NATIONAL RURAL WATER ASSOCIATION
NRWA America's Largest Utility Membership

Mission Critical Global Alliance

MCGA & NRWA Joint Position Statement on Cybersecurity Readiness

On Monday, February 8, 2021, Sheriff Bob Gualtieri held a press conference surrounding the unlawful intrusion to the City of Oldsmar's water treatment system. During the press conference, Sherriff Gualtieri laid out the sequence of events:

- On Friday 5th February at approximately 8am an operator at a water treatment plant noticed someone accessing the control system Human Machine Interface (HMI) remotely. The operator was aware that his supervisor and other users routinely used remote access to view the HMI screen and so did not report the incident.
- At approximately 1:30pm on the same day, the operator noticed a user again accessing the HMI remotely. This time the user navigated through various screens and eventually modified the set point for sodium hydroxide (Lye) to a level that would be toxic to humans.
- The remote user logged off and the operator immediately reset the sodium hydroxide level back to normal. He then disabled remote access and reported the incident to the City and to local and state law enforcement.

There are over 145,000 active public water systems in the United States (including territories). Of these, 97% are considered small systems under the Safe Drinking Water Act, meaning they serve 10,000 or fewer people. Systems of the size of City of Oldsmar (15,000 population) have limited resources to manage the threat to their operations.

In the field of cybersecurity, guidance is often too complex or difficult to action. Experts provide lists of 20 or more points that need to be investigated, and many of these require specialist skills. Specialist service providers are often driven by their own business interests, focusing their services on technology at the expense of people and process.

MCGA and NRWA have produced this position statement to help provide simple guidance that will help all rural systems better manage their cybersecurity risk. There are many things that small and rural water and wastewater systems should do, but this statement outlines the top five actions that should be taken immediately. These actions should not require the involvement of third parties, or complex technical support. These actions are not the silver bullet that will address all cybersecurity risks, but they will greatly reduce the exposure most organizations have today.

What are my cybersecurity risks?

Ransomware on computers can impact operations due to loss of systems or data, but incidents involving SCADA systems can have much more severe consequences. As the City of Oldsmar incident shows, cybersecurity incidents at water treatment facilities can have the potential to cause serious harm to the public. They can also result in significant damage to plant, major outages, harm to the environment, serious regulatory actions, and major negative publicity.

Who is most likely to cause a cybersecurity incident at my facility?

Many people believe cybersecurity incidents only arise from specialist hackers who are targeting their organization or nation states who want to disrupt society. In fact, rural systems are much

more likely to experience an incident through other causes. The following is the list of likely causes, in priority order:

- Authorized employee or contractor makes a mistake.
- Current or former disgruntled employee or contractor seeks revenge.
- Ransomware attack from organized crime or random individual.
- Targeted attack from nation state.

What should I do?

It is impossible to completely remove all cybersecurity risk. However, rural water and wastewater systems can take actions that will reduce the likelihood of an incident, or the consequences of that incident.

MCGA and NRWA recommends systems take the following actions immediately, in this order:

1. **Remove insecure remote access** - Delete from all SCADA servers and HMIs any remote access software such as Team Viewer, LogMeIn, Parallels, Chrome Remote Desktop, and Windows Remote Desktop. These types of applications provide full access to computer desktops which gives unauthorized users the same access as your local operators. Authorized users should only be able to access your SCADA resources through secure channels involving multiple layers of protection (virtual private networks, two-factor authentication, geofencing, etc.).
2. **Perform risk assessment** – Arrange with process specialists to conduct a review of the SCADA system capabilities and the risks with abuse of these capabilities. List all the capabilities that the system provides to operators (e.g., adjust sodium hydroxide level). Then assess what could happen if that capability is abused (e.g., sodium hydroxide level changed to toxic level) and the timescales for this abuse to create a serious situation (e.g., toxic water in the distribution network). Finally identify what controls are in place to detect such abuse and the timescales for this detection (e.g., online sensor detects pH level and will generate an alarm within a certain time period). The objective of this process is to ensure that controls are in place, independent of the SCADA system and individual operators, to detect abuse situations, local or remote, before they result in serious consequences. All processes involving individual decision making should follow the *four-eyes principle* where one person checks another's actions. Any gaps need to be resolved and this may involve a temporary oversight process until a permanent solution can be identified.
3. **Raise awareness** – Formal comprehensive training in cybersecurity would be ideal, but as a priority all rural systems should make their employees and contractors aware of the cybersecurity risks that exist, and the actions that they need to take to contribute to the mitigation of these risks: be aware of the risk and be vigilant; report any unusual activity on SCADA systems, or suspicious behavior of individuals; stop any insecure actions by individuals, such as use of unverified removable media, installation of additional software, or inappropriate use of equipment.
4. **Secure user accounts** – There are many things that can be done to secure accounts, but as a minimum, rural systems should: change all passwords for all user accounts; store new account details in a secure password manager tool (e.g., LastPass, KeePass); issue account details only to those individuals who need these details to perform their roles.

5. **Review leavers process** – One of the biggest risks rural systems face is from disgruntled former employees. Systems must ensure that the leaver process involves the following steps: collection of all devices and software owned by the organization; update of all user accounts that the leaver had access to, either deleting, suspending, or changing the password. The process needs to ensure these steps are taken immediately on announcement of resignation or termination.

MCGA and NRWA consider these actions essential for all member organizations. Undertaking these actions does not remove all cybersecurity risk, but it does reduce the risk considerably. There are many more actions that should be taken, and the cybersecurity risk continually changes. MCGA and NRWA will provide advice to rural and small water and wastewater systems on an ongoing basis, to help manage the risk.