STATE OF CONNECTICUT
DEPARTMENT OF PUBLIC HEALTH

Manisha Juthani, MD
Commissioner

QUI TRANSTULIT SUSTINET

Ned Lamont
Governor
Susan Bysiewicz
Lt. Governor

ENVIRONMENTAL HEALTH AND DRINKING WATER BRANCH

DWS Circular Letter# 2022-13

TO: Community Public Water Systems

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

DATE February 16, 2022

SUBJECT: Potential Cyber Threat to United States Critical Infrastructure due to Geopolitical Tensions

The Department of Public Health (DPH) Drinking Water Section (DWS) is alerting the Community Water Systems to new information regarding a potential cyber threat to United States critical infrastructure. All Community water system owners and operators should read this alert and attached advisories and adopt the recommended mitigation actions if needed.

Given the increased focus on the geopolitical landscape, CISA is proactively leaning forward to ensure that our industry partners are aware of all CISA resources available to combat potential threats. On January 11, we released a joint cybersecurity advisory (CSA) with the FBI and NSA about the Russian threat to U.S. critical infrastructure, including specific tactics, techniques, and procedures associated with Russian actors. We followed this advisory with an executive-level product urging every organization to take urgent, near-term steps to reduce the likelihood and impact of a potentially damaging compromise.

In an Intelligence Brief issued on January 23, 2022, the Department of Homeland Security (DHS) stated, "*We assess that Russia would consider initiating a cyber-attack against the Homeland if it perceived a US or NATO response to a possible Russian invasion of Ukraine threatened its long-term national security. Russia maintains a range of offensive cyber tools that it could employ against US networks—from low-level denials-of- service to destructive attacks targeting critical infrastructure.*" See attached DHS Office of Intelligence and Analysis, Intelligence in Brief, *Warning of Potential for Cyber Attacks Targeting the United States in the Event of a Russian Invasion of Ukraine* (DHS-IA-IB-2022-00927).

On February 11, 2022, National Security Advisor Jake Sullivan stated that new Russian forces continue to arrive at the Ukrainian border and that, "*we are in the window when an invasion could happen at any time*." If Russia takes military action against Ukraine, the response by the United States, "*would include severe economic sanctions with similar actions taken by the European Union, the United Kingdom, Canada and other countries.*" CISA, the FBI, and NSA encourage the critical infrastructure network defenders—to adopt a heightened state of awareness and to conduct proactive threat hunting, as outlined in the Detection section of the joint CSA. Additionally, CISA, the FBI, and NSA strongly urge network defenders to implement the recommendations detailed in the linked pdf. These mitigations will help organizations improve their functional resilience by reducing the risk of compromise or severe business degradation:

Keeping Connecticut Healthy
DPH
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
Affirmative Action/Equal Opportunity Employer

Accredited Health Department • Public Health Accreditation Board • PHAB Advancing public health performance

1. Be prepared. Confirm reporting processes and minimize personnel gaps in IT/OT security coverage. Create, maintain, and exercise a cyber incident response plan, resilience plan, and continuity of operations plan so that critical functions and operations can be kept running if technology systems need to be taken offline.

2. Enhance your organization's cyber posture. Follow best practices for identity and access management, protective controls and architecture, and vulnerability and configuration management.
3. Increase organizational vigilance. Stay current on information pertaining to this threat. Subscribe to CISA's mailing list and feeds to receive notifications when CISA releases information about a security topic or threat.

The *Cybersecurity and Infrastructure Security Convergence Action Guide* describes the complex threat environment created by increasingly interconnected cyber-physical systems, and the impacts that this interconnectivity has on an organization's cybersecurity and physical security functions. It also provides information that organizations can consider to adopt a holistic cyber-physical security approach through a flexible framework. The CISA Services Catalog | CISA provides information about all of the tools and resources CISA offers for both cyber and physical security.

Due to these current events, WaterISAC and the USEPA strongly encourage Water system owners and operators to maintain a heightened awareness for possible intrusions into their operational networks and to prepare to maintain critical operations if process control networks are disabled. Review the December 20, 2021, Advisory from WaterISAC and USEPA for tactics, techniques, and procedures used by Russian and Russian state-sponsored proxies and, where necessary, adopt the recommended mitigation actions to reduce risk from and build resilience to potential attacks. (See attached USEPA-WaterISAC Advisory, *Cybersecurity Recommendations in Consideration of the CISA/FBI/NSA Advisory on Russian State-Sponsored Cyber Operations Against U.S. Critical Infrastructure*). The USEPA and WaterISAC delivered a webinar recently to provide additional information on the Cybersecurity Recommendations Advisory that is located at the following link: https://www.waterisac.org/portal/dec21-jan22-epa-waterisac-webinars. To access the webinar recording, login to your WaterISAC account. If you are not a member, please request a free trial membership at https://www.waterisac.org/.

You can find all of our recent alerts and advisories on our alerts web page, including AA22-011A : Understanding and Mitigating Russian State-Sponsored Cyber Threats to U.S. Critical Infrastructure and AA21-200B : Chinese State- Sponsored Cyber Operations: Observed TTPs. CISA also maintains a dedicated public webpage providing an overview of the Russian government's malicious cyber activities as well as all of our advisories and products on Russian state- sponsored cyber threats.

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