STATE OF CONNECTICUT
DEPARTMENT OF PUBLIC HEALTH

Deidre S. Gifford, MD, MPH
Acting Commissioner

Ned Lamont
Governor

Susan Bysiewicz
Lt. Governor

Environmental Health & Drinking Water Branch

DWS Circular Letter #2021-12

TO: **Public Water Systems and Certified Operators**

FROM: Lori Mathieu, Public Health Branch Chief, EHDW

DATE: February 10, 2021

SUBJECT: Cybersecurity Preparedness

Due to the cyber-attack on a water treatment plant in Florida on February 5th, 2021; the Environmental Protection Agency (EPA) and the Connecticut Department of Public Health (DPH) Drinking Water Section (DWS) are asking Public Water Systems (PWS's) and Certified Operators to review the following materials. The cybersecurity breech was performed by unidentified cyber actors who obtained unauthorized access to the Supervisory Control and Data Acquisition (SCADA) system used at a local municipality's water treatment plant, and altered the amount of multiple chemicals within the water treatment process.

EPA recommends that all water systems implement the mitigation measures listed below:

Recommended Mitigation:

- Restrict all remote connections to SCADA systems, specifically those that allow physical control and manipulation of devices within the SCADA network. One-way unidirectional monitoring devices are recommended to monitor SCADA systems remotely.
- Install a firewall software/hardware appliance with logging and ensure it is turned on. The firewall should be secluded and not permitted to communicate with unauthorized sources.
- Keep computers, devices, and applications, including SCADA/industrial control systems (ICS) software, patched and up-to-date.
- Use two-factor authentication with strong passwords.
- Only use secure networks and consider installing a virtual private network (VPN).
- Implement an update and patch management cycle. Patch all systems for critical vulnerabilities, prioritizing timely patching of Internet-connected systems for known vulnerabilities and software processing Internet data, such as Web browsers, browser plugins, and document readers.

Phone: (860) 509-7333 • Fax: (860) 509-7359
Telecommunications Relay Service 7-1-1
410 Capitol Avenue, P.O. Box 340308, MS#12DWS
Hartford, Connecticut 06134-0308
www.ct.gov/dph/publicdrinkingwater

The Federal Bureau of Investigation (FBI) is using Private Industry Notification (PIN) 20210209-001 ***"Cyber Actors Compromise US Water Treatment Facility."*** PIN 20210209-001 is being disseminated in order to help cyber security professionals and system administrators guard against the persistent malicious actions of cyber actors.

In addition, the Department of Public Health (DPH) Drinking Water Section (DWS) reminds water utilities to remain vigilant and evaluate system security. This includes both cybersecurity and physical security of system assets to protect operation of the critical services that the water sector provides. To assist with this, the Cybersecurity & Infrastructure Security Agency (CISA) has developed a new informational guide on a security strategy that provides a flexible framework to align cybersecurity and physical security functions including case studies, which can be accessed at: Cybersecurity and Physical Security Convergence Guide.

"See Something, Say Something"

Department of Public Health
Drinking Water Section

1-860-692-2333

Connecticut Intelligence Center (CTIC)

TIPS Line: 1-866-HLS-TIPS (1-866-457-8477) Web: www.ct.gov/sar
Email: ctic@ct.gov Text: TIPS711 Mobile App: CTSAFE

c: Deputy Commissioner Heather Aaron, MPH, LNHA, Department of Public Health
Certified Operators
Local Health Directors

Assist Visits and the Infrastructure Survey Tool

The Department of Homeland Security (DHS) conducts various assessments to identify vulnerabilities, interdependencies, capabilities, and cascading effects of impacts on the Nation's critical infrastructure to help critical infrastructure owners and operators better prevent, deter, and mitigate risk in an all-hazards environment. The effectiveness of these assessments depends on the voluntary collaboration of Federal, State, local, and private sector owners and operators.

Assist Visits

Assist Visits are a cornerstone of the voluntary outreach effort to critical infrastructure owners and operators. An Assist Visit, conducted by Protective Security Advisors (PSAs) alongside critical infrastructure facility representatives, establishes and enhances the DHS relationship with critical infrastructure owners and operators, informs them of the importance of their facility, and explains how their facility or service fits into its specific critical infrastructure sector. In addition, the Assist Visit provides an overview of the IP resources available to the facility to enhance security and resilience, and reinforces the need for continued vigilance. These relationships serve to increase communications and information sharing, enhance sector security, and provide facility owners and operators access to various Federal tools and resources.

Officials preparing to conduct an assessment at a facility (Source: DHS)

Infrastructure Survey Tool

One of these IP resources available to facility owners and operators is the Infrastructure Survey Tool (IST). The IST is a voluntary, web-based vulnerability survey conducted by the PSA to identify and document the overall security and resilience of the facility. The vulnerability survey information is provided to the owners and operators via the IST Dashboard and a written report. The survey data, which is composed of weighted scores on a variety of factors for specific critical infrastructure, is graphically displayed in the IST Dashboard that compares the data against similar facilities and informs protective measures, resilience planning, and resource allocation. In addition to providing a sector security and resilience overview, the Dashboards highlight areas of potential concern and feature options to view the impact of potential enhancements to protection and resilience measures. The written report, developed from the IST data, contains a description of the facility and its vulnerabilities as well as recommendations to mitigate identified vulnerabilities. The information is protected under the Protected Critical Infrastructure Information (PCII) Program and is used by DHS for steady-state analysis, special event planning, and incident management.

Contact Information

For more information on the Assist Visit, or to contact your local PSA, please email NICC@hq.dhs.gov.