Iran Conflict is Increasing the Likelihood of Low-Level Cyberattacks Against US Networks

The U.S. EPA is issuing this alert to inform water and wastewater system owners and operators of the need for increased vigilance for potential cyber activity in the United States due to the current geopolitical environment. The U.S. Department of Homeland Security (DHS) published a National Terrorism Advisory System Bulletin, indicating that low-level cyberattacks against U.S. networks by pro-Iranian hacktivists are likely, and cyber actors affiliated with the Iranian Government may conduct attacks against U.S. networks. Additionally, the Cybersecurity and Infrastructure Security Agency (CISA) published a fact sheet warning that Iranian-affiliated cyber actors may target U.S. devices and networks for near-term cyber operations.

Iranian-affiliated cyber actors have demonstrated the ability to exploit operational technology (OT) devices at U.S. water and wastewater systems, forcing many systems to revert to manual operations and resulting in operational impacts.

Mitigations

All drinking water and wastewater systems are strongly encouraged to implement the following mitigations immediately to enhance resilience against low-level cyberattacks:

- **Reduce OT Exposure to the Public-Facing Internet**
- **Replace All Default Passwords on OT Devices with Strong, Unique Passwords**
- **Implement Multifactor Authentication for Remote Access to OT Devices**

In addition to these immediate actions, drinking water and wastewater systems are encouraged to adopt the actions outlined in the CISA, EPA, and FBI Top Cyber Actions for Securing Water Systems Fact Sheet to further reduce cyber risk and improve resilience against malicious cyber activity.

Conclusion

The U.S. EPA requests that the Water Sector Coordinating Council (WSCC)/Government Coordinating Council (GCC) review this advisory and pass it along to all water & wastewater entities that may be susceptible to this threat. Additionally, we encourage the EPA Regions share the advisory with the state primacy agencies and direct implementation utilities.

Water and wastewater system owners and operators should direct their IT/OT system administrators to review this alert for further use and implementation. If you rely on third party vendors for technology support, then you are encouraged to contact them to confirm their awareness of this threat. Organizations are encouraged to report information concerning suspicious or criminal activity to FBI Internet Crime Complaint Center (IC3) at IC3.gov or to CISA via CISA's Incident Reporting System. If you have questions about any of the information contained in this document, please contact the Water Infrastructure and Cyber Resilience Division, Cybersecurity Branch at watercyberta@epa.gov.