STATE OF CONNECTICUT
DEPARTMENT OF PUBLIC HEALTH

Manisha Juthani, MD
Commissioner

Ned Lamont
Governor

Susan Bysiewicz
Lt. Governor

ENVIRONMENTAL HEALTH AND DRINKING WATER BRANCH

DWS Circular Letter# 2022-22

TO: Community Public Water Systems

FROM: Lori Mathieu, Public Health Branch Chief

DATE: March 22, 2022

SUBJECT: Cybersecurity and Infrastructure Security Agency (CISA) Unclassified Broad Stakeholder Call

---

The Department of Public Health Drinking Water Section is alerting Community Water Systems regarding the March 21, 2022 White House statement indicating there is now evolving intelligence that Russia may be exploring options for potential cyberattacks. The White House is emphasizing action to protect against potential cyberattacks. CISA is convening an Unclassified "Broad Stakeholder Call" today, March 22 to address impacts of the Russia-Ukraine situation on the U.S. Homeland. Community public water system owners and operators are encouraged to listen in to the call

Call Details

- Date/Time: **Tuesday, March 22, from 2 to 3 pm (EDT)**
- Audience: Critical infrastructure partners and stakeholders
- Dial-in Information: **800-857-6546**; Passcode: **2824553**

The following guidance has been emphasized with a greater sense of urgency:

- Mandate the use of multi-factor authentication on your systems including the lock down of privileged accounts and monitoring for anomalous account activity
- Deploy modern security tools on your devices to **continuously look for and mitigate threats.**
- Make sure **systems are patched and protected against all known vulnerabilities**, and **change passwords across your networks so that previously stolen credentials are useless to malicious actors**.
- **Back up** your data and ensure you have **offline backups**.
- Understand and be proficient in **incident response procedures (IRPs)** and **emergency plans** before an incident occurs, including practicing IRPs in tabletop exercises with emphasis on being prepared to **maintain continuity of operations**, specifically for any ICS/OT dependencies that could be disrupted and the sustaining of manual operations to maintain critical functions.
- **Encrypt** your data so it cannot be used if it is stolen.
- **Educate your employees** to common tactics that attackers will use over email or through websites, and **encourage them to report** if their computers or phones have shown unusual behavior, such as unusual crashes or operating very slowly.

Connecticut Department of Public Health

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

- **Drop the threshold for the sharing of information** regarding suspicious network activity – engage proactively with your local FBI field office or CISA Regional Office to establish relationships in advance of any cyber incidents. Organizations should report incidents and anomalous activity to CISA and/or the FBI via your local FBI field office or the FBI's 24/7 CyWatch at (855) 292-3937 or CyWatch@fbi.gov.

The Department of Public Health encourages all public water systems to report malicious or suspicious activities to CISA or CTIC@ct.gov /(860) 706-5500.

c. Deputy Commissioner Heather Aaron, MPH, LNHA, Department of Public Health