THE METROPOLITAN WATER DISTRICT OF SOUTHERN CALIFORNIA

BOARD ACTION

- Board of Directors
  Organization, Personnel and Technology Committee

5/10/2011 Board Meeting

8-5

Subject

Appropriate $1.47 million; and authorize the implementation of Supervisory Control and Data Acquisition Cyber Security Upgrades as identified in the Information Technology Strategic Plan (Approp. 15378). **[Any discussion of specific threats or facilities to be heard in closed session. Conference with Metropolitan's security operations manager – threat to public services or facilities; may be heard in closed session pursuant to Gov. Code Section 54957(a)]**

Description

This action authorizes the implementation of Supervisory Control and Data Acquisition (SCADA) Cyber Security Upgrades to reduce cyber security risks for Metropolitan's SCADA system by implementing additional countermeasures to help protect against unauthorized access.

Timing and Urgency

Staff recommends proceeding at this time with this project to help ensure that Metropolitan's SCADA system used to control the flow and treatment of water is adequately protected from cyber threats by implementing additional security software and hardware. The number of cyber incidents involving SCADA systems is growing and such systems are increasingly becoming the target of unauthorized access attempts. Therefore it is important that this initiative move forward at this time.

This project has been reviewed with Metropolitan's updated Capital Investment Plan (CIP) prioritization criteria, and is categorized in the Information Technology System - Security Program. This project is budgeted within Metropolitan's CIP for fiscal year 2010/11.

Background

Cyber security is a high priority and is a key part of the Information Technology Strategic Plan (ITSP). Maintaining a secure computing environment requires regular enhancements and upgrades to Metropolitan's IT information security infrastructure to ensure protection against continually evolving cyber threats. New vulnerabilities are identified on a regular basis and require ongoing efforts to analyze risks and to implement countermeasures to protect against them to maintain the security and reliability of our systems.

Metropolitan utilizes a SCADA system to control the flow and treatment of water. It is comprised of instrumentation, hardware, software, and data networks that run 24/7 throughout the distribution system, Colorado River Aqueduct, and treatment plants. The SCADA system also supplies information for more than 80 core business functions at Metropolitan. Any compromise or attack of the SCADA system could cause major damage and disruption to the flow and treatment of water.

The number of industrial SCADA cyber security incidents has increased according to a 2010 report by the Security Incidents Organization (SIO), a group that tracks accidental and intentional cyber-related incidents. While there were an average of approximately 14 such incidents per year over the last 10 years that number now averages 40 new incidents per year. The power and water industries experience the majority of such incidents.

In 2010, the arrival of the Stuxnet worm/virus was a watershed in the cyber security world as it was the first time a sophisticated computer program was written to specifically target Programmable Logic Controllers (PLCs), common components used in many SCADA systems. Stuxnet was able to slip by detection technologies to affect control systems in nuclear facilities in Iran.

Metropolitan makes a concerted effort to be proactive in protecting the SCADA system. A number of measures have been instituted, including a regular program to apply security patches, antivirus protection, biometric-based access control, intrusion detection, etc. It is important that Metropolitan continue to be vigilant in its efforts and institute new cyber security best practices as they are developed in that new types of threats are being identified on an ongoing basis.

In October 2006, the Board approved a cyber security initiative which focused primarily on implementing cyber security countermeasures on Metropolitan's business network. Some of the best practice cyber security measures implemented included additional firewalls, enhanced virus protection, and intrusion prevention systems. This appropriation further enhances SCADA cyber security by transitioning countermeasures now implemented on the business network to the SCADA environment, following best practices to address ongoing and evolving threats. Staff has already deployed several improvements after having attended advanced hands-on SCADA cyber security training sponsored by the Department of Homeland Security. Lessons learned and best practices from the technical training have been incorporated into the plan to better secure Metropolitan's SCADA systems.

The SCADA Cyber Security upgrades will strengthen cyber software security countermeasures on the SCADA network by implementing best practices upgrades and by validating previous efforts. The milestones include: (1) further segregating the SCADA and Business Networks; (2) conducting an independent validation of the effectiveness of the segregation and completing the design for implementing additional measures; (3) implementing additional countermeasures on the SCADA network, as appropriate; and (4) conducting independent validation once installations are complete. Some of these cyber software countermeasures include:

Secure Remote Access

This will provide a highly secure and encrypted way to access SCADA remotely. It is important to provide access to SCADA, particularly during off-hours for support staff. It is critical that such connections are not vulnerable to unauthorized intrusions. The security mechanism already in place will be upgraded so that it is strengthened. This will enable the programming staff and support personnel to have secure, authenticated, remote access to the SCADA system.

Network Risk Management

This software will provide Metropolitan with the ability to conduct automated SCADA security self-assessments on an ongoing basis to augment periodic third-party vulnerability assessments. This will reduce risk by automatically identifying system vulnerabilities and proactively alerting staff for prompt response. The system will provide staff with the ability to triage identified risks and to prioritize and apply SCADA software updates in a controlled and timely manner to protect critical SCADA software from new security vulnerabilities.

Security Device Management

This software helps protect against unauthorized and undetected changes to critical SCADA network devices. This software acts as a "trip-wire" on the devices, automating the early detection of changes being made to SCADA network components which will be an improvement over the current method. The benefit is reducing the risk of downtime or vulnerabilities being introduced through unauthorized changes to the SCADA network.

Database Monitoring

This software provides the ability to proactively monitor changes to the SCADA database. It acts as a "trip-wire," alerting staff if unauthorized modifications are made to the SCADA databases. This will reduce the risk of intentional or unintentional changes being introduced to critical SCADA data.

Security Event Management

This software will automatically consolidate and analyze information from SCADA-related security monitoring systems described above and alert Metropolitan staff of any anomalies to ensure prompt analysis of the incident and appropriate corrective action. To date, we have relied on analyzing alerts and reports from the various SCADA-related security monitoring systems in place. As additional monitoring capabilities will be implemented as part of this initiative and the amount of data to be analyzed will increase accordingly, it is important to have a software tool to consolidate and automatically analyze the information to quickly identify anomalies. The Security Event System will serve as a central monitoring and alerting center for security-related SCADA system events.

Summary

This action appropriates $1.47 million (**Attachment 1**) and authorizes the design and implementation of SCADA cyber security enhancements, purchase of security-related software and hardware tools, and validation of the implementation of best practice cyber security measures. The appropriated funds include $685,000 for labor for staff to select, test, and deploy cyber security upgrades; $452,000 for hardware and software; $199,000 for professional services to create a design for the implementation of cyber security upgrades and to perform independent validation that the countermeasures implemented are working as designed; and $134,000 for remaining budget. Specialized technical assistance will be provided by consulting firms selected through a competitive process to perform various elements of the work as the different components may require different skill sets. It is anticipated that these consulting agreements will be awarded under the General Manager's contracting authority.

This project has been reviewed with Metropolitan's updated Capital Investment Plan (CIP) prioritization criteria, and is categorized in the Information Technology System - Security Program. This project is budgeted within Metropolitan's CIP for fiscal year 2010/11.

This project is consistent with Metropolitan's goals for sustainability by enhancing the cyber security of Metropolitan's SCADA systems in order to maintain reliable water deliveries in the future.

Project Milestones

September 2011 – Completion of preliminary design of SCADA cyber security enhancements

June 2012 – Completion of purchase and testing of security-related software and hardware tools

December 2012 – Completion of independent validation of SCADA cyber security enhancements

Policy

Metropolitan Water District Administrative Code Section 5108: Appropriations

California Environmental Quality Act (CEQA)

CEQA determination for Option #1:

The proposed action is not defined as a project under CEQA because it involves continuing administrative activities, such as general policy and procedure making (Section 15378(b)(2) of the State CEQA Guidelines). In addition, the proposed action is not subject to CEQA because it involves other government fiscal activities, which do not involve any commitment to any specific project, which may result in a potentially significant physical impact on the environment (Section 15378(b)(4) of the State CEQA Guidelines).

The CEQA determination is: Determine that the proposed action is not subject to CEQA pursuant to Sections 15378(b)(2) and 15378(b)(4) of the State CEQA Guidelines.

CEQA determination for Option #2:

None required

Board Options

Option #1

Adopt the CEQA determination and

a. Appropriate $1.47 million in budgeted funds; and
b. Authorize the SCADA Cyber Security Upgrades initiative.

Fiscal Impact: $1.47 million of budgeted funds under Approp. 15378 and approximately $80,000 for ongoing yearly maintenance for implemented cyber security software.

Business Analysis: This option will reduce cyber security risks for Metropolitan's SCADA system by implementing additional countermeasure to help protect against unauthorized access; to assist staff in addressing new vulnerabilities as they are identified; and to alert staff in the event that an intrusion occurs so immediate action can be taken.

Option #2

Do not implement the SCADA Cyber Security Upgrades initiative. Perform mitigation efforts under O&M funds as they are available.

Fiscal Impact: No additional expenditure of budgeted capital funds. Expenditure of O&M funds to phase in measures over time as budgets permit.

Business Analysis: In this option, staff will continue to rely on existing security measures in place and perform ongoing cyber security monitoring, Metropolitan will operate at a higher level of risk than in Option #1 because additional countermeasures will not be put in place to strengthen the SCADA system's protection to quickly address new security vulnerabilities as they arise.

Staff Recommendation

Option #1

Roy L. Wolfe — 4/18/2011
Roy L. Wolfe — *Date*
Manager, Business Technology

Jeffrey Kightlinger — 4/26/2011
Jeffrey Kightlinger — *Date*
General Manager

Attachment 1 – Financial Statement

Ref# bt12610803

Financial Statement for Information Technology System - Security Program

A breakdown of Board Action No. 5 for Appropriation No. 15378 for the SCADA Cyber Security Upgrades project is as follows:

	Previous Total Appropriated Amount (Oct. 2006)		Current Board Action No. 5 (May 2011)	New Total Appropriated Amount
Labor	$ 1,923,004	*	$ 685,000	$ 2,608,004
Materials and Supplies	957,260	*	452,000	1,409,260
Incidental Expenses	29,823	*	-	29,823
Professional Services	1,140,232	*	199,000	1,339,232
Operating Equipment	73,083	*	-	73,083
Contracts	140,500		-	140,500
Remaining Budget	172,098	*	134,000	306,098
Total	**$ 4,436,000**		**$ 1,470,000**	**$ 5,906,000**

Funding Request

Program Name:	15378 – Information Technology System - Security Program		
Source of Funds:	General Funds		
Appropriation No.:	15378	**Board Action No.:**	5
Requested Amount:	**$** 1,470,000	**Capital Program No.:**	15378
Total Appropriated Amount:	**$** 4,436,000	**Capital Program Page No.:**	292
Total Program Estimate:	**$** 5,906,000	**Program Goal:**	Infrastructure Reliability & Stewardship

* Includes previous reallocation of $196,000 from Remaining Budget to Labor, Materials and Supplies, Incidental Expenses, Professional Services and Operating Equipment and includes a correction for a typographical error in Action No. 4 in October 2006.