



Cybersecurity Projects & Funding for Water Utilities

About the Speaker

- Nushat Thomas, Cybersecurity Branch Chief
- EPA's Office of Water
 - Office of Ground Water and Drinking Water
 - Water Infrastructure and Cyber Resilience Division
 - Cybersecurity Branch
- Email: thomas.nushat.a@epa.gov

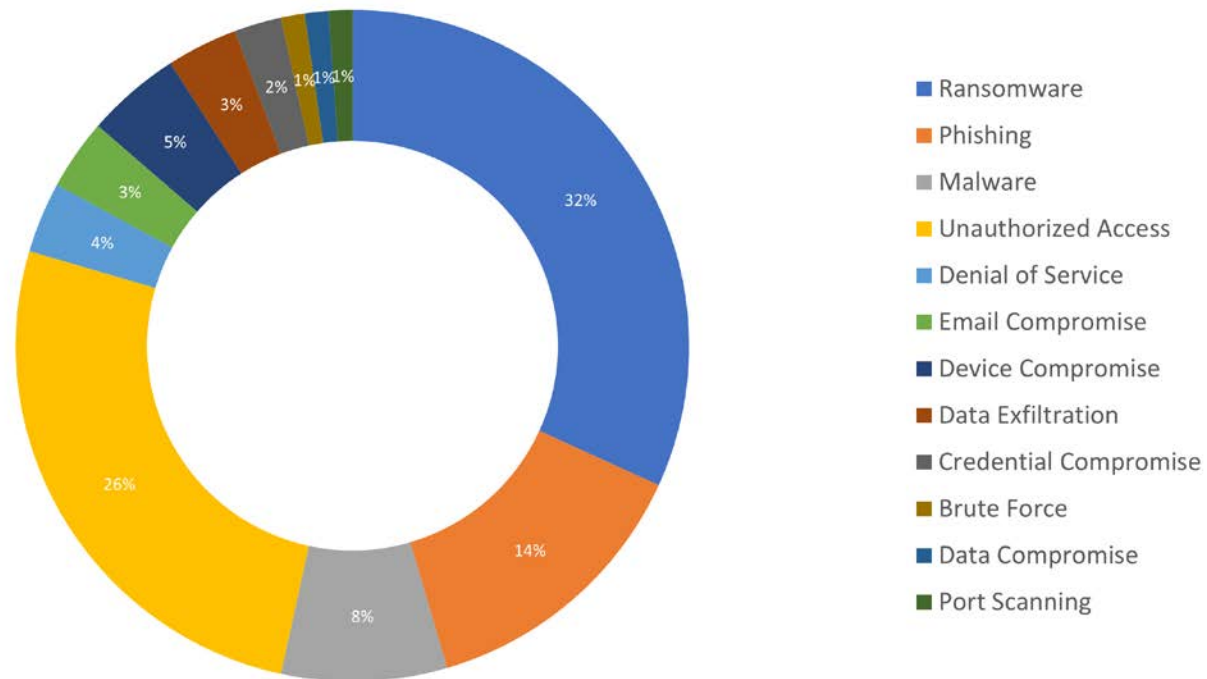




Water Sector Cybersecurity Threat Landscape

Water Sector Cybersecurity Incident Statistics*

*Updated as of January 30th, 2024. This chart only includes the incidents that have been voluntarily reported to EPA, CISA, or FBI.





EPA's Cybersecurity Assessment and Technical Assistance Resources

EPA Water Sector Cybersecurity Evaluation Program

- EPA conducts free cybersecurity assessment for Water and Wastewater Systems to identify cybersecurity gaps.
- The program uses the EPA Cybersecurity Checklist.
- You will receive an Assessment Report and a Risk Mitigation Plan template.

U.S. EPA Water Sector Cybersecurity Evaluation Program

How is the Cybersecurity Evaluation Program helping water and wastewater systems build cyber resilience?
The EPA will conduct a free cybersecurity assessment for Water/Wastewater Systems (W/WSs) to identify gaps or vulnerabilities in information technology (IT) and operational technology (OT) using the EPA Cybersecurity Checklist.

What is the EPA Cybersecurity Checklist?
The Cybersecurity Checklist is a list of questions EPA derived from CISA's Cybersecurity Performance Goals to help W/WSs assess their cyber risk. The Cybersecurity Checklist is available in the EPA guidance document, EPA Cybersecurity Risk Assessment Guidance for Drinking Water and Wastewater Systems. W/WSs are encouraged to use the resources and technical assistance offered in EPA's guidance document to address identified gaps and reduce the risk of cyberattacks.

How does the Cybersecurity Evaluation program work?
A W/WS must register to receive a cybersecurity assessment. Once registered, an EPA contractor will contact the W/WS to gather basic information, provide guidance on how to prepare and schedule an assessment. During the assessment, the EPA contractor will ask the W/WS each of the questions in the Cybersecurity Checklist.
The contractor will generate a report that identifies cybersecurity gaps and/or vulnerabilities in the W/WS's IT/OT based on response to the Cybersecurity Checklist. In addition, a template for a Risk Mitigation Plan will be generated, which the W/WS can use to plan and document actions to address cybersecurity gaps.

What does the W/WS need to prepare before the assessment?
The assessment will require input from management, operations, business, and IT and OT staff as appropriate. The W/WS will also need to compile any existing system documentation, diagrams, policies, and procedures to help answer the Checklist questions.

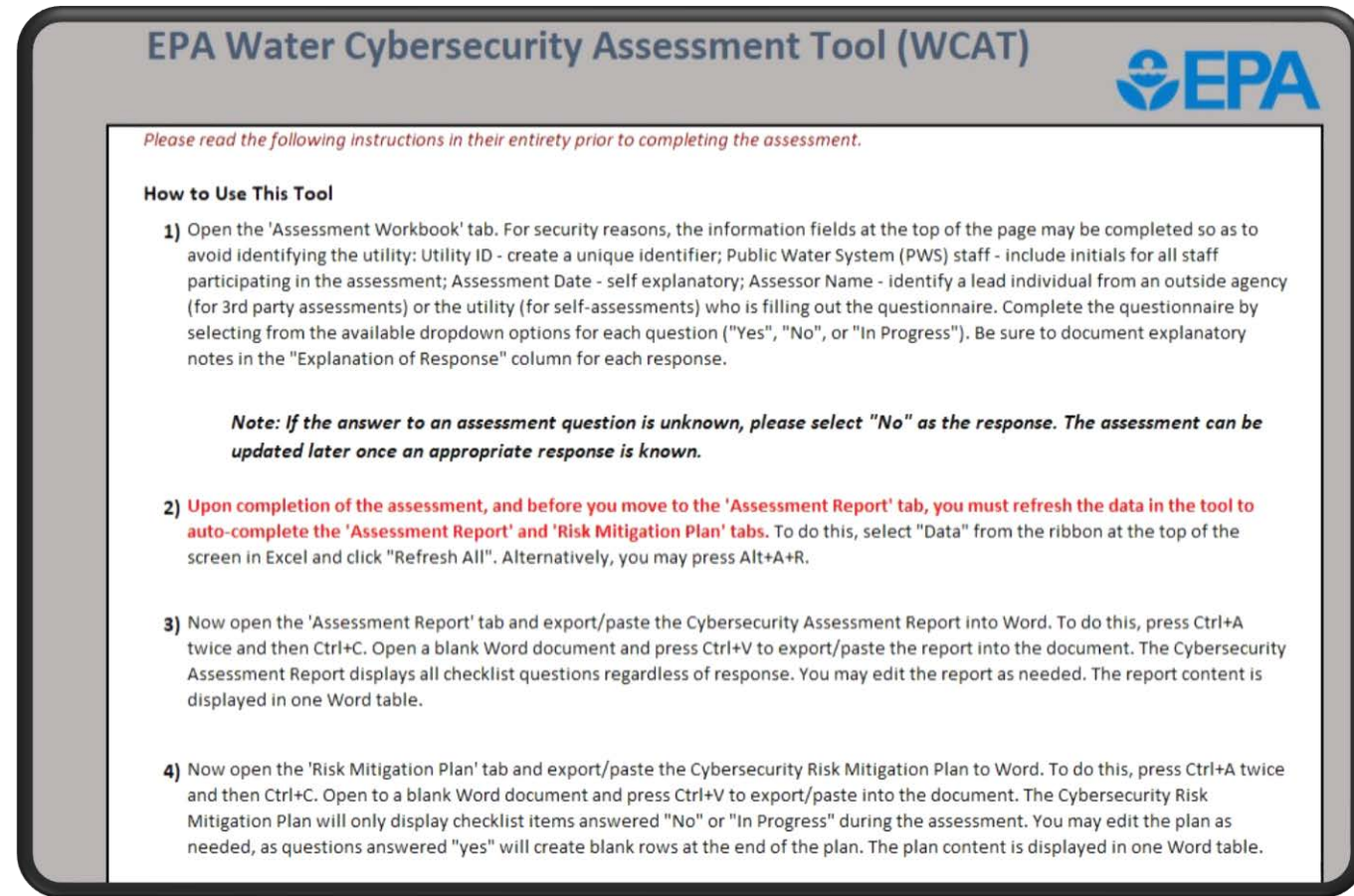
How does EPA protect the results of the W/WS Cybersecurity Assessment?
EPA does not share the results of the assessment with any party beyond the W/WS. The file is delivered using a secure file transfer. The contractor shares the anonymized, aggregated results with EPA. EPA will protect information submitted to the agency in accordance with applicable authorities. The EPA contractor supporting this program is the Horsley Witten Group, Inc.

To register your W/WS, please visit:
www.epa.gov/waterresilience/forms/epas-water-sector-cybersecurity-evaluation-program

For more information, contact:
Horsley Witten Group
508-833-6600 x501

EPA Water Cybersecurity Assessment Tool (WCAT)

- Utilizes EPA's Cybersecurity Checklist and provides a method to evaluate cybersecurity practices at water and wastewater utilities.
- The Tool Features:
 - Assessment Workbook
 - Assessment Report
 - Risk Mitigation Plan



The screenshot displays the title "EPA Water Cybersecurity Assessment Tool (WCAT)" and the EPA logo. Below the title, a red instruction reads: "Please read the following instructions in their entirety prior to completing the assessment." The main content is titled "How to Use This Tool" and contains four numbered steps:

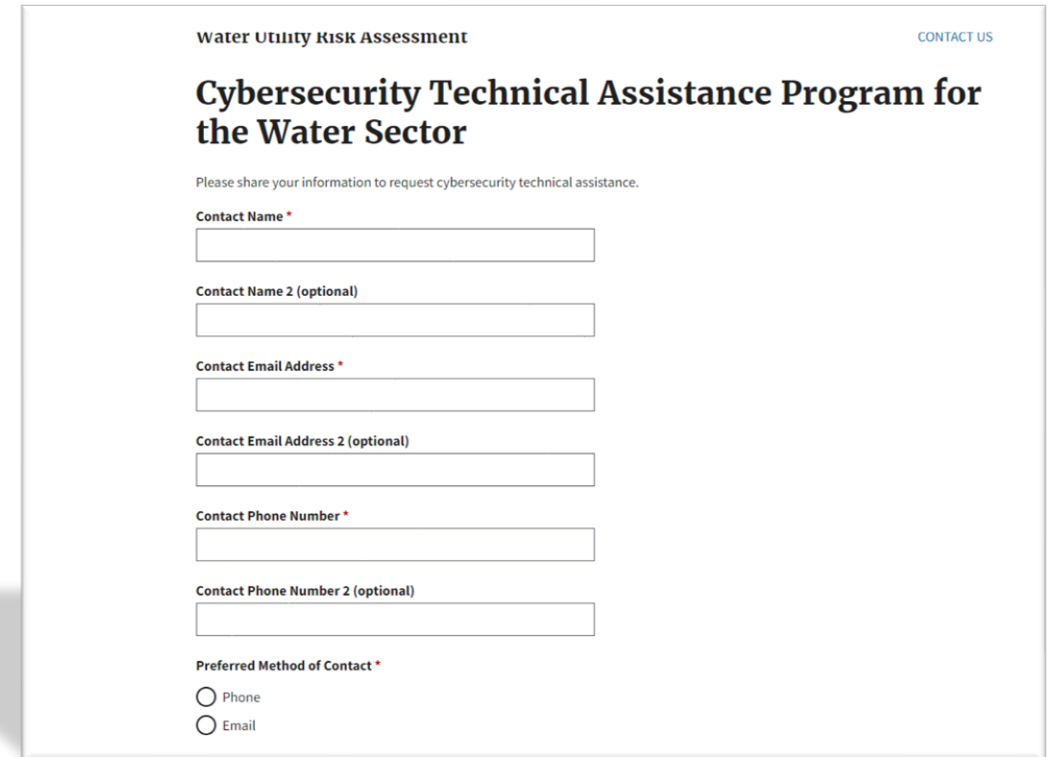
- 1) Open the 'Assessment Workbook' tab. For security reasons, the information fields at the top of the page may be completed so as to avoid identifying the utility: Utility ID - create a unique identifier; Public Water System (PWS) staff - include initials for all staff participating in the assessment; Assessment Date - self explanatory; Assessor Name - identify a lead individual from an outside agency (for 3rd party assessments) or the utility (for self-assessments) who is filling out the questionnaire. Complete the questionnaire by selecting from the available dropdown options for each question ("Yes", "No", or "In Progress"). Be sure to document explanatory notes in the "Explanation of Response" column for each response.
Note: If the answer to an assessment question is unknown, please select "No" as the response. The assessment can be updated later once an appropriate response is known.
- 2) Upon completion of the assessment, and before you move to the 'Assessment Report' tab, you must refresh the data in the tool to auto-complete the 'Assessment Report' and 'Risk Mitigation Plan' tabs. To do this, select "Data" from the ribbon at the top of the screen in Excel and click "Refresh All". Alternatively, you may press Alt+A+R.
- 3) Now open the 'Assessment Report' tab and export/paste the Cybersecurity Assessment Report into Word. To do this, press Ctrl+A twice and then Ctrl+C. Open a blank Word document and press Ctrl+V to export/paste the report into the document. The Cybersecurity Assessment Report displays all checklist questions regardless of response. You may edit the report as needed. The report content is displayed in one Word table.
- 4) Now open the 'Risk Mitigation Plan' tab and export/paste the Cybersecurity Risk Mitigation Plan to Word. To do this, press Ctrl+A twice and then Ctrl+C. Open to a blank Word document and press Ctrl+V to export/paste into the document. The Cybersecurity Risk Mitigation Plan will only display checklist items answered "No" or "In Progress" during the assessment. You may edit the plan as needed, as questions answered "yes" will create blank rows at the end of the plan. The plan content is displayed in one Word table.



Cybersecurity Technical Assistance

Cybersecurity Technical Assistance Program for the Water Sector

- Under this program, water and wastewater systems, state primacy agencies, and technical assistance providers can submit questions or request to consult with a subject matter expert (SME) regarding cybersecurity.
- EPA will strive to have an SME respond within two business days.
- All assistance will be remote.



Water Utility Risk Assessment CONTACT US

Cybersecurity Technical Assistance Program for the Water Sector

Please share your information to request cybersecurity technical assistance.

Contact Name *

Contact Name 2 (optional)

Contact Email Address *

Contact Email Address 2 (optional)

Contact Phone Number *

Contact Phone Number 2 (optional)

Preferred Method of Contact *

Phone

Email



Cybersecurity Planning



Water Sector Cybersecurity Program Case Studies

Case Studies highlighting the cybersecurity success stories at water and wastewater utilities.

- [Small Wastewater System](#)
- [Medium Drinking Water System](#)
- [Medium Combined System](#)
- [Large Combined System](#)

The screenshot shows a document from the EPA titled "WATER SECTOR CYBERSECURITY PROGRAM CASE STUDY: Small Wastewater System" with the subtitle "Asset Inventory: A Good First Step to Balancing Risks". It includes an overview, a cybersecurity approach, and a table of security measures.

OVERVIEW
All mechanical operations at this system became automated when a new wastewater treatment plant came online in 2017. The plant operator had to balance the welcomed convenience of automation and productivity with the new cybersecurity risks introduced.

CYBERSECURITY APPROACH
The utility developed a cybersecurity policy document to ensure that vulnerabilities were considered, and cybersecurity risks mitigated. Topics covered include:

ACCOUNT SECURITY	RESPONSE AND RECOVERY
<ul style="list-style-type: none">• Separate standard user and privileged accounts• Password length requirements• Secure remote access policy	<ul style="list-style-type: none">• Cybersecurity incident reporting• Cybersecurity Incident Response Plan for critical threat scenarios, including disabled or manipulated process control systems• System backups for post-incident recovery efforts
DEVICE SECURITY	
<ul style="list-style-type: none">• OT and IT network asset inventory	
DATA SECURITY	OTHER
<ul style="list-style-type: none">• Log collection and monitoring frequency for intrusion detection	<ul style="list-style-type: none">• Segmentation of OT and IT networks
VULNERABILITY MANAGEMENT	
<ul style="list-style-type: none">• OT asset connection to the public Internet	

The policy document detailed the expectations, standards, and safeguards to reduce cybersecurity risks at the utility. For example, staff have unique user accounts with separate logins and passwords, and not all staff have programming privileges once logged into the SCADA system. The document clearly defined who to call for help once a cyber incident is discovered and provided contact information. In addition to the cyber policy, the Incident Response Plan was updated to describe how to run the plant in full "manual mode" without the benefit of the SCADA system in case of a cyber incident.

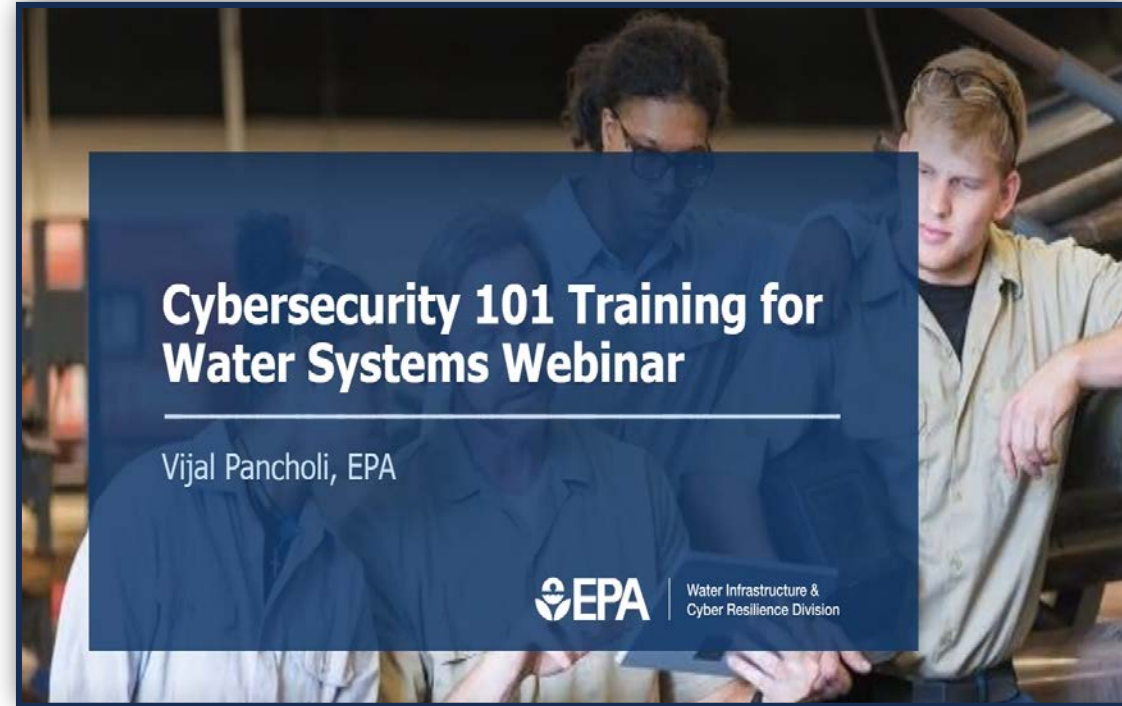


Cybersecurity Training



Cybersecurity 101 Webinar for Water Systems

- This webinar reviews basic cybersecurity topics including:
 - Account security
 - Device security
 - Data security
 - Training, and more.
- You can use this webinar during your annual cybersecurity training!
- EPA plans to release Cybersecurity 201 in 2024.



Link: <https://www.youtube.com/watch?v=e2QDbgrojb0>

Cybersecurity Tabletop Exercises

- EPA offers free cybersecurity tabletop exercises for water and wastewater utilities to test incident response procedures and to provide resources to develop and improve incident response plans.
- EPA partners with primacy agencies, state agencies, water sector associations, WARNs, CISA, and FBI.
- Email watercyberta@epa.gov to request a tabletop exercise.



Cybersecurity Response

Where to Report?



Threat Response (FBI)	Asset Response (CISA)	Centralized Response (EPA)
<p>Submit an internet crime complaint form to the FBI at www.ic3.gov or contact your local field office at www.fbi.gov/contact-us/field.</p> <p>The FBI will conduct the investigation.</p>	<p>Submit a computer security incident form to the Cybersecurity and Infrastructure Security Agency (CISA) Incident Reporting System at www.uscert.cisa.gov/forms/report.</p> <p>CISA can be contacted by phone at 888-282-0870 and by email at Central@cisa.gov.</p> <p>CISA will provide technical assets and assistance to mitigate vulnerabilities and reduce the impact of the incident.</p>	<p>Please reach out to the U.S. Environmental Protection Agency (EPA) Water Infrastructure and Cyber Resilience Division (WICRD) at watercyberta@epa.gov.</p> <p>EPA's WICRD will act as a centralized federal point of contact between the affected parties/stakeholders and all appropriate federal agencies incorporated in the incident response.</p>



Cybersecurity Funding



Cybersecurity Funding Opportunities

Clean Water State Revolving Fund	Drinking Water State Revolving Fund
<ul style="list-style-type: none">• Provides assistance to any public, private, or nonprofit entity for measures to increase the security of publicly owned treatment works, including cybersecurity.• Learn more about the CWSRF here: https://www.epa.gov/cwsrf/clean-water-state-revolving-fund-cwsrf-environmental-benefits-report	<ul style="list-style-type: none">• Provides assistance with All-Hazard Risk and Resilience Assessment, Training, Equipment, and Infrastructure, including cybersecurity.• Learn more about the DWSRF here: https://www.epa.gov/dwsrf

Midsize & Large Drinking Water System Infrastructure Resilience & Sustainability Program

- Purpose: Protecting drinking water sources from natural hazards, extreme weather events, and cybersecurity threats
- Funding amount: ~\$5,000,000 +
- Eligibility: Public water systems serving more than 10,000 people
- **Application period: Announced and open for applications in 2024**

Future Examples

- **Successfully funded projects**
- **Explicit criteria**
- **Water Utility Case Studies**

EPA's Cybersecurity for the Water Sector Website

<https://www.epa.gov/waterriskassessment/epa-cybersecurity-best-practices-water-sector>

