

# STATE OF CONNECTICUT

## DEPARTMENT OF PUBLIC HEALTH

Manisha Juthani, MD  
Commissioner



Ned Lamont  
Governor  
Susan Bysiewicz  
Lt. Governor

Environmental Health & Drinking Water Branch

### DWS Circular Letter #2021-89

**TO:** Public Water Systems

**FROM:** Lori Mathieu, Public Health Branch Chief, EHDW

Handwritten signature of Lori J. Mathieu '21 in blue ink.

**DATE:** December 1, 2021

**SUBJECT:** Emergency Response Planning and Cybersecurity Risk Self-Assessment

[America's Water Infrastructure Act of 2018 \(AWIA\)](#) requires public water systems (PWS) serving more than 3,300 people to develop or update risk assessments and emergency response plans (ERPs). The law specifies the components that the risk assessments and ERPs must address and establishes deadlines by which water systems must certify to EPA completion of the risk assessment and ERP. AWIA requires that no later than December 31, 2021, each system serving more than 3,300 people to prepare or revise, where necessary, an emergency response plan that incorporates the findings of the assessment, and the plan shall include the strategies and resources to improve the resilience of the system, including the physical security and **cybersecurity** of the system.

Pursuant to Connecticut General Statutes (CGS) Section 25-32d, PWS supplying water to one thousand or more persons or two hundred fifty or more consumers shall prepare a water supply plan that includes contingency procedures for public drinking water supply emergencies, including procedures for sabotage prevention and response. Obviously, sabotage prevention and response plan should include **cyber-attack** prevention and response component.

The Regulations of Connecticut State Agencies (RCSA) Section 19-13-B102(w) requires that each community water system (CWS) that is not subject to the requirements in section 25-32d of the CGS shall prepare not later than August 17, 2016, an emergency contingency and response plan (ERP), and shall be kept up to date and on file at the CWS. **Cybersecurity** should be added as a component to the ERP.

Furthermore, the federal rule and the RCSA Section 19-13-B102(a) defines "**Significant deficiency**" to mean any situation, practice, or condition in a public water system with respect to



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

*Affirmative Action/Equal Opportunity Employer*



design, operation, maintenance, or administration that the department determines to be causing, or has the potential for causing, risks to health or safety of the public served by the system.

The Department wants to remind our PWSs of the afore-noted state and federal requirements and ask you to prepare and update your ERP to ensure that the cybersecurity prevention and response component is included in the ERP with emphasis on eliminating or minimizing the risk to health and safety of the public served by the system. Our sanitary engineers will be assessing your compliance with these requirements during the next routine sanitary survey of your PWS.

To assist you in developing your cybersecurity prevention and response plan component of your ERP, the Department is sharing this self-assessment [checklist](#), and urge you to reach out to [CISA](#) and [EPA](#) where resources are available to support you in your efforts to update your ERP. EPA is offering free, [confidential assessments and technical assistance](#) to interested PWSs. The assessment and assistance will focus on best practices on how to prepare for, respond to, and recover from a cyber incident. Adoption of these practices can reduce the likelihood that a cyber attack will be successful and allow a utility to recover from cyber attacks faster and at a lower cost. The assessment and assistance will include the development of a cyber action plan to guide the implementation of best practices. Also, Richard Berthao of CISA, who can be reached at 202-839-1429, E-Mail: [richard.berthao@cisa.dhs.gov](mailto:richard.berthao@cisa.dhs.gov) is willing to assist if your PWS is interested in cybersecurity presentations or assessments.

In addition, CISA, the Federal Bureau of Investigation (FBI), and the EPA published recently a joint advisory ([AA21-287A](#)) warning of “ongoing malicious activity—by both known and unknown actors” directed against water and wastewater treatment facilities. It emphasizes the threat of [spear-phishing](#) as well as exploitation of outdated operating systems and vulnerable control system firmware. The intent of the advisory is not indicative of increased malicious activity, but only highlights consistent activity observed against water and wastewater sector entities over the last several years. [The advisory](#) contains recommended mitigations, including immediate actions water and wastewater utilities can take now to protect against malicious cyber activity. Also, in light of the ongoing threat activity, [WaterISAC](#) and the EPA [recommend that all members and partners of the water sector review FBI PIN 20210317-001: \*Business Email Compromise Actors Targeting State, Local, Tribal, and Territorial Governments, Straining Resources\* and adopt the recommended mitigations](#). WaterISAC encourages any water utility who has experienced malicious or suspicious activity to email [analyst@waterisac.org](mailto:analyst@waterisac.org), call 866-H2O-ISAC, or use [the online incident reporting form](#)

For additional resources, please visit the [National Critical Functions Supply Water and Manage Wastewater webpage](#), which includes an announcement regarding this Joint Advisory along with additional resources – including two informative infographics – for Cyber Risks and Resources for the Water and Wastewater Sector.

c: Deputy Commissioner Heather Aaron, MPH, LNHA, Department of Public Health  
Local Health Directors  
Certified Operators  
Brenda Bergeron, Deputy Commissioner, DESPP  
Richard Berthao, CISA  
Jane Downing, EPA Region 1  
Jennifer McLain, EPA  
Jack Betkoski, PURA