



*Providing Outstanding Service Since 1963*

**Board of Directors**

Janna Orkney, Chair

Susan Pan, Vice Chair

Leon Shapiro, Director

Raymond Tjulander, Director

James Wall, Director

August 26, 2019

Board of Directors  
Triunfo Water & Sanitation District  
Ventura County, California

**DISCUSSION: SECURITY PROTECTION FOR DATA-WEBSITE-SCADA SYSTEMS**

**Summary**

At the June 24, 2019, Triunfo Sanitation District (District) Board Meeting, Chair Orkney requested that staff provide the District Board with an overview of the District's current plan for internet security for the website, District databases, and reservoir Supervisory Control And Data Acquisition (SCADA) systems.

The District's Information Technology (IT) services provider is FTI Services via a contract through Ventura Regional Sanitation District. FTI is responsible for maintaining the networks and databases for the District's computers, communication, and database systems. FTI has confirmed that the District's level of protection is very good in that it includes a comprehensive system of protocols that allows for secure networks while still maintaining flexible user controls and access

Current security protocols and incorporated software include:

- 1) Firewall protection and Iprism monitoring of sites
- 2) Antivirus from system level down to each workstation/connection
- 3) Barracuda filter for email traffic
- 4) Remote access via TSOPS has separate firewall and monitoring alerts
- 5) Great Plains (database) uses 3<sup>rd</sup> party certificate verification to authenticate and verify remote server access
- 6) SCADA is individually protected through Sierra Security and in compliance with Patriot Act and CDPH requirements for vulnerability assessments and protocols

FTI provides routine penetration testing on several of the systems but a more thorough and extensive assessment can be requested by outside parties for approximately \$2,000. In addition, there are other packages that could be employed to further encapsulate the system such as Alien (firewall and alerting) and SSL 256-bit encryption. However, as more protection is added the availability by staff to access networks becomes more difficult and restrictive with many outside internet providers limiting access if such protocols are in place.

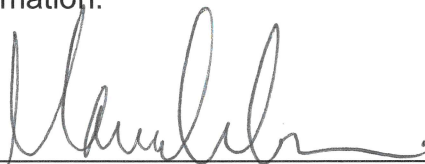
Sierra Security is the District's services provider for the SCADA system security and recently has recommended that the District upgrade its system to a more advanced level. The approximate cost for this upgrade is \$3,000.

In addition, the other internet based applications utilized by the District (i.e., SOHO, theAgency, Sensus Analytics, Paymentus, Diamond) all follow standard level security protocols and threat assessments and have indicated that they are current and secure.

Based on the current levels of protection used by FTI and the other providers, and coupled with the need to allow reasonable access to staff outside of the local network and lack of any previous cyber attacks, it is not recommended to add the additional layers of protection for the District's networks and systems. Staff does recommend upgrading the current software and protocols for the SCADA system for a cost of approximately \$3,000. In addition, a penetration test could also be performed for an approximate cost of \$2,000 if the Board so chooses.

Please contact me at 805-658-4621 or email [marknorris@vrzd.com](mailto:marknorris@vrzd.com) if you have any questions or need additional information.

REVIEWED AND APPROVED:



Mark Norris - General Manager

Attachment: None