs for sensitive data files taken outside of Metro worksites	The GEN 8 Policy will be revised to include the requirement for controls such as logs for sensitive data files taken outside of Metro worksites. Procedures for implementing this part of the policy will be included in the Information Security SOPs, and communicated and reinforced through the Records Management MOP training course	Paragraph 1.3 states "Each department will keep a list of all persons with approved access and their access levels"	Paragraph 1.1 states "Sensitive documents may not be removed from LACMTA worksites unless for business use and the information content is properly logged and authorized by a department manager."
c. Attaching Metro data files to emails	The revised GEN 8 Policy will prohibit attaching Metro data files to e-mails for non-business purposes	Paragraph 1.5.3.3 states "Employees shall not copy or retain MTA records for any unofficial or personal reason."	Paragraph 1.1.2 states "LACMTA e-mail is for business purposes only. Employees may not send or attach data files to e-mails and send or forward them outside of the LACMTA for non-business use."
d. Opening and/or saving metro data files on employee's personal computers	The current GEN 8 policy addresses opening or saving Metro data files on employees' personal computers in section 1.5.3.3 Employee Copying and Use of MTA Records, and section 1.5.3.4 Results of Using Personal Computers or Other Electronic Devices to do MTA Work. This will be included in the revised policy as well.	Paragraph 1.5.3.3 states "Each employee, through their continued employment shall agree that they have not and will not copy MTA records for any purpose that is not directly related to their job duties and responsibilities." 1.5.3.4 "Staff shall not work on or transfer any MTA record onto a non-MTA issued computer or other electronic device."	Paragraph 1.1 states "Employees may not copy, retain, or send LACMTA records or data files for any purpose not related to LACMTA business" 1.1.1 "Employees who transfer electronic data files onto a personal computer or other device may be subject to search and seizure at the direction of the LACMTA, or a court order, which could tie up an employee's use of their personal computer or personal device until searched and relevant files are copied and removed."

Final Report Distribution

Board of Directors

Antonio R. Villaraigosa, Board Chair
Michael D. Antonovich
Diane DuBois
John Fasana
José Huizar
Richard Katz
Don Knabe
Gloria Molina
Ara Najarian
Pam O'Connor
Mark Ridley-Thomas
Mel Wilson
Zev Yaroslavsky
Michael Miles, Non-voting Member

Metro

Chief Executive Office
Ethics Officer/Acting Inspector General
County Counsel
Board Secretary
Chief Administrative Services Officer
Chief Information Officer
Executive Officer, Administration
Deputy Executive Officer, General Services
Policy Research and Library Services Administrator
Manager, Records and Information Management
Deputy Chief Information Officer
Director, Information Management
Information Security Officer
Chief Auditor