Community Water System Emergency Planning Cybersecurity Guidance Document

The Drinking Water & Groundwater Bureau (DWGB) requires community water systems (CWSs) to submit and maintain an updated emergency plan (EP) per Env-Dw 503.21. Plans are due every six years, but they should be reviewed annually and updated as necessary. Please review this guidance document with these considerations in mind as you plan to update your EP. A copy of your water system's EP is due to DWGB by March 31, 2021.

CYBERSECURITY

Cyberattacks are a growing threat to critical infrastructure sectors including water systems. Many facilities have experienced cybersecurity incidents that led to an interruption of a business process or critical operation. Now is a good time to remind your staff to anticipate cyber threats including social engineering, phishing, and other cyberattack tactics that can result in a disruption of your billing system or supervisory control and data acquisition operations like SCADA.

Examples of cyberattacks can include…

- Interruption of treatment processes by unauthorized users accessing the system remotely to open and close valves, overriding alarms, or disabling pumps and other equipment.
- Compromised email system or website.
- Stolen customer information (personal data or credit card information) from the utility's billing department.
- Installation of malicious programs that can disable utility operations.

Compromised safety and security is a threat that remains on ALL systems and organizations. Please remember to be vigilant and ensure that your system incorporates safety and security as a regular part of operations. The COVID-19 pandemic has given an unprecedented opportunity to cyber attackers to hack and break down an organizations' IT infrastructure. Recently a water utility was impacted by an Egregor ransomware incident.

Recommended actions when it comes to ransomware (as recommended by WaterISAC):

- Revisit, review and discuss ransomware and data breach playbooks/policies/procedures, and keep them up-to-date. The CISA/MS-ISAC Ransomware Guide is a valuable resource to be used for prevention and response best practice guidance.
- Keep a reputable incident response firm on retainer before an incident occurs.
- Evaluate cyber insurance policies to confirm proper coverage.
- Send out security awareness reminders to all staff on how phishing is a very common initial infection vector for ransomware.
- Remind staff not to open attachments or click on links contained in emails, even if the email looks like it is from a trustworthy source. If they already have received and/or actioned a suspicious email, encourage them to report the event now.
- Check device and network logs and events for potential intrusions, and consider configuring alerts for changes to files.
- Test backups and restore procedures before you need them and make sure you have a valid tested copy stored offline.
- Report ransomware incidents to authorities (and WaterISAC).

Cyberattacks can happen at any time, and although we can never predict the timing or severity of a cyber-emergency, we can diminish the effects if you have a strong EP that is up-to-date and encompasses as many hazards as possible. Review the EPA Incident Action Checklist on Cybersecurity and consider adding this as an appendix in your EP.

Now in its 17th year, the National Cybersecurity Awareness Month (NCAM) campaign continues to raise awareness of the importance of cybersecurity, ensuring that all Americans have the resources to be safer and more secure online.

CYBERSECURITY RESOURCES

Water utilities must assess their risks and mitigate vulnerabilities. Below are resources to help maintain a safe and security water utility while reducing risks and mitigating potential impacts.

- EPA Baseline Information on Malevolent Acts for Community Water Systems
- WaterISAC Cybersecurity Fundamentals for Water and Wastewater Utilities
- AWWA Resources on Cybersecurity
- EPA Cybersecurity Incident Action Checklist
- CISA/MS-ISAC Ransomware Guide – valuable resource to be used for prevention and response best practice guidance.
- Water Sector Cybersecurity Brief for States – EPA developed this brief in cooperation with the Association of State Drinking Water Administrators' Security Committee to help state staff (or their designated assistance providers) start a conversation with utilities about cybersecurity.

CONTACT INFORMATION

A copy of your water system's EP is due to NHDES DWGB by March 31, 2021. We appreciate your efforts in maintaining your EP!

How to Submit your EP

By Email (preferred): stephanie.nistico@des.nh.gov

By Mail: Stephanie Nistico

NHDES Drinking Water & Groundwater Bureau

29 Hazen Drive, PO Box 95

Concord, NH 03302-0095

For more information on emergency planning please contact stephanie.nistico@des.nh.gov at (603) 271-0867.