STAFF REPORT

To: Honorable Mayor and Members of Town Council

Through: David L. Corliss, Town Manager

From: Mark Marlowe, P.E., Director of Castle Rock Water
Shawn Griffith, Assistant Director of Operations
Nicolas Van Kooten, SCADA Supervisor

Title: **Castle Rock Water (CRW) Cybersecurity Update** *[Serves entire Castle Rock Water Service Area]*

Executive Summary

As part of the 2025-2029 SCADA Master plan update requested by CRW, Tetra Tech's security team provided a proposal titled "Operational Technology Cybersecurity Projects". This document provides guidance and recommendations for improving and enhancing the security of CRW's Operational Technology (OT). The document references the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF) and the necessity to have the All Hazards Assessment completed to meet regulatory requirements for the America's Water Infrastructure Act (AWIA) Risk and Resiliency Assessment by March 31, 2025. This project will be integral to the SCADA Master Plan (MP) implementation.

Discussion

The assessment resulted in the following evaluation:

CRW requires a comprehensive, structured program to enhance operational technology (OT) cybersecurity, OT asset management, and operational reliability. The CRW OT Cybersecurity Program intends to mitigate cybersecurity risk by establishing an OT risk management strategy based on the NIST Cybersecurity Framework (CSF) 2.0. Both the EPA Cybersecurity Guidelines and the Cybersecurity and Infrastructure Security Agency Cross-Sector Cybersecurity Performance Goals (CPGs) align with the CSF.

The CSF emphasizes continuous assessment, protection, detection, and recovery, ensuring that water utilities are equipped to manage risks that could impact water quality and availability.

Addressing OT cybersecurity is essential for protecting public health, ensuring ongoing regulatory compliance, safeguarding critical infrastructure, and building resilience against increasingly sophisticated cyber threats. Aligning the OT cybersecurity program with the CSF not only strengthens the security of OT systems but also enhances operational efficiency, financial stability, and public trust in the utility.

The Scope of Work (SoW) outlines a multi-phase engagement to develop and implement robust OT security and resilience measures tailored to CRW's operational environment. The following tasks are aligned with the CSF's six core functions of **Govern**, **Identify**, **Protect**, **Detect**, **Respond**, and **Recover,** and align with EPA Cybersecurity Guidance. The tasks are prioritized in order and are not necessarily executed in the order of the CSF functions.

Task 1: The OT Cybersecurity - All Hazards Assessment: examines CRW's OT vulnerabilities for America's Water Infrastructure Act of 2018 (AWIA) compliance by March 31, 2025. Tetra Tech will deliver a risk assessment aligned with Cybersecurity and Infrastructure Security Agency (CISA) and Environmental Protection Agency (EPA) guidelines to provide CRW with a clear understanding of its OT risk landscape. The All Hazards Assessment Project was approved and awarded to Tetra Tech in January of 2025.

Task 2: OT Network Cybersecurity Improvements enhance CRW's OT network architecture by implementing the CSF "Protect" function. Key improvements will focus on network segmentation, secure access protocols, and OT firewall upgrades, reducing risks tied to outdated configurations and insufficient access controls.

Task 3: The OT Risk Management Strategy introduces a structured approach to assess, manage, and mitigate cybersecurity risks, aligning with the CSF. This strategy will equip CRW with a framework to prioritize resources and make informed, risk-based decisions that enhance resilience.

Task 4: The OT Incident Response, Disaster Recovery, and Continuity Plans developed to ensure CRW's rapid response and recovery capabilities in the event of a cyber incident. These plans will align with SDWA 1433 and EPA guidelines, enabling CRW to maintain critical OT operations and minimize disruption during adverse events.

Task 5: The OT Asset Management and Lifecycle Program establishes a comprehensive asset inventory and lifecycle management approach to mitigate risks related to unsupported or end-of-life OT equipment. This program will support CRW's compliance with resilience standards while enhancing operational reliability.

Task 6: The OT Cybersecurity Awareness Training Program helps foster a strong security culture. This training program will educate CRW personnel on the critical role they play in protecting infrastructure. This training program will align with the CSF to build the necessary knowledge, skills, and awareness to counter cybersecurity threats effectively.

Task 7: The OT Change Management Program establishes the process and procedures to minimize risks from system changes. It will include the development of change management forms and approval processes, a Change Advisory Board (CAB), and a change-tracking mechanism.

Task 8: The OT Patch Management Program establishes the processes, procedures, and technical measures to track component vulnerabilities, identify and vet available updates, and the methodologies to test and deploy software and firmware updates without impacting the availability of OT systems.

Task 9: OT Cybersecurity Policies and Procedures Development develops baseline OT cybersecurity policies and procedures for CRW, aligned with the CSF and NIST SP 800-82. This effort will enhance the security, resilience, and compliance of CRW's Operational Technology (OT) systems and staff, addressing both technical and human factor cybersecurity.

Through these targeted tasks, CRW will gain a comprehensive OT cybersecurity program that not only addresses immediate risks but also establishes sustainable practices for long-term resilience. Each task is strategically interlinked, reinforcing CRW's ability to respond to threats, manage risks, protect assets, and ensure operational continuity in compliance with regulatory standards. This program represents a proactive commitment to cybersecurity and a significant step forward in safeguarding CRW's critical infrastructure.

Currently, the SCADA system is isolated, segregated or commonly known as "air-gapped" and protected from external disruption by hackers and disruptive external (internet) forces. In lay terms, this translates to a complete inability for the SCADA system to connect to the outside world. However, there are cases where the outside world relies on internal data, thus CRW has installed Data Diodes as opposed to Firewalls. Data Diodes, known as unidirectional security gateways, combines hardware and software that ensure that only one-way (unidirectional) information transfers between two networks.

CRW has requested two additional SCADA staff positions: an OT SCADA Systems Administrator and an OT SCADA Network Administrator. The addition of these two positions will assist the CRW team in providing top cybersecurity, updated networks, and instrumentation, which includes the implementation of proper SCADA System programming, updates, and patching.

CRW has implemented security measures that effectively control infiltration from potential threats, an ongoing and dynamic process. With the assistance of specialized consultants and highly trained SCADA staff, CRW is committed to proactively defending its infrastructure and the Town's water supply against cyber threats and attacks.