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# 2022-19

TO: Community Public Water Systems

FROM: Lori J. Mathieu, Public Health Branch Chief Lori J. Mathieu '22

DATE March 18, 2022

SUBJECT: Mitigating Threats Posed by Russian State-Sponsored Cyber Actors

The Department of Public Health (DPH) Drinking Water Section (DWS) is alerting the Community Water Systems regarding the joint Cybersecurity Advisory released by the Cybersecurity and Infrastructure Security Agency (CISA) and the Federal Bureau of Investigation (FBI) on March 15, 2022. All Community water system owners and operators should read this advisory and adopt the recommended mitigation actions if needed. The Cybersecurity and Infrastructure Security Agency (CISA) and the Federal Bureau of Investigation (FBI) released this joint Cybersecurity Advisory (CSA) [https://www.cisa.gov/uscert/ncas/alerts/aa22-074a] to warn organizations that Russian state-sponsored cyber actors have gained network access through exploitation of default multifactor authentication (MFA) protocols and a known vulnerability.

As early as May 2021, Russian state-sponsored cyber actors took advantage of a misconfigured account set to default MFA protocols at a non-governmental organization (NGO) allowing them to enroll a new device for MFA and access the victim network. The actors then exploited a known Windows Print Spooler vulnerability, "PrintNightmare" (CVE-2021-34527) to run arbitrary code and access the victim's Google cloud and email accounts for document exfiltration. One of the most important security practices to reduce the risk of intrusions remains MFA and every organizations should implement it for all users. MFA should be implemented according to best practices, such as reviewing default configurations and modifying as necessary, to reduce the likelihood that a sophisticated adversary can circumvent this control, as described in this CISA and FBI joint advisory.

Now, more than ever, organizations must put their Shields Up to protect against cyber intrusions. Actions that executives and leaders can implement to help protect against this Russian state-sponsored malicious cyber activity include enforcing MFA and then reviewing configuration policies; ensuring inactive accounts are disabled uniformly across the active directory and MFA systems; and patching all systems, especially prioritizing known exploited vulnerabilities [https://www.cisa.gov/known-exploited-vulnerabilities].

DWS encourages Public Water Systems to remain vigilant and lower the threshold for reporting. In the event of a cybersecurity incident, please contact at CTIC@ct.gov /(860) 706-5500 or Report a ransomware incident to the FBI.

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