December 20, 2021

U.S. ENVIRONMENTAL PROTECTION AGENCY-WaterISAC ADVISORY

To: Water and Wastewater Systems, SLTT Governments and Private Sector Stakeholders

(TLP:AMBER) Cybersecurity Recommendations in Consideration of the CISA/FBI/NSA Advisory on Russian State-Sponsored Cyber Operations Against U.S. Critical Infrastructure

On December 16, 2021, the Cybersecurity and Infrastructure Security Agency (CISA), FBI, and the National Security Agency (NSA) issued a joint advisory on Russian state-sponsored cyber operations against United States critical infrastructure (see attachment for advisory AA21-350B).

What is the Purpose of the CISA/FBI/NSA Joint Advisory?

The joint advisory describes commonly observed tactics, techniques, and procedures; detection actions; incident response guidance; and mitigations. It is intended to help critical infrastructure reduce the risk presented by these threats and to encourage the adoption of a heightened state of awareness during the holidays (a time when many disconnect from work).

The joint advisory complemented a December 15, 2021 CISA Insights publication - Preparing For and Mitigating Potential Cyber Threats. It asserted that due to persistent cyber-threats from sophisticated actors, including nation-states and their proxies, critical infrastructure owners and operators should take immediate steps to strengthen their computer network defenses. These actors have the capability to leverage network access for targeted operations with the potential to disrupt critical infrastructure functions.

What Actions are Recommended for Water and Wastewater Systems?

Water and wastewater system owners and operators should review the attached joint advisory and assess how to apply the recommended detection, incident response, and mitigation actions to their operations. Key actions for water and wastewater systems include the following:

1) **Require Strong, Unique Passwords.** Malicious cyber actors repeatedly use stolen or easily guessed credentials. Consider forcing a global reset of all passwords in your environment before staff begin taking time off.
2) **Implement Multi-Factor Authentication.** After changing passwords, make implementing multi-factor authentication (MFA) a priority. MFA significantly reduces your risk from almost all opportunistic attempts to gain entry into your systems.
3) **Address known exploited vulnerabilities.** This could include patching and/or additional controls such as network segmentation to protect vulnerable devices that cannot effectively be patched. CISA maintains a catalog of Known Exploited Vulnerabilities that utilities are encouraged to review to identify vulnerable systems. Also, prioritize network segmentation to prevent unauthorized access to your operational technology (OT) systems from the internet and to reduce connectivity between OT and vulnerable information technology (IT) systems.
4) **Surge Support.** Identify surge support for responding to an incident. Malicious cyber actors are known to target organizations on weekends and holidays when there are gaps in organizational cybersecurity.

5) **Network/Systems Awareness.** Be alert for unusual behavior in OT and IT systems, such as unexpected reboots of digital controllers and other OT hardware and software, and delays or disruptions in communication with field equipment or other OT devices. Enhance logging to investigate anomalous activity – including collecting more logs and increasing storage capacity and retention time.
6) **Backup Data.** Implement and test data backup procedures on both IT and OT networks and ensure copies of backups are isolated (stored offline) from the network.
7) **Incident Response Plans.** Create, maintain, and exercise a cyber incident response and continuity of operations plans.
8) **Manual Operations.** Have a resilience plan that addresses how to operate your system if you lose access to or control of critical OT or IT systems – including the ability to sustain manual operations for extended periods.

How Can I Learn More About the CISA/FBI/NSA Joint Advisory?

WaterISAC and EPA, in conjunction with water sector associations, will hold a TLP:AMBER webinar on the dates/times listed below to present and discuss the joint advisory. The webinar is intended for water and wastewater system owners and operators, along with state, local, tribal, and territorial (SLTT) government officials and private sector organizations that directly support water and wastewater system operations. Registration links for the webinar are provided. For those unable to join live, the webinar will be recorded and posted to the WaterISAC website for members and trial members.

- Date 1: Wednesday, December 29, 2021, 2:00 – 3:00 pm EST.
  Register: https://attendee.gotowebinar.com/register/8355582904364747792
- Date 2: Wednesday, January 5, 2022, 2:00 – 3:00 pm EST.
  Register: https://attendee.gotowebinar.com/register/5595566826088940559

Additional Resources

- Protecting Against Malicious Cyber Activity before the Holidays (White House; 12/16/21)
- Joint Cybersecurity Advisory Ongoing Cyber Threats to U.S. Water and Wastewater Systems (CISA, FBI, NSA, EPA; 10/14/21)
- WaterISAC's 15 Cybersecurity Fundamentals for Water and Wastewater Utilities
- U.S. EPA Cybersecurity Best Practices for the Water Sector
- AWWA Resources on Cybersecurity

WaterISAC Incident Reporting

WaterISAC encourages all utilities that have experienced malicious or suspicious activity to email analyst@waterisac.org, call 866-H2O-ISAC, or use the confidential online incident reporting form. Reporting to WaterISAC helps utilities and stakeholders stay aware of the threat environment of the sector.

TLP:AMBER Definition: *Recipients may only share TLP:AMBER information with members of their own organization, and with clients or customers who need to know the information to protect themselves or prevent further harm. For more information on the Traffic Light Protocol, see https://www.cisa.gov/tlp.*