SCADA Cyber Security Audit Report

Office of the General Auditor

Audit & Ethics Committee

January 23, 2018

SCADA Cyber Security Audit Report

Supervisory Control and Data Acquisition (SCADA) Network:

- Commercial application/network
- Enterprise-wide, real-time monitoring and control system
- Operates 24/7 throughout CRA, treatment plants and the conveyance and distribution system.
- Monitors and controls remote terminal units (RTUs), programmable logic controllers (PLCs), instruments, and various operating systems.

Audit & Ethics Committee Meeting
January 23, 2018

SCADA Cyber Security Audit Report

SCADA is a mission critical computer system:

- Supplies information for more than 80 Metropolitan core business functions.
- Functions include water operations, maintenance management, geographic information systems, regulatory compliance, and power management.
- Operated and maintained by WSO in collaboration with the Information Technology Group

Audit & Ethics Committee Meeting
January 23, 2018

SCADA Cyber Security Audit Report

Audit Scope:

- Evaluated adequacy of cyber security controls
- Conducted vulnerability scans to identify potential weaknesses
- Examined intrusion detection and prevention mechanisms
- Reviewed user account and password management

SCADA Cyber Security Audit Report

Audit Scope (Continued):

- Assessed physical security for remote, unmanned SCADA devices
- Examined incident management procedures
- Reviewed the Cyber Vulnerability Assessment Reports performed by an outside security consultant in 2012 and 2015

SCADA Cyber Security Audit Report

Generally Satisfactory opinion with concerns

- **Management Reporting/Tone at the Top**
- **Vulnerability Management**
- **Physical Security Controls**

Audit & Ethics Committee Meeting
January 23, 2018

SCADA Cyber Security Audit Report

Management Reporting/Tone at the Top

- **Documentation could not be located:**
  - **Action plans to address concerns noted in the cyber vulnerability assessments of 2012 and 2015.**
  - **Discussion of the repeat findings included in the 2015 report.**
- **Communication of these reports along with a corrective action plan was not made to available executive management.**

SCADA Cyber Security Audit Report

Vulnerability Management

- **Scans of over 60,000 plug-ins identified vulnerabilities.**
- System log analysis and event monitoring procedures were not thoroughly documented.
- **Automated log analysis tool was not configured to provide immediate alerts.**
- Improvements needed in the use of dedicated intrusion detection devices.
- **Screen lockout time settings for SCADA operating systems and applications are not consistent.**
- One testing account ID in SCADA OnSite application was still active at the time of our review. (corrected)

SCADA Cyber Security Audit Report

Physical Security Controls

One SCADA RTU suffered three break-ins between the period of December 2015 and January 2016.

WSO reinforced the steel box enclosing the RTU after the second event and yet a third intrusion occurred.

Questions