# EPA warns of rising cyberattacks on U.S. water utilities, urges immediate action



The Environmental Protection Agency (EPA) issued a warning on May 20, 2024, about increasing cyberattacks on U.S. water utilities, urging immediate actions to safeguard the nation's drinking water. Over the past year, about 70% of inspected utilities failed to meet cybersecurity standards, exposing vulnerabilities that adversaries such as Russia and Iran have exploited.

Basic lapses, including unchanged default passwords and retained system access for former employees, were highlighted as significant risks. Cyberattacks on water systems could interrupt treatment processes, damage infrastructure, and compromise water safety.

The EPA's enforcement alert stressed that even small water systems must enhance cybersecurity measures. Named adversaries include China, Russia, and Iran, with recent incidents linked to these nations: Iranian group "Cyber Av3ngers" targeted a small Pennsylvania town’s water provider, Russian "hacktivists" attacked Texas utilities, and the Chinese group Volt Typhoon compromised IT systems within U.S. critical infrastructures.

The Biden administration's broader strategy to defend critical infrastructure includes this cybersecurity push. EPA Administrator Michael Regan and National Security Advisor Jake Sullivan have called on states to formulate cybersecurity plans for water systems. Regulatory challenges persist, with states like Missouri, Arkansas, and Iowa contesting the EPA's authority under the Safe Drinking Water Act.

Efforts to improve cybersecurity are ongoing, with EPA offering free training and advocating for comprehensive planning and updated protections. Financial and staffing constraints in small communities present significant hurdles, emphasizing the need for federal support and coordinated policy development.