City of McCleary

STAFF REPORT

To:	City Council
From:	Kevin Trewhella
Date:	August, 2026
Department:	Water and Wastewater

Water and Wastewater:

"With the groundwater table dropping for the summer, influent flow at the Wastewater Treatment Plant has decreased significantly to around 100,000 gallons per day. This reduction to typical summer flows provides an ideal operational window to complete pending plant projects much more efficiently.".

On July 30, 2026 the Federal Bureau of Investigation issued a Public Service Announcement regarding Malicious Cyber Actors Targeting Water and Wastewater Sector Internet-facing PLC's, Causing Operational Disruptions.

Here are the Key Highlights of the Alert.

☐ **Targeted Devices:** Malicious Cyber Actors (MCAs) are actively targeting internet-facing Operational Technology (OT) devices, specifically **Rockwell Automation/Allen-Bradley MicroLogix 1100 and 1400 series PLCs**.

☐ **Affected Sector:** Water and Wastewater Sector (WWS) utilities across at least seven states have reported incidents to the FBI, with some suffering operational degradation.

☐ **Attack Method:** Cyber actors remotely access internet-facing PLCs and change their IP addresses and passwords, leading to a direct loss of monitoring and control functionality.

At the Wastewater Treatment Plant, we utilize Rockwell SLC 500 series PLCs across our entire system. These units share the same core security vulnerabilities as the MicroLogix series currently highlighted in national cyber advisories, as both platforms rely on legacy RSLogix 500 messaging protocols lacking modern cybersecurity defenses. At the Water Treatment Plant, we run Square D PLCs, which have not seen similar targeted attacks.

While no network is entirely un-hackable, we can significantly reduce our risk profile by implementing basic OT security protocols. During a recent cybersecurity briefing hosted by an Air Force defense contractor, our 900 MHz radio telemetry link between the two well houses was identified as a notable security risk and point of vulnerability.

Proposed Action & Operational Benefit:

We can eliminate this security vulnerability and resolve ongoing communication failures by transitioning the communication loop between the well houses directly to our existing ethernet infrastructure improvement project that is currently on the proposed budget agenda for the Water Treatment Plant.

Beyond strengthening network security, this upgrade solves a costly operational problem. Currently, communication glitches across the 900 MHz radio link—such as the one experienced this past Tuesday evening—cause an estimated loss of **54,000 gallons (7,219** ft^3**)** of water per event at Well #3. Converting to ethernet will stabilize remote operations and stop these unforced water losses.

Additionally, there are a few key budget agenda items I would like to discuss with you:

- **Pani ZED Operational AI:** A specialized AI tool designed to assist plant operators by analyzing operational data in real time to optimize plant efficiency and lower operating costs.
- **SCADA System Upgrade:** Modernizing our primary control software to ensure reliable long-term operations, better monitoring, and enhanced cybersecurity.
- **Granular Activated Carbon (GAC) Filtration:** Following up on questions regarding options for water quality improvements, installing GAC filtration is the most effective solution to elevate our overall water quality.

I look forward to discussing these proposals and providing additional details at the meeting.

Kevin Trewhella