MWD
METROPOLITAN WATER DISTRICT OF SOUTHERN CALIFORNIA

Report
February 28, 2005
Office of the General Auditor

- **Internal Audit Report for February 2005**

Summary

- **Metropolitan Water District Network Security Audit Report**

Detailed Report

This report highlights significant activities of the Internal Audit Department during February 2005. In addition to presenting the opinions expressed in the audit report, background information and discussions of findings noted during the review are presented.

MWD Network Security Audit Report

Opinion
In our opinion, the network security practices and procedures over the Management Network provide for a less than satisfactory internal control structure. This opinion is the result of concerns related to the lack of formally documented security policies and procedures and the deployment and management of network security controls as of October 31, 2004. It should be noted that management has initiated immediate remedial actions in response to our concerns. In other instances, they have initiated proactive action plans to address the weaknesses noted. We commend IT management for their quick response to these issues and intend to work with them in evaluating permanent solutions to these internal control structure concerns.

Background
The Information Technology (IT) Section of the Corporate Resources Group is responsible for managing information and technology infrastructures including network security controls. Network security controls are the countermeasures to prevent, detect, and remedy security violations and incidents that could negatively impact Metropolitan's information assets. These events could result in disclosure of confidential data, operation breakdowns, and/or service disruptions. Adequate and effective security controls are required to protect Metropolitan's information assets from being compromised by Internet attackers and/or unauthorized internal users.

Metropolitan has two primary networks: the Management Network and the Supervisory Control and Data Acquisition (SCADA) Network. The Management Network supports and hosts data, files, application systems and software that support Metropolitan's daily operations, such as Oracle Financial, PeopleSoft Human Resources, and other such systems. The SCADA Network supports the online/real-time application that manages Metropolitan's water resource operations. The SCADA Network was not included as part of this review.

Comments and Recommendations

Specific concerns regarding the MWD Network Security are presented in detail. Again, we commend Information Technology (IT) Management for their quick response to these issues and intend to work with them in evaluating effective solutions to these control concerns. It is important to note that IT had completed more than 70% of the remediation action by the time of the issuance of the audit report. We also noted that IT has contracted with a vendor to complete a security vulnerability assessment that will complement the work done for this audit. We understand that this assessment is in process. The comments and recommendations are:

Information Security Policies and Procedures

Information security policies and procedures should be established, formally documented and implemented to provide a framework for achieving adequate security controls. IT Section policies and procedures should provide Metropolitan with consistent structured security guidelines for the various information system platforms, assist in establishing security countermeasures to mitigate against internal and external threats, and provide a baseline to manage unexpected security violation incidents. During our review, we noted that the existing information security policies and procedures were inadequate for the following:

1) Data sensitivity and confidentiality classification policy and standards,

2) Patch management practices for security updates and "hotfixes" for Cisco routers/firewalls, Microsoft Windows, HP UNIX, Sun Solaris and other operating system level software.

3) Policies and procedures to regulate wireless communication.

4) Enhancement of the existing password management policies.

5) Formal policies or procedures relating to modem usage.

Lack of a confidentiality policy could result in unauthorized disclosure of sensitive data and may violate regulations and state laws. In addition, lack of a standardized patch management process may result in security holes or bugs in the production servers. Further, lack of a wireless communication policy could result in unauthorized access to production servers. Lack of strong password practices may contribute to unauthorized access to sensitive information. Finally, unregistered or unattended modems may allow attackers to gain unauthorized access to Metropolitan's Management Network.

We recommend IT document and officially publish these policies and procedures.

Network Infrastructure Security

Network equipment and software should be properly configured to reduce security vulnerabilities. Proper configuration includes preventive and/or detective countermeasures to safeguard Metropolitan's information assets from sabotage, abuse, and disclosure to unauthorized parties.

During our review of security control over perimeter routers, firewalls and intrusion detection devices we noted:

- Enhancements need to be made to the existing Intrusion Detection System (IDS) devices.

- Removal of the two identified security vulnerabilities on Metropolitan's Internet demilitarized zone (DMZ) should be implemented.

- Restrictions of Telnet usage, adding warning banners on the router, and intrusion detection software should be installed on the selected laptop computers.

Lack of an effective network infrastructure could result in the unauthorized use, destruction, manipulation, etc. of Metropolitan's information assets. We recommend that IT initiate remediation actions to address these issues.

Microsoft Windows Servers/Operating System Security
Wide area networks (WAN) and operating systems should have effective security controls to safeguard Metropolitan's data, files, application systems and other information resources. Proper security controls include good authentication, authorization, and accounting processes that provide controls to prevent, detect and timely remedy security violations and incidents within the Management Network.

We performed a vulnerability scan on five Windows domain controllers, one application server, and one proxy server. The Microsoft Baseline Security Analyzer (MBSA), a tool recommended by Microsoft, was used. We noted security vulnerabilities and recommended IT perform corrective actions in the following areas: enhancements of security patch management practices, disabling guess accounts, proper management of administrator accounts, and resetting of "Restrict Anonymous" registry on the servers reviewed.

Hewlett-Packard (HP) UX Server/Operating System Security
Unix servers and operating systems should have effective security controls to safeguard Metropolitan's data, files, application systems and other information resources. Proper security controls include good authentication, authorization, and accounting processes that provide controls to prevent, detect and initiate timely remedial actions to correct security violations and incidents within the Management Network.

Our review of security controls on the HP-UX servers that host Oracle Financials and other application systems noted comments and recommendations in the following areas: installation of host-based intrusion detection tools, enabling logging and enhancing security settings on the system startup file.

Sun Solaris Servers/Operating System Security
Unix servers and operating systems should have effective security controls to safeguard Metropolitan's data, files, application systems and other information resources. Proper security

controls include good authentication, authorization, and accounting processes that provide controls to prevent, detect and initiate timely remedy actions to correct security violations and incidents within the Management Network.

We reviewed five Sun UNIX servers that have Peoplesoft and Water Resources Management applications. The reviewed servers include itsrv12, itsrv13, Glacier, Stream, and Niagara. The following observations were noted: lack of password expiration procedures, enabling logging, installation of host-based intrusion detection software, disabling unnecessary user accounts, disabling unnecessary system services, and restriction of “trusted relationship” usage between servers.