THE METROPOLITAN WATER DISTRICT
OF SOUTHERN CALIFORNIA

Report
Office of the General Auditor
July 31, 2013

Internal Audit Report for July 2013

Summary

One report was issued during the month:

- **Application Security Controls Audit Report**

Discussion Section

This report highlights the significant activities of the Internal Audit Department during July 2013. In addition to presenting background information and the opinion expressed in the audit report, a discussion of findings noted during the examination is also provided.

Application Security Controls Audit Report

Background

Metropolitan uses more than 20 application systems to support operations such as monitoring water quality, managing water supply, forecasting long-range water demand, and maintaining critical infrastructure. The Information Security Team is responsible for establishing information security policies, procedures, and standards to prevent unauthorized changes to data maintained on these systems.

The Information Technology Section designates a functional manager with the overall responsibility for the ownership of each of its business and financial computer applications. In this role, the System Owner has the responsibility for ensuring that the application's capabilities meet business needs. In addition, they are responsible for providing leadership and direction regarding system development, enhancement, and ongoing operations ensuring that appropriate application controls are in place.

With regard to access controls, the System Owner establishes criteria for controlling user access to the various features of the system including the prerequisites required to be met prior to granting user access to specific system roles. With the support of the Information Security Team, they validate that user access and assigned roles and permissions are consistent with business need.

Opinion

In our opinion, the administrative procedures over application security controls include those practices usually necessary to provide for a generally satisfactory internal control structure. The degree of compliance with such policies and procedures provided effective control for the period between January 1, 2011 and May 31, 2013.

Comments and Recommendations

FORMAL LOG REVIEW AND INCIDENT HANDLING PROCEDURES

Information regarding security incidents resides within the event logs of networks and application systems. An effective log review process can help detect the occurrence of a security incident.

Prompt response to incidences and formal incident handling procedures may prevent a greater breach when those procedures are followed. Metropolitan should have formal log review and handling procedures to respond to security violations and incidents. During our review, we could not locate documented log reviews and incident handling procedures for use in the event of a security incident for the applications selected for the review.

We recommend that Information Security document formal log reviews and incident handling procedures.

USER ACCOUNT MANAGEMENT

Compliance with Metropolitan's Operating Policies and Computing Security Standards is necessary to ensure a secure and consistent access-control environment. Established policies and standards ensure Metropolitan systems and data are properly safeguarded from intentional and unintentional alterations. Operating Policy I-01, Security of Computer Resources, requires accounts of separated employees to be deactivated timely to ensure that only authorized personnel have access to Metropolitan systems.

During our review, we noted that one Oracle user-account belonging to an employee, separated from Metropolitan in December 2012, was not deactivated at the time of testing. It should be noted that this account had Oracle administrator-access privileges. Information Security has since deactivated the account.