Incident Response Guide/Water and Wastewater Sector: Three Federal Agencies Issue Joint Publication

Walter Wright, Jr.
wwright@mwlaw.com
(501) 688.8839

11/11/2024

Three federal agencies have collectively developed a document titled:

Incident Response Guide - Water and Wastewater Sector ("Guide").

The Guide was produced by the following federal agencies:

- Cybersecurity and Infrastructure Security Agency.
- Federal Bureau of Investigation.
- Environmental Protection Agency.

Water and wastewater infrastructure are noted to be a potential target of cyber threat actors because of their potential to cause significant harm.

The Guide notes that raising cyber resilience in the water and wastewater sectors poses challenges because:

- Governance and regulation involve a mix of federal and state, local, tribal, and territorial authorities.
- Cybersecurity maturity levels across the sector are disparate.
- Often, WWS Sector utilities must prioritize limited resources toward the functionality of their water systems over cybersecurity.
- Universal solutions to cyber challenges in a diverse, target-rich, and resource-poor environment are unfeasible.

The three federal agencies intend for the Guide to provide water and wastewater sector owners and operators information about:

… the federal roles, resources, and responsibilities for each stage of the cyber incident response (IR) lifecycle.

They intend for sector owners and operators to use the information provided by the Guide to augment their respective incident response plans and procedures.

Objectives of the Guide include:

- Providing clear guidance for reporting cyber incidents.
- Connecting utilities with available cyber security resources, services, and no-cost trainings.
- Empowering utilities to build a strong cyber security baseline to improve cyber resilience and cyber hygiene.
- Encouraging utilities to integrate into their local cyber communities.

Key chapters in the Guide include:

- Key Federal Partners.
- Information Sharing.
- Incident Response Process.
- Preparation.
- Detection and Analysis.
- Containment, Eradication, and Recovery.
- Post-Incident Activity.
- Annex I: A More Advanced Collective Response:
- Annex II: Preparation Resources.

The Guide notes that it is not intended to mandate action or establish requirements.

A copy of the Guide can be downloaded here.