NPDES Program – Old (Hound) Dog, New Tricks?

ACWA

Annual Meeting

August 2022

Meeting Agenda

- Environmental Justice & NPDES Permitting
  - EPA
  - Q&A session
- Cybersecurity
  - EPA
  - Q&A session
- Water Quality Trading/Market Based Approaches
  - EPA
  - Q&A Session

EJ & NPDES Permitting

Executive Orders

- EO 12898, “Federal Actions to Address Environmental Justice in Minority Populations and Low-Income Populations,”
  - Identify & address adverse human health or environmental effects of their actions on minority and low-income populations, as permitted by law
  - develop a strategy for implementing environmental justice.
- EO 13985: “Advancing Racial Equity and Support for Underserved Communities Through the Federal Government”
  - calls on agencies to advance equity through identifying and addressing barriers to equal opportunity that underserved communities may face due to government policies and programs.
- EO 14008: “Tackling the Climate Crisis at Home and Abroad
  - directs federal agencies to develop programs, policies, and activities to address the disproportionate health, environmental, economic, and climate impacts on disadvantaged communities

Investments

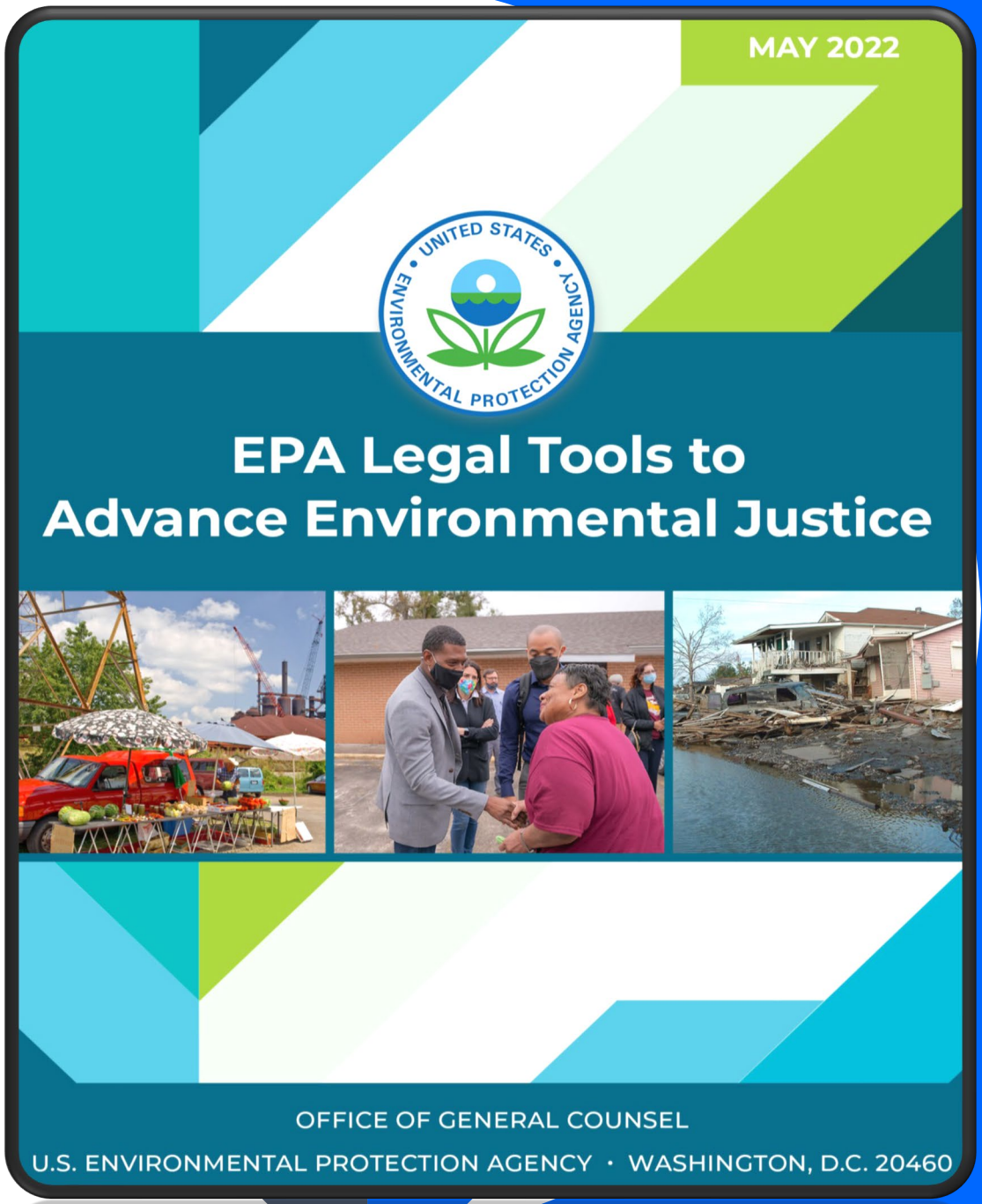
- Bipartisan Infrastructure Law (BIL), EPA is making investments into communities overburdened by pollution to solve many legacy EJ issues, such as toxic hotspots, access to water infrastructure, and ensuring safe drinking water.
- EPA received $100 million in American Rescue Plan funding for EJ issues.
- EPA launched a $20 million grant program from our air office to fund air quality monitoring projects in communities across the United States.
- EPA is investing $1 billion to initiate cleanup and clear the backlog of 49 previously unfunded Superfund sites and advance progress at dozens of other sites.
- BIL provides $50 billion to EPA's water programs
  - $15 Billion to replace lead pipes
  - $20 billion for safe drinking water infrastructure, upgrading aging systems
  - $12 Billion for clean water infrastructure (wastewater, stormwater, decentralized systems)

"At EPA, we know that our most vulnerable communities bear a disproportionate burden when it comes to the impacts of pollution and climate change. That's why advancing environmental justice is so critical to our mission. In support of this mission, the Agency is releasing EPA Legal Tools to Advance Environmental Justice, a document that identifies a wide range of legal authorities that EPA can deploy to ensure its programs and activities protect the health and environment of all people, no matter the color of their skin, their zip code, or how much money they have in their pocket."

Michael S. Regan
Administrator
U.S. Environmental Protection Agency

EJ in Permitting

- EPA Legal Tools to Advance Environmental Justice (EJ Legal Tools)
  - Compilation of legal authorities available to EPA to identify and address impacts of pollution to underserved and overburdened communities.
  - The document does not provide action-specific legal advice
    - *Addendum with more specific examples. MS4 & PGP.*
  - Is intended to foster a dialogue among EPA offices and programs to accelerate EPA efforts to advance environmental justice and equity.
  - Plan EJ 2014: Legal Tools



EJ in Permitting

- EPA EJ and Civil Rights in Permitting FAQs
  - The FAQs focus on the importance of EJ and civil rights in the environmental permitting process
  - Includes discussion of EJ and civil rights authorities and obligations
  - Potential approaches to screening for EJ and civil rights concerns, approaches to EJ and civil rights analysis, possible considerations about the mitigation of adverse and disproportionate impacts, and approaches to community outreach and engagement.

EJ and Permitting Efforts
Lessons Learned

- Public Involvement / Communication:
  - Enhanced public participation by developing templates, best practices and checklist for effective public outreach and notifications.
  - Public notification outside of newspapers (aka the internet)
  - Translations of documents into appropriate languages
  - Direct and targeted outreach to community organizations and institutions
  - Seeking ways to improve information flow from the facility, community and permitting authority.
- Permit process:
  - Developed permit checklist and process flowcharts
  - Increased training opportunities for EJScreen
- Technical Assistance Resources

EJ in NPDES Permitting
We want more

- Assessments:
  - Use of EJ Screen and other related tools
  - Integrated Planning
  - Permit Quality Reviews
  - Cumulative Impact Analysis
    - Framework as part of a Chelsea, MA permit
- Compile EJ efforts in the States
  - Colorado example- Simplified factsheet
- Compile Best Management practices to share


Draft water quality permit renewal
Suncor Refinery

About Suncor and water

¿Desea leer este en español? Haga clic aquí.

The Suncor facility is a petroleum refinery in Commerce City, Colorado. It makes gasoline, jet fuel, diesel fuels, and asphalt. The facility is along the banks of Sand Creek, close to the South Platte River. The Burlington Ditch crosses through the property.

The contaminated groundwater at the site has petroleum products, like benzene, as well as toxic chemicals known as PFAS. The Hazardous Materials and Waste Management Division supervises the groundwater cleanup.

Discharge permit basics

Discharge permits limit the amount of used water from the facility, treated groundwater, and stormwater that Suncor can put into Sand Creek. The permit will better protect the creeks and rivers surrounding the facility.

Major changes

→ Combined wastewater and stormwater permit.
The facility had two separate permits issued in 2012. This renewal combines them into one permit (CO0001147).

→ Per- and Polyfluoroalkyl Substances (PFAS).
PFAS are a group of human-made chemicals with thousands of compounds. These chemicals have been used for decades in firefighting foams and common products. Health effects from these chemicals may include pregnancy complications, developmental effects, and liver and kidney effects. Additionally, there is evidence linking exposure to PFAS to certain cancers. This CDPHE FAQ gives more information.

In July 2020, Colorado's Water Quality Control Commission issued Policy 20-1, Policy for Interpreting the Narrative Water Quality Standards for PFAS (July 14, 2020). This policy established specific limits for PFAS to protect drinking water supplies, like the South Platte River.

- PFOA/PFOS/PFNa and their parents -- 70 parts per trillion (ppt)
- PFXs and parents -- 700 ppt
- PFBS and parents -- 400,000 ppt

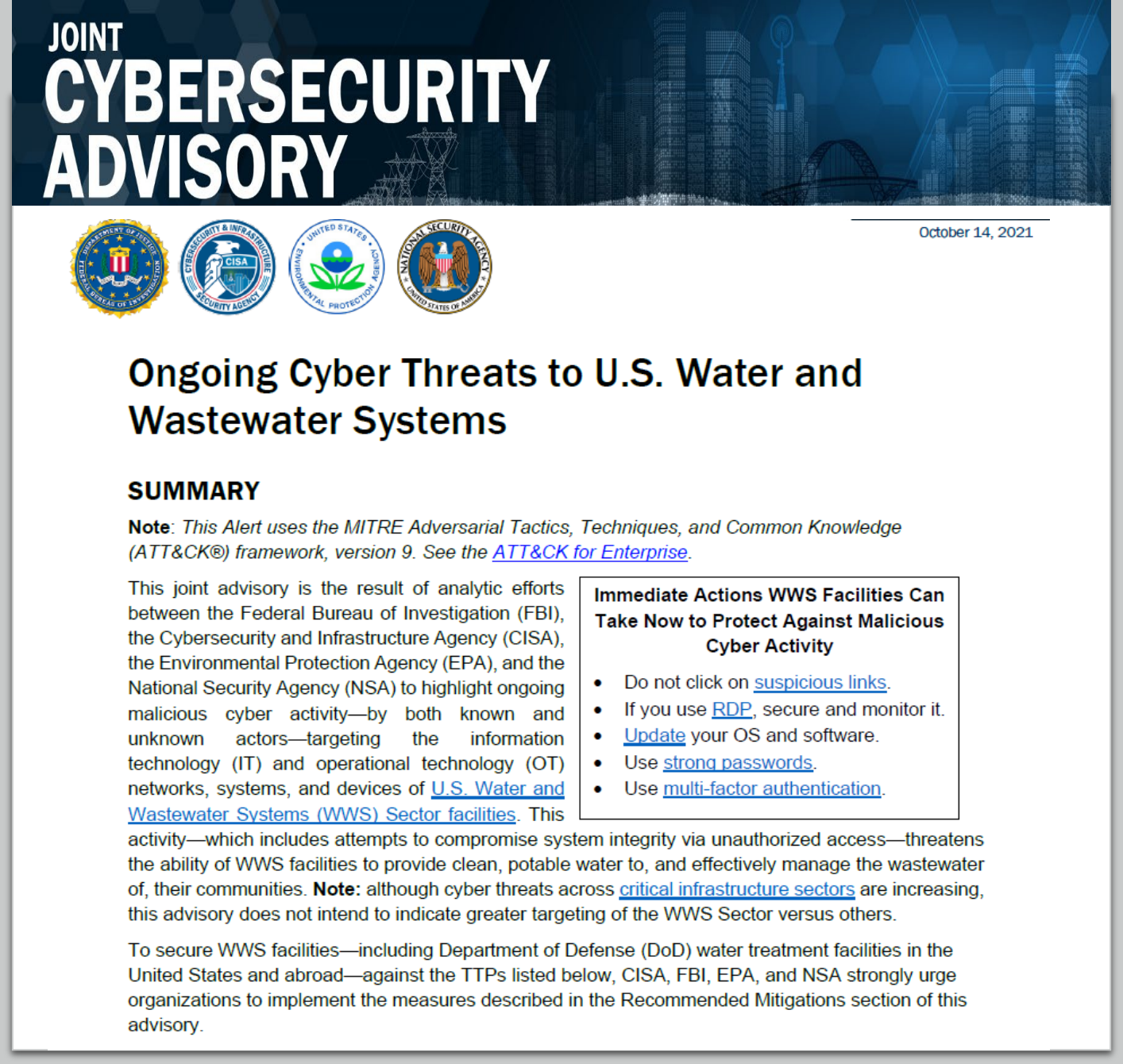
Q&A Session

- What are some best practices your state is exploring or currently does to engage with disadvantage communities?
- Are there specific assessments and/or tools your permit writers are using to look at impacted communities?
- Anything that EPA could do to help integrate EJ in NPDES permits?

Cybersecurity

Actions to Take:

- Spearphishing personnel to deliver malicious payloads, including ransomware
  - Personnel & lack of cyber awareness
  - Open malicious attachments/links which bypass filtering controls.
  - Remote desktop protocols, which increased with COVID.
- Exploitation of unsupported or outdated operating systems & software.
  - Facilities are inconsistently resourced which contribute to the use of unsupported or outdated operating systems and software.
- Exploitation of control system devices with vulnerable firmware versions.



JOINT
CYBERSECURITY
ADVISORY

October 14, 2021

Ongoing Cyber Threats to U.S. Water and Wastewater Systems

SUMMARY

Note: *This Alert uses the MITRE Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK®) framework, version 9. See the ATT&CK for Enterprise.*

This joint advisory is the result of analytic efforts between the Federal Bureau of Investigation (FBI), the Cybersecurity and Infrastructure Agency (CISA), the Environmental Protection Agency (EPA), and the National Security Agency (NSA) to highlight ongoing malicious cyber activity—by both known and unknown actors—targeting the information technology (IT) and operational technology (OT) networks, systems, and devices of U.S. Water and Wastewater Systems (WWS) Sector facilities. This activity—which includes attempts to compromise system integrity via unauthorized access—threatens the ability of WWS facilities to provide clean, potable water to, and effectively manage the wastewater of, their communities. **Note:** although cyber threats across critical infrastructure sectors are increasing, this advisory does not intend to indicate greater targeting of the WWS Sector versus others.

Immediate Actions WWS Facilities Can Take Now to Protect Against Malicious Cyber Activity

- Do not click on suspicious links.
- If you use RDP, secure and monitor it.
- Update your OS and software.
- Use strong passwords.
- Use multi-factor authentication.

To secure WWS facilities—including Department of Defense (DoD) water treatment facilities in the United States and abroad—against the TTPs listed below, CISA, FBI, EPA, and NSA strongly urge organizations to implement the measures described in the Recommended Mitigations section of this advisory.

Cyber intrusions targeting U.S. facilities highlight vulnerabilities with the following threats:

- Insider threats from current or former employees who maintain improperly active credentials
- Ransomware attacks

Examples:

- In August 2021, malicious cyber actors used Ghost variant ransomware against a California based facility. The ransomware variant had been in the system for about a month and was discovered when three SCADA servers displayed a ransomware message.
- In July 2021, cyber actors used remote access to introduce ZuCaNo ransomware onto a Maine-based wastewater facility SCADA computer. The treatment system was run manually until the SCADA computer was restored.
- In March 2021, cyber actors used an unknown ransomware variant against a Nevada-based WWS facility. The SCADA system provides visibility and monitoring but is not a full industrial control system.
- In September 2020, personnel at a New Jersey-based WWS facility discovered potential Makop ransomware had compromised files within their system.
- In March 2019, a former employee at Kansas-based WWS facility unsuccessfully attempted to threaten drinking water safety by using his user credentials, which had not been revoked at the time of his resignation, to remotely access a facility computer.

City of Oldsmar Water Supply Attack

Vulnerabilities exploited:

- Unsecured remote access software (TeamViewer),
- Poor password security,
- Outdated operating systems (Windows 7)

Lessons learned:

- Adopted multiple-factor authentication;
- use of strong passwords;
- auditing remote connection activity;
- close unused remote access connection ports;
- establish cyber awareness training for users;
- ensure anti-virus, spam filters, and
- firewalls are properly configured and up to date

Ransomware

- In recent months there have been a significant number of Ransomware attacks against the U.S critical infrastructure to include targeted attacks against the Water sector.
- In response to the pervasive ransomware threat, the White House issued a memo titled, *What We Urge You to Do to Protect Against the Threat of Ransomware*, which outlines the five best cybersecurity practices to reduce the risk of a successful ransomware.
- CISA has launched a *Stop Ransomware* campaign that contains a collection of resources devoted to preventing and responding to ransomware attacks: **https://www.cisa.gov/ransomware**

Ransomware

EPA issued an alert to the Water sector on July 1st, urging all water and wastewater facilities to adopt these five basic practices:

1. Backup your data, system images, configurations, and regularly test them, and keep the backups offline
2. Update and Patch Systems Promptly
3. Test your incident response plan
4. Check Your Security Team’s Work
5. Segment your network

Mitigation Strategies

- Employee Cybersecurity Training program
- Keep inventory of control systems and devices
- Require strong passwords & password management practices.
- Monitor network intrusions & have a plan to respond.

How to Use This Brief

EPA developed this brief in cooperation with the Association of State Drinking Water Administrators' Security Committee to help state staff (or their designated assistance providers) start a conversation with utilities about cybersecurity. Information gathered from the questions on this page can help you to understand a utility's current cybersecurity practices and point them toward resources to enhance their program. You may also leave the next two pages with the utility as a reminder of your discussions. Those pages provide recommendations for building a cybersecurity program and responding to cyber-attacks.

10 Questions for a Cybersecurity Dialogue with a Utility*

Does your utility …

1. **Keep an inventory of control system devices and ensure this equipment is not exposed to networks outside the utility?**
   - Never allow any machine on the control network to "talk" directly to a machine on the business network or on the Internet.
2. **Segregate networks and apply firewalls?**
   - Classify IT assets, data, and personnel into specific groups, and restrict access to these groups.
3. **Use secure remote access methods?**
   - A secure method, like a virtual private network, should be used if remote access is required.
4. **Establish roles to control access to different networks and log system users?**
   - Role-based controls will grant or deny access to network resources based on job functions.
5. **Require strong passwords and password management practices?**
   - Use strong passwords and have different passwords for different accounts.
6. **Stay aware of vulnerabilities and implement patches and updates when needed?**
   - Monitor for and apply IT system patches and updates.
7. **Enforce policies for the security of mobile devices?**
   - Limit the use of mobile devices on your networks and ensure devices are password protected.
8. **Have an employee cybersecurity training program?**
   - All employees should receive regular cybersecurity training.
9. **Involve utility executives in cybersecurity?**
   - Organizational leaders are often unaware of cybersecurity threats and needs.
10. **Monitor for network intrusions and have a plan in place to respond?**
    - Be capable of detecting a compromise quickly and executing an incident response plan.
11. For more information about each of these questions, see WaterISAC *15 Cybersecurity Fundamentals for Water and Wastewater Utilities* at https://www.waterisac.org/fundamentals.

Who are the cyber players?

- EPA is the sector-specific Agency lead for protecting critical infrastructure in the water sector.
- EPA works with DHS, CISA, FBI, utility and operators, industry reps, to develop cyber protection and resilience strategies.
- Sector specific partners: NIST, AWWA, Water Research Foundation, Water Env Research Foundation, state and local agencies
- R3 & VA: Evaluation of 24 utilities varying in size & characteristic to understand their cyber practices
- CA formed a committed to promote awareness of cyber practices at PWS.
- AWWA released the Process Control System Security Guidance for the Water sector.

Federal Assistance

EPA cybersecurity best practices for the water sector, including:

- The *Water Sector Cybersecurity Brief for States*, which can assist state technical assistance providers with assessing cybersecurity practices at water systems and developing an improvement plan to reduce cyber risks;
- The *Cybersecurity Incident Action Checklist*, which suggests steps for wastewater systems to prepare for, respond to, and recover from a cybersecurity incident; and
- The *Water Utility Tabletop Exercise Toolbox*, which helps water systems to plan, conduct and evaluate tabletop exercises for all-hazards scenarios, including cybersecurity incidents.
- The *Supporting Cybersecurity Measures with the Clean Water State Revolving Fund*, which provides information on how facilities can access assistance through Clean Water State Revolving Fund (CWSRF) to fund initial water infrastructure projects related to cybersecurity.

- The National Institute of Standards and Technology's cybersecurity framework, which helps organizations to better improve their management of cybersecurity risk.
- The Cybersecurity & Infrastructure Security Agency provides a National Cyber Awareness System and a portal to report cyber incidents.

Non-governmental organization cybersecurity resources:

- The Water Information Sharing and Analysis Center, which has developed *15 Cybersecurity Fundamentals for Water and Wastewater Utilities.*
- The Multi-State Information Sharing and Analysis Center.
- The American Water Works Association, which has developed a *Water Sector Cybersecurity Risk Management Guidance & Cybersecurity Tool*.

RESOURCES

Cyber Hygiene Services

CISA offers a range of no-cost cyber hygiene services—including vulnerability scanning and ransomware readiness assessments—to help critical infrastructure organizations assess, identify, and reduce their exposure to cyber threats. By taking advantage of these services, organizations of any size will receive recommendations on ways to reduce their risk and mitigate attack vectors.

Rewards for Justice Reporting

The U.S. Department of State's Rewards for Justice (RFJ) program offers a reward of up to $10 million for reports of foreign government malicious activity against U.S. critical infrastructure. See the RFJ website for more information and how to report information securely.

StopRansomware.gov

The StopRansomware.gov webpage is an interagency resource that provides guidance on ransomware protection, detection, and response. This includes ransomware alerts, reports, and resources from CISA and other federal partners, including:

- CISA and MS-ISAC: Joint Ransomware Guide
- CISA Insights: Ransomware Outbreak
- CISA Webinar: Combating Ransomware

Additional Resources

For additional resources that can assist in preventing and mitigating this activity, see:

- FBI-CISA-EPA-MS-ISAC Joint CSA: Compromise of U.S. Water Treatment Facility
- WaterISAC: 15 Cybersecurity Fundamentals for Water and Wastewater Utilities
- American Water Works Association: Cybersecurity Guidance and Assessment Tool
- EPA: Cybersecurity Incident Action Checklist
- EPA: Cybersecurity Best Practices for the Water Sector
- EPA: Supporting Cybersecurity Measures with the Clean Water and Drinking Water State Revolving Funds
- CISA: Cyber Risks & Resources for the Water and Wastewater Systems Sector infographic
- CISA: Critical ICS Cybersecurity Performance Goals and Objectives

Free Cybersecurity Assessment and Technical Assistance

EPA is providing free cybersecurity technical assistance to water and wastewater utilities to improve cyber incident preparation, response, and recovery in order to maintain critical operations and meet water quality goals

- Technical Assistance Provider performs a cyber assessment with utility staff
- Utilities receive an overview of their vulnerabilities and suggested best practices to remediate or mitigate the risk
- A customized Cyber Action Plan will be provided to each utility to assist them with implementing recommended best practices
- Two follow-ups to gauge progress and see if additional assistance is required
- To date, EPA has provided assistance to over 100 utilities
- **Information remains confidential. Only anonymized, aggregated data is shared with EPA**
- To register your utility:
- www.horsleywitten.com/cybersecurityutilities

Additional EPA Water Sector Cyber Resources

Cybersecurity Brief for States

This guide can assist utilities with assessing cybersecurity practices and developing an improvement plan to reduce cyber risks.

Vulnerability Self-Assessment Tool 2.0 (VSAT Web 2.0)

This online tool leads water and wastewater systems through an all-hazards risk assessment, including risks from cybersecurity incidents, and the assessment of costs and benefits

Water Resilience Tabletop Exercise (TTX) Tool

This tool provides water and wastewater systems with the resources to plan, conduct and evaluate tabletop exercises for all-hazards scenarios, including cybersecurity incidents.

CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY

CISA offers several scanning and testing services to help organizations reduce their exposure to threats by taking a proactive approach to mitigating attack vectors.

Vulnerability Scanning: offers persistent scanning of internet-accessible systems for vulnerabilities, configuration errors, and use of risky services.

Web Application Scanning: Evaluates publicly-accessible websites for potential bugs and weak configurations and provides recommendations for mitigation.

Phishing Campaign Assessment: Measures your organization's propensity to click on email phishing lures. Results can be used to provide guidance for anti-phishing training and awareness.

Remote Penetration Test: Simulates the tactics and techniques of real-world adversaries to identify and validate exploitable pathways. This service is ideal for testing perimeter defenses, the security of externally-available applications, and the potential for exploitation of open-source information.

All services are available free-of-charge

Results are kept confidential between the customer and CISA

Email vulnerability_info@cisa.dhs.gov with questions or to get started

15 Cybersecurity Fundamentals for Water and Wastewater Utilities

- Overview of important security measures
- Links to additional information about each measure
- Free resource

waterisac.org/fundamentals

How can NPDES Permits Program Help?

- What are ways the NPDES permitting program can help if we are not the experts in cybersecurity?
- What tools/resources do we need to help make facilities understand the risks and prepare for a potential cyber incident?
- Other areas where states think EPA could further assist?

Water Quality Trading

Market Based Approaches

Market-Based Approaches under NPDES

- Case Studies – thank you for your help
- Nutrient Compendium
- Flexibilities Policy Statement
- Regulation

Reframing the Market-Based Paradigm

- Water quality trading has traditionally been discussed in terms of cost effectiveness.
- Market-based approaches are not stand-alone tools that can significantly reduce pollutant discharges in isolation, but rather, can be important mechanisms for the feasible implementation of WQBELs based on **regulatory drivers** such as:
  - numeric criteria in nutrient water quality criteria,
  - translators of narrative criteria,
  - TMDLs that provide action-forcing waste load allocations, and
  - other State performance standards.

Market-Based Flexibilities Policy Statement

- September 19, 2019, Federal Register requested comments on 6 potential flexibilities.
- Current draft policy statement addresses three flexibilities:
  - Incremental water quality trading baseline for NPS where TMDL
  - Accounting for Credit Generation in Compliance Schedules
  - Incorporating Credit Generation into WQS Variances
- Current draft policy statement does not address
  - ‘Immediate credit generation’ trading baseline for NPS
  - In-lieu fee programs
  - Alternative approaches to disaggregation of Load Allocations

Incremental Baseline Approach for NPS

- Current EPA guidance is barrier/inconsistent with practice
- Approach is optional – States can use existing/other approaches
- Timing of meeting the baseline.
  - Nonpoint sources are to make progress on meeting their load allocation before they can generate credits.
- Clarifies that control measures eligible for credit generation are *in addition to* control measures described in TMDL documents for achieving the load allocation.

Other Flexibilities

- **Credit Generation in Compliance Schedules:** A compliance schedule in an NPDES permit account for the time needed for either a point source seller or a nonpoint source seller to implement controls necessary to generate the pollutant reduction credits.

- **Incorporating Nonpoint Source Credits in Water Quality Standards Variances:** May states consider whether it is appropriate for the permittee(s) subject to a WQS variance to use a market-based approach, including water quality trading between point sources or between a point source and nonpoint source, to support achieving the WQBEL in its NPDES permit based on the WQS variance?

Rulemaking Background

- Stakeholders have expressed interest in having more explicit regulatory authority for trading

- April 5, 2022 Fox Nutrients memo provides:
  - Initiating a rulemaking to explicitly state that NPDES permits may include conditions allowing market-based approaches, including trading, to meet applicable effluent limits.

Objectives of Rulemaking

- To provide simple, clear regulatory language that clarifies that market-based approaches can be used under the NPDES program to comply with effluent limitations.

- Secondary objective: The rulemaking is an opportunity to clarify the legal basis under the CWA for market-based approaches.

- Goal: Keep regulation as simple as possible

Draft Regulation – what will it say?

Market-based approaches, including trading and offsets, may be used to meet applicable effluent limitations in NPDES permits

- Market-based approaches **cannot** be used to meet technology-based requirements with a few exceptions.

Market-based approaches can't result in localized exceedances of water quality standards

Q&A Session

- Are there states that have avoided using market-based approaches due to risk of litigation?
- Are there states that currently do not have market-based approaches considering developing them as a viable option for their programs?
- Are there any states interested in piloting a program if EPA contractor dollars were available to assist with a case study?
- What can we do to support States with active trading/market-based approaches?

Thank you.