

THE WHITE HOUSE
WASHINGTON

March 18, 2024

Dear Governor:

Disabling cyberattacks are striking water and wastewater systems throughout the United States. These attacks have the potential to disrupt the critical lifeline of clean and safe drinking water, as well as impose significant costs on affected communities. We are writing to describe the nature of these threats and request your partnership on important actions to secure water systems against the increasing risks from and consequences of these attacks.

Two recent and ongoing threats illustrate the risk that cyberattacks pose to the nation's water systems:

- Threat actors affiliated with the Iranian Government Islamic Revolutionary Guard Corps (IRGC) have carried out malicious cyberattacks against United States critical infrastructure entities, including drinking water systems. In these attacks, IRGC-affiliated cyber actors targeted and disabled a common type of operational technology used at water facilities where the facility had neglected to change a default manufacturer password. See [Exploitation of Unitronics PLCs used in Water and Wastewater Systems | CISA](#) for further information on these attacks.
- The People's Republic of China (PRC) state-sponsored cyber group known as Volt Typhoon has compromised information technology of multiple critical infrastructure systems, including drinking water, in the United States and its territories. Volt Typhoon's choice of targets and pattern of behavior are not consistent with traditional cyber espionage. Federal departments and agencies assess with high confidence that Volt Typhoon actors are pre-positioning themselves to disrupt critical infrastructure operations in the event of geopolitical tensions and/or military conflicts. See [PRC State-Sponsored Actors Compromise and Maintain Persistent Access to U.S. Critical Infrastructure](#) for further information.

Drinking water and wastewater systems are an attractive target for cyberattacks because they are a lifeline critical infrastructure sector but often lack the resources and technical capacity to adopt rigorous cybersecurity practices. As the Sector Risk Management Agency identified in Presidential Policy Directive 21 for water and wastewater systems, the U.S. Environmental Protection Agency (EPA) is the lead Federal agency for ensuring the nation's water sector is resilient to all threats and hazards. Partnerships with State, local, tribal, and territorial governments are critical for EPA to fulfill this mission. In that spirit of partnership, we ask for your assistance in addressing the pervasive and challenging risk of cyberattacks on drinking water systems.

We need your support to ensure that all water systems in your state comprehensively assess their current cybersecurity practices to identify any significant vulnerabilities, deploy practices and controls to reduce cybersecurity risks where needed, and exercise plans to prepare for, respond to, and recover from a cyber incident. In many cases, even basic cybersecurity precautions – such as resetting default passwords or updating software to address known vulnerabilities – are not in place and can mean the difference between business as usual and a disruptive cyberattack. The Department of Homeland Security’s Cybersecurity and Infrastructure Security Agency’s (CISA) website has a [list of actions](#) water and wastewater systems can take to reduce risk and improve protections against malicious cyber activity.

Additionally, both EPA and CISA offer [guidance, tools, training, resources, and technical assistance](#) to help water systems to execute these essential tasks. Further, cybersecurity support and technical assistance are available from private sector associations like the American Water Works Association, the National Rural Water Association, and the Water Information Sharing and Analysis Center. State leadership and messaging to connect water systems with these tools and resources is essential to ensure that utility leaders assess and mitigate critical cyber risks. Your state Homeland security advisors are a resource, as they have links into Federal cybersecurity efforts and access to relevant information about these threats.

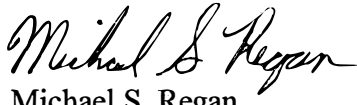
We will invite your Environmental, Health and Homeland Security Secretaries to participate with us in a convening to discuss the improvements needed to safeguard water sector critical infrastructure against cyber threats. This meeting will highlight current Federal and state efforts to promote cybersecurity practices in the water sector, discuss priority gaps in these efforts, and emphasize the need to take immediate action. We will provide details about this convening to your teams shortly.

Additionally, EPA will engage the Water Sector and Water Government Coordinating Councils to form a Water Sector Cybersecurity Task Force, which will build on recommendations from your Environmental, Health and Homeland Security Secretaries. The Task Force will identify the most significant vulnerabilities of water systems to cyberattacks, the challenges that water systems face in adopting cybersecurity best practices, and near-term actions and long-term strategies to reduce the risk of water systems nationwide to cyberattacks.

The White House and EPA are hopeful that the efforts outlined in this letter, and others we may undertake together, will protect the water systems from cyberattacks and prevent the need to use other Federal authorities.

In recognition of the significant risk that cyberattacks pose for mission critical water utility operations, we appreciate your attention to this important issue and thank you for your partnership. If you or your staff would like to engage with the EPA or the National Security Council staff on any aspect of this request, please contact Deputy Director of the EPA Janet McCabe and Deputy National Security Advisor for Cyber and Emerging Technologies Anne Neuberger at the National Security Council at mccabe.janet@epa.gov and anne.neuberger@nsc.eop.gov.

Sincerely,



Michael S. Regan
Administrator
Environmental Protection Agency



Jake Sullivan
Assistant to the President for
National Security Affairs