IDEM

INDIANA DEPARTMENT OF ENVIRONMENTAL MANAGEMENT

We Protect Hoosiers and Our Environment.

100 N. Senate Avenue • Indianapolis, IN 46204
(800) 451-6027 • (317) 232-8603 • www.idem.IN.gov

Eric J. Holcomb
Governor

Brian C. Rockensuess
Commissioner

June 20, 2024

[redacted]

Dear [redacted]. [redacted]:

Re: Berne Water Department
PWSID# IN[redacted]
Indiana Water Sector Utility
Cybersecurity Program

The Indiana Department of Environmental Management (IDEM) is reaching out to all municipal drinking water systems to share the details of a cybersecurity assessment program for the water sector. The threat of cyber-attacks to critical infrastructure targets is growing daily, and the water sector has seen a sharp increase in recent months. Several Indiana utilities have been impacted within the past six months. In March, the Whitehouse sent a letter to all governors detailing the rising risks and threats to the water sector, and subsequently issued a mandate for all states to develop and submit a plan to address these risks.

The America's Water Infrastructure Act (AWIA) of 2018 requires drinking water systems serving populations of 3,300 or larger to both assess their system's vulnerabilities to physical and cybersecurity threats, and implement mitigation plans to address them. Additionally, they must update their emergency response plans accordingly, and must renew these activities on a 5-year basis.

Effective immediately, IDEM is initiating a program strongly encouraging municipal drinking water utilities to perform annual cybersecurity vulnerability assessments, and to take actions to mitigate identified vulnerabilities and increase the cybersecurity resilience of Indiana's water sector. If you serve a population of over 3,300 customers, this will simply mean increasing the frequency of your AWIA assessment schedule and as a result this will help meet the federal rule requirements when the next assessment cycle begins (2025/26). The annual assessment schedule is currently voluntary, but IDEM believes with the rising risks being seen in the water sector, requirements both federally and within Indiana are extremely likely to come to pass in the near future. Taking part in the annual assessment schedule will both increase your resilience and prepare your utility future regulatory programs.

Utilities can choose any assessment tool that fits their unique needs, but IDEM would highlight that there are free self-assessment tools tailored to the water sector and are readily available from the American Water Works Association (AWWA), and the U.S. EPA. The Indiana Chapter of the AWWA provides free training, funded by the Indiana Finance Authority, to train utility personnel to use the AWWA assessment tool. Information detailing where to learn about both assessment tools is attached to this letter.

Once you begin assessing your vulnerabilities, IDEM, U.S. EPA, the Cybersecurity and Infrastructure Security Agency (CISA), and many water sector partners stand ready to help you should you encounter issues requiring mitigations beyond your current capacities. IDEM is currently working with the Indiana Office of Technology, the Indiana Finance Authority, and the Indiana Department of Homeland Security to cultivate in-state resources to assist utilities with identifying and mitigating vulnerabilities. U.S. EPA has a multitude of guidance documents, a 24-hour cybersecurity hotline for questions, and supports a Continuing Education Unit (CEU) based assessment program administered through Technical Assistance providers for very small utilities. CISA offers a suite of services and guidance materials to water sector utilities that even includes remote penetration testing of internet facing devices.

In addition to completing regular vulnerability assessments, it is critical to make sure your utility is practicing good, basic cybersecurity hygiene. Employing strong password protocols, making sure all your system's internet-facing systems are password protected (and not using default passwords), using multifactor authentication, keeping software updated, and doing some regular form of basic awareness training for employees about things like "phishing", recognizing suspicious emails and links, avoiding social engineering schemes, and creating strong passwords. Also attached to this letter are two CISA guidance documents IDEM has provided to assist utilities in implementing some of these basic but essential practices that will make you much more prepared to recognize and avoid many of the most common cyber risks. Many of the recent high-profile cyber-attacks on water sector utilities could have been avoided by securing internet facing devices with passwords other than the default password.

In closing, IDEM hopes every utility will begin an annual assessment practice to identify potential cybersecurity vulnerabilities. If you do so, and encounter issues requiring mitigation steps beyond your capabilities, please contact IDEM and we will try to help you find support, guidance, and resources you need. We no longer live in a time where you can hope to be overlooked by cyber criminals. Acting now can help ensure you are not an easy target in the future.

If you have any questions, please contact Travis Goodwin at 317/234-7426 or by email at Tgoodwin1@idem.IN.gov.

Sincerely,

Matt Prater, Branch Chief
Drinking Water Branch
Office of Water Quality

cc: [redacted] County Health Department, e-copy
Travis Goodwin, DWB, IDEM e-copy
File