



EPA Cybersecurity for the Water Sector

About Me

- **Cole Dutton, Cybersecurity Specialist**
- **EPA's Office of Water – Water Infrastructure and Cyber Resilience Division**
- **M.S – Computer Science, Information Security**





Eighth Circuit Court of Appeals Stay in State of Missouri, et al v. U.S. EPA



United States
Environmental Protection
Agency

Office of Water

8/25/2023

3

What does the stay order mean for state primacy agencies?

EPA's interpretive rule issued on March 3, 2023, via the Memorandum on Addressing Public Water System Cybersecurity in Sanitary Surveys or an Alternate Process is not in effect and therefore states are not required on the basis of the interpretive rule and EPA's regulations to include cyber in their sanitary surveys or develop an alternate process at this time.

What is EPA's response to the stay order?

- **EPA is disappointed by the Eighth Circuit Court of Appeals order that undercuts EPA's efforts to protect the safety of the nation's drinking water from malicious cyberattacks.**
- **EPA is committed to ensuring that all people have access to clean, safe water. Cybersecurity threats to the water sector are real, and EPA is committed to using its authorities to advance cybersecurity and reduce the possibility of cyber threats impacting the delivery of clean, safe water.**

Who does the stay apply to?

The stay of the interpretive rule memo applies nationwide, thus affecting all states and PWSs with respect to EPA's interpretation of its sanitary survey regulations, pending the resolution of the case.

What actions should primacy agencies take in the meantime?

- **States that have state level authorities to do so may require their water systems to undergo a cyber assessment to be reviewed by the state.**
- **EPA encourages all states and PWSs to voluntarily engage in review of PWS cybersecurity during the sanitary survey to ensure utilities are addressing cybersecurity gaps.**

What is EPA doing in the meantime?

- **EPA is committed to supporting the Water Sector in addressing the high risk of cyber-attacks from domestic, adversarial state and non-state actors. As the Sector Risk Management Agency, EPA will continue in a voluntary context to provide robust support to all states and water systems that seek to protect the drinking water of their populace from the growing cyber threat.**
- **We are continuing to host Regional Cyber Workshops to support primacy agencies in understanding funding and resources available to build cybersecurity capacity in the water sector.**

What is EPA doing in the meantime?

- In addition, EPA is continuing to provide technical assistance to drinking water and wastewater utilities via the Cybersecurity Evaluation Program, which conducts cyber assessments for water systems, and the Cybersecurity Technical Assistance Program, where water systems, states, and other parties can submit questions concerning cybersecurity and receive a response from a cyber subject matter expert.

What is EPA doing in the meantime?

- EPA is also providing training on how to conduct a Cybersecurity Assessment for circuit riders and other technical assistance providers to increase capacity for assessments in the Water Sector. EPA plans to support states that request similar training as well.
- EPA is conducting Water Sector Cybersecurity Incident Tabletop Exercises with states, drinking water systems, wastewater systems, emergency responders, FBI, and CISA to provide opportunities for systems to test their cyber response plans and promote available resources to increase cyber resilience.
- EPA continues to work with FBI, CISA, and other federal partners on reported cyber incidents to notify the targeted utility, assess the consequences of the cyber incident, and formulate recommendations for response and future mitigation actions.



EPA Cybersecurity Assessment Resources for Water and Wastewater Utilities

Free Cybersecurity Assessment Resources

Self-Assessment

EPA' Checklist and Water
Cybersecurity Evaluation Tool
(WCAT)

Third-Party Assessment

EPA's Water Sector
Cybersecurity Evaluation
Program

Cybersecurity Assessment Resources Available on our Website

Resources to Conduct Cybersecurity Assessments

Self-Assessment Resources

- EPA: [Water Cybersecurity Assessment Tool and Risk Mitigation Plan Template \(xlsx\)](#) (100.48 KB, 03/31/2023)
- EPA: [Guidance on Evaluating Cybersecurity During Public Water System Sanitary Surveys \(pdf\)](#) (883.93 KB, 02/23, 817-B-23-001) (Checklist in Appendix)
- [CISA: Cyber Resilience Review](#) [↗](#)
- [CISA: Cross-Sector Cybersecurity Performance Goals](#) [↗](#)
- [CISA: Cybersecurity Evaluation Tool](#) [↗](#)
- [NIST: AXIO Cybersecurity Program Assessment Tool](#) [↗](#)
- [MS-ISAC: Risk Assessment Method](#) [↗](#)
- [MS-ISAC: Critical Security Controls](#) [↗](#)


Third-Party Assessment Resources

- [EPA: Water Sector Cybersecurity Evaluation Program](#)
- [CISA: CISA Cybersecurity Advisor](#) [↗](#)

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 Includes:
 - Assessment Workbook
 - Assessment Report
 - Risk Mitigation Plan

EPA Water Cybersecurity Assessment Tool (WCAT)



Please read the following instructions in their entirety prior to completing the assessment.

How to Use This Tool

- 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.

WCAT Assessment Workbook

EPA Cybersecurity Checklist

Utility ID:

W/WS Staff (Initials Only):

Assessment Date:

Assessor:



Topic	Topic Number	Checklist Number	Question	Response	Recommendation	Explanation of Response
Account Security	1.0	1.1	Does the W/WS detect and block repeated unsuccessful login attempts?		Where technically feasible, System Administrators should be notified after a specific number of consecutive, unsuccessful login attempts in a short amount of time. At that point, future login attempts by the suspicious account should be blocked for a specified time or until re-enabled by an Administrator.	
		1.2	Does the W/WS change default passwords?		When feasible, change all default manufacturer or vendor passwords before equipment or software is put into service.	
		1.3	Does the W/WS require multi-factor authentication (MFA) wherever possible, but at a minimum to remotely access W/WS Operational Technology (OT) networks?		Deploy MFA as widely as possible for both information technology (IT) and operational technology (OT) networks. At a minimum, MFA should be deployed for remote access to the OT network.	
		1.4	Does the W/WS require a minimum length for passwords?		Where feasible, implement a minimum length requirement for passwords. Implementation can be through a policy or administrative controls set in the system.	
		1.5	Does the W/WS separate user and privileged (e.g., System Administrator) accounts?		Restrict System Administrator privileges to separate user accounts for administrative actions only and evaluate administrative privileges on a recurring basis to be sure they are still needed by the individuals who have these privileges.	
		1.6	Does the W/WS require unique and separate credentials for users to access OT and IT networks?		Require a single user to have two different usernames and passwords; one set is to be used to access the IT network, and the other set is to be used to access the OT network. This reduces the risk of an attacker being able to move between both networks using a single login.	
		1.7	Does the W/WS immediately disable access to an account or network when access is no longer required due to retirement, change of role, termination, or other factors?		Take all steps necessary to terminate access to accounts or networks upon a change in an individual's status making access unnecessary.	
		2.1	Does the W/WS require approval before new software is installed or deployed?		Only allow Administrators to install new software on a W/WS-issued asset.	

Introduction

Assessment Workbook

Assessment Report

Risk Mitigation Plan



Overview of EPA's Cybersecurity Checklist

Cybersecurity Control Family	# of Questions/Goals
1. Account Security	7
2. Device Security	5
3. Data Security	4
4. Governance and Training	5
5. Vulnerability Management	3
6. Supply Chain/Third Party	2
7. Response and Recovery	4
8. Other	3
Total:	33

Questions from the WCAT

- ***1.2 Does the w/ws change default passwords?***
- ***2.3 Does the w/ws maintain an updated inventory of all OT and IT network assets?***
- ***3.1 Does the w/ws collect security logs (e.g., system and network access, malware detection) to use in both incident detection and investigation?***

Questions from the WCAT

- ***4.3 Does the w/ws provide at least annual training for all utility personnel that covers basic cybersecurity concepts?***
- ***5.1 Does the w/ws patch or otherwise mitigate known vulnerabilities within the recommended timeframe?***
- ***6.2/6.3 Does the w/ws require that all OT and IT vendors and service providers notify the utility of any security incidents or vulnerabilities in a risk-informed timeframe?***

Questions from the WCAT

- ***7.2 Does the w/ws have a written cybersecurity Incident Response (IR) Plan for critical threat scenarios which is regularly practiced and updated?***
- ***8.1 Does the w/ws segment OT and IT networks and deny connections to the OT network by default unless explicitly allowed?***

WCAT Assessment Report Tab

- Provides a summary of results from the completed Cybersecurity Assessment
- This assessment report is intended to be placed in a Word Document and provided to the utility. To do this, highlight the cells on this tab, copy, and paste in a blank Word Document

Account Security			
Checklist Number	Question	Response	Explanation of Response
1.1	Does the PWS detect and block repeated unsuccessful login attempts?	Yes	
1.2	**Does the PWS change default passwords?	Yes	
1.3	**Does the PWS require multi-factor authentication (MFA) wherever possible, but at a minimum to remotely access PWS Operational Technology (OT) networks?	In Progress	
1.4	**Does the PWS require a minimum length for passwords?	No	
1.5	Does the PWS separate user and privileged (e.g., System Administrator) accounts?	No	
1.6	Does the PWS require unique and separate credentials for users to access OT and IT networks?	No	
1.7	**Does the PWS immediately disable access to an account or network when access is no longer required due to retirement, change of role, termination, or other factors?	No	

WCAT Cybersecurity Risk Mitigation Plan Template

Account Security	1.4	Question:	Does the W/WS require a minimum length for passwords?
		Planned Risk Mitigation Action:	<i>Where feasible, implement a minimum length requirement for passwords. Implementation can be through a policy or administrative controls set in the system.</i>
		Current Status:	Not Started
		Target Completion Date:	January 1st, 2024
		W/WS Personnel Responsible:	Joe Smith and Kate Ward
		Involved Departments and/or Agencies:	System Administrator
		W/WS Notes:	We will be working internally to get a procedure in place to implement this control.

EPA Water Sector Cybersecurity Evaluation Program

- This program will conduct cybersecurity assessments for water and wastewater utilities.
- Uses the EPA Checklist.
- Utilities will receive a report with response to the checklist questions that shows cybersecurity gaps.
- Link:
<https://www.epa.gov/waterriskassessment/forms/epas-water-sector-cybersecurity-evaluation-program>

EPA's Water Sector Cybersecurity Evaluation Program

Please share your information to receive more information about EPA's Water Sector Cybersecurity Evaluation Program.

Primary Contact Name *

Secondary Contact Name

Primary Contact Email Address *

Secondary Contact Email Address

Primary Contact Phone Number *

Secondary Contact Phone Number

Email addresses for all additional contacts to be included in communications (if applicable)

Cybersecurity Technical Assistance Program for the Water Sector

- Under this program, states and PWSs 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.
- Link:
<https://www.epa.gov/waterriskassessment/forms/cybersecurity-technical-assistance-water-utilities>

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

EPA Cybersecurity Checklist Fact Sheets

- Fact Sheets are available for each question on the EPA Checklist and include:
 - Recommendations
 - Overview of why the control is important
 - Additional Guidance
 - Implementation Tips
 - Additional Resources
 - Estimate for Cost, Impact, and Complexity

Account Security: Detection of Unsuccessful (Automated) Login Attempts

COST: \$\$\$\$ IMPACT: HIGH COMPLEXITY: LOW

1.1: Does the PWS detect and block repeated unsuccessful login attempts?

Recommendation: Where technically feasible, system administrators should be notified after a specific number of consecutive, unsuccessful login attempts in a short amount of time. At that point, future login attempts by the suspicious account should be blocked for a specified time or until re-enabled by an administrator.

Why is this control important?

A common technique that attackers use to break into OT and IT systems is to attempt to “guess” an actual username and password login combination. This can be accomplished by manually guessing an account’s password, using a list of common passwords, or through a technique called a *brute force attack*. In this type of attack, an attacker uses a trial-and-error approach to systematically guess login credentials. The attacker submits combinations of usernames and passwords, generally using an automated password-breaking tool, until the guess is correct. Blocking an attacker from future guesses after a specified number of incorrect guesses can stop these types of attacks.

Additional Guidance

- Enable systems to automatically notify (e.g., by a computer-generated alert) security teams or the system administrator after a specific number of consecutive, unsuccessful login attempts in a short time period (e.g., five failed attempts in under 2 minutes).
- Enable account lockout settings on applicable systems to prevent future login attempts for the suspicious account for a minimum time or until the account is re-enabled by the system administrator.
- It is a good practice to ensure that the account lockout duration is set to 15 minutes (or more) or to require a user with administrative privileges to unlock a user’s account.
- Log and store the alert information for analysis. Use sound logging procedures - a log should capture event source, date, username, timestamp, source addresses, destination addresses, and any other useful information that could assist in a forensic investigation.

Implementation Tips

Depending on your version of Windows, you can use the Local Security Policy to restrict the number of login attempts. To access this feature, type “Local Security Policy” in the search box in the Start menu and click on the Local Security Policy App. Once the menu pane opens, click on “Account Policies” to adjust login attempts and lockout duration.

If your PWS utilizes a Microsoft Domain where many systems and user accounts are connected to a single domain, these settings can be managed using Group Policy Objects (GPOs). The Account Lockout Policy settings can be enabled in the following location in the Group Policy Management Console: Computer Configuration\Windows Settings\Security

Cybersecurity Incident Action Checklist



Incident Action Checklist – Cybersecurity

For on-the-go convenience, the actions in this checklist are divided up into three "rip & run" sections and provide a list of activities that water and wastewater utilities can take to prepare for, respond to and recover from a cyber incident. You can also populate the "My Contacts" section with critical information that your utility may need during an incident.

Cyber Incidents and Water Utilities

Cyberspace and its underlying infrastructure are vulnerable to a wide range of hazards from both physical attacks as well as cyberthreats. Sophisticated cyber actors and nation-states exploit vulnerabilities to steal information and money and are developing capabilities to disrupt, destroy or threaten the delivery of essential services such as drinking water and wastewater.

As with any critical enterprise or corporation, drinking water and wastewater utilities must evaluate and mitigate their vulnerability to a cyber incident and minimize impacts in the event of a successful attack. Impacts to a utility may include, but are not limited to:

- Interruption of treatment, distribution or conveyance processes from opening and closing valves, overriding alarms or disabling pumps or other equipment
- Theft of customers' personal data such as credit card information and social security numbers stored in on-line billing systems
- Defacement of the utility's website or compromise of the email system
- Damage to system components
- Loss of use of industrial control systems (e.g., SCADA system) for remote monitoring of automated treatment and distribution processes



Actions to Prepare for a Cyber Incident



Utility

- ☐ Identify all mission critical information technology (IT) systems, considering business enterprise, process control and communications. Document the key functions of the mission critical objectives, and identify the personnel or entity responsible for operating and maintaining each IT system.
- ☐ Identify an overall IT security lead to coordinate with each IT system manager and oversee all cyber-related duties.
- ☐ Ensure that IT system managers enforce cybersecurity practices on all business enterprise, process control and communications systems. For example, verify adherence to user authentication, current anti-virus software and installation of security patches.
- ☐ Identify priority points of contact for reporting a cyber incident and requesting assistance with response and recovery. Include any state resources that may be available such as State Police, National Guard Cyber Division or mutual aid programs, as well as the Department of Homeland Security Cybersecurity and Infrastructure Security Agency (CISA) at <https://www.cisa.gov/reporting-cyber-incidents>.
- ☐ Review and update the utility's emergency response plan (ERP) to address a cyber incident impacting business enterprise, process control and communications systems. Account for all potential impacts on operations, and ensure emergency contacts are current.
- ☐ Prevent unauthorized physical access to IT systems through security measures such as locks, sensors and alarms. Include workstations and process control systems (e.g., programmable logic controllers or PLCs).
- ☐ Train all essential personnel to perform mission critical functions during a cyber incident that disables business enterprise, process control and communications systems. Include the manual operation of water collection, storage, treatment and conveyance systems.
- ☐ Conduct drills and exercises for responding to a cyber incident that disables critical business enterprise, process control and communications systems.

Cybersecurity Incident Action Checklist

Actions to Respond to a Cyber Incident



Utility

- ☐ If possible, disconnect compromised computers from the network to isolate breached components and prevent further damage, such as the spreading of malware. Do not turn off or reboot systems – this preserves evidence and allows for an assessment to be performed.
- ☐ Notify IT personnel and/or IT vendor of the incident and the need for emergency response assistance. In addition, DHS CISA can assist with IT system response and recovery (<https://www.cisa.gov/reporting-cyber-incidents>).
- ☐ Assess any damage to utility systems and equipment, along with disruptions to utility operations.
- ☐ Execute the utility ERP as needed, including notification of utility personnel, actions to restore operations of mission critical processes (e.g., switch to manual operation if necessary), and public notification (if required).
- ☐ Report the cyber incident as required to law enforcement and regulatory agencies.
- ☐ Notify any external entities (e.g., vendors, other government offices) that may have remote connections to the affected network(s).
- ☐ Document key information on the incident, including any suspicious calls, emails, or messages before or during the incident, damage to utility systems, and steps taken in response to the incident (including dates and times).

IT Staff or Vendor

- ☐ Review system and network logs, and use virus and malware scans to identify affected equipment, systems, accounts and networks.
- ☐ Document which user accounts were or are logged on, which programs and processes were or are running, any remote connections to the affected IT systems or network(s) and all open ports and their associated applications.
- ☐ If possible, take a “forensic image” of the affected IT systems to preserve evidence. Tools to take forensic images include Forensic Tool Kit (FTK) and EnCase.
- ☐ If possible, identify any malware used in the incident, any remote servers to which data may have been sent during the incident, and the origin of the incident. DHS CISA can assist with the forensic analysis (www.cisa.gov/reporting-cyber-incidents).
- ☐ Research and identify if any employee or customer personally identifiable information (PII) was compromised.
- ☐ Check the system back-up time stamp to determine if the back-up was compromised during the incident.
- ☐ Document all findings, and avoid modifying or deleting any data that might be attributable to the incident.

Actions to Recover from a Cyber Incident



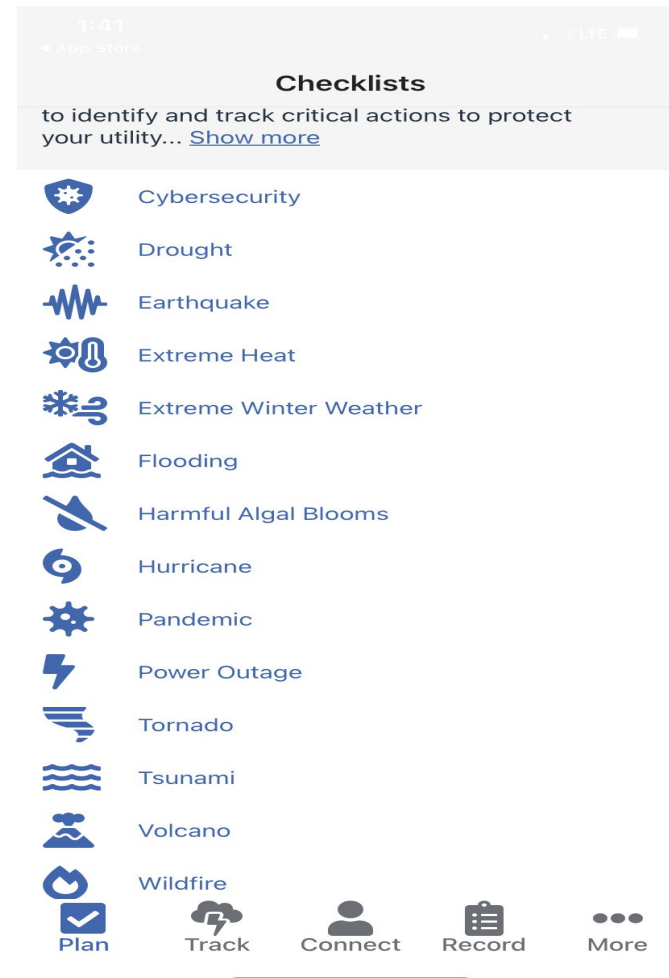
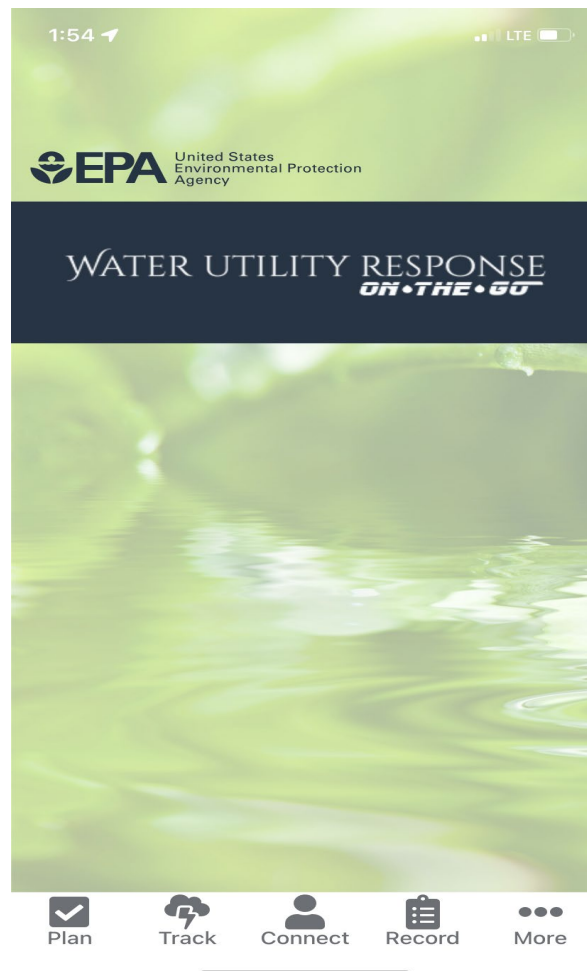
Utility

- ☐ Continue to work with IT staff, vendors and integrators, government partners and others to obtain needed resources and assistance for recovery.
- ☐ Notify affected employees and customers if any PII was compromised.
- ☐ Submit an incident report through WaterISAC (866-H2O-ISAC). Membership is not required to submit a report.
- ☐ Develop a lessons learned document and/or an after action report (AAR) to document utility response activities, successes, and areas for improvement. Create an improvement plan (IP) based on your AAR and use the IP to update your vulnerability assessment, ERP and contingency plans.
- ☐ Register for cybersecurity alerts and advisories from water sector and government partners to be aware of new vulnerabilities and threats. Two sources of cybersecurity alerts are WaterISAC, which has a basic membership that is free, and ICS-CERT (<https://ics-cert.us-cert.gov/alerts>).

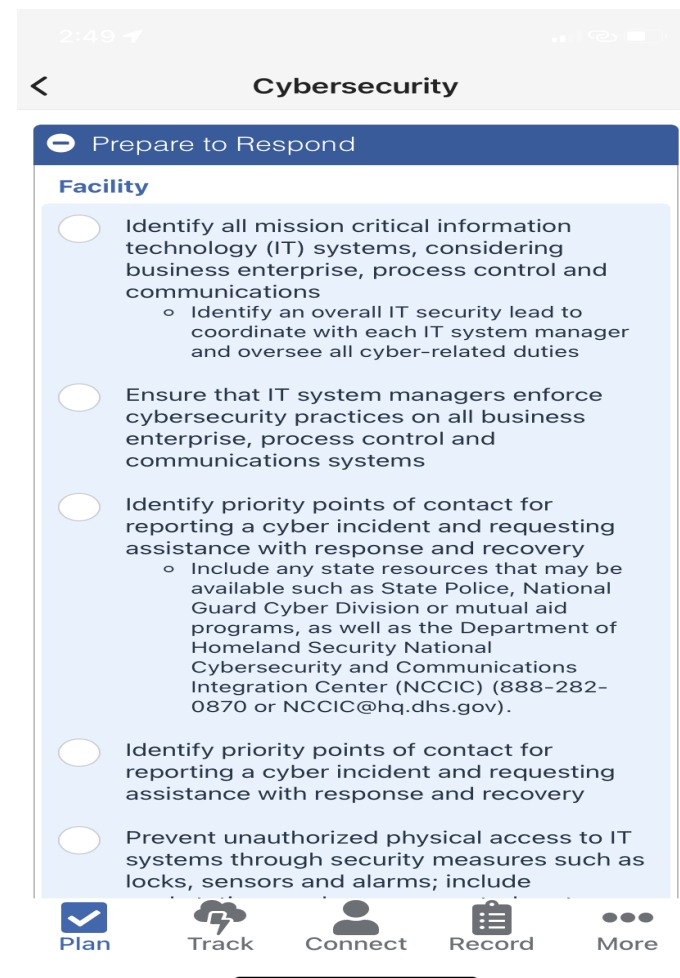
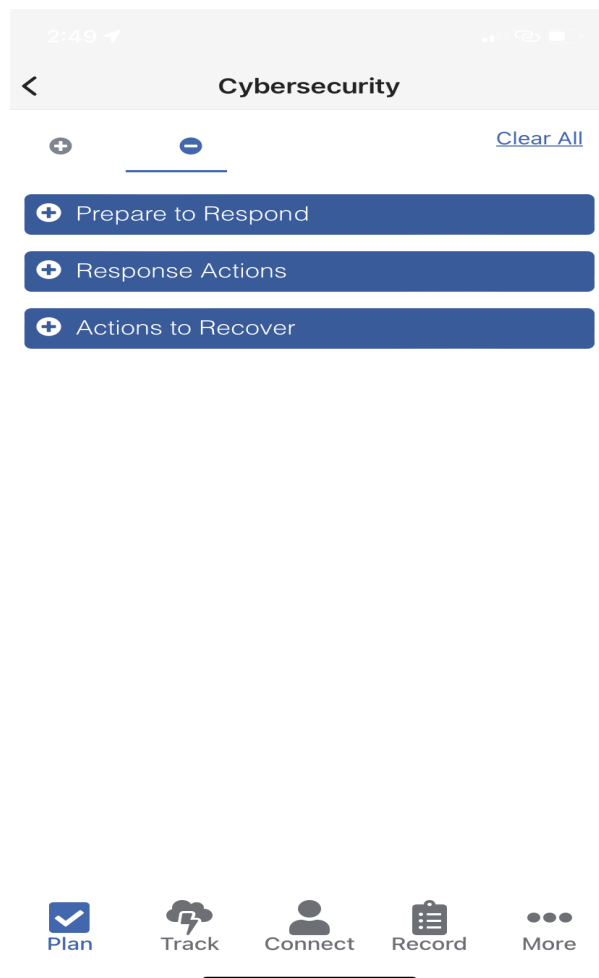
IT Staff or Vendor

- ☐ Remove any malware, corrupted files and other changes made to IT systems by the incident.
- ☐ Restore IT systems as required (e.g., re-image hard drives, reload software). DHS CISA can assist with the IT system recovery (<https://www.cisa.gov/reporting-cyber-incidents>).
- ☐ Restore compromised files from a system back-up that has not been compromised.
- ☐ Install patches and updates, disable unused services and perform other countermeasures to harden the system against known vulnerabilities that may have been exploited.

EPA Water Utility Response On The Go App



EPA Water Utility Response On The Go App



EPA-Provided Training

- **Webinars:**

- **Cybersecurity 101 – recording available on website**

- **Cybersecurity Assessment Training for Circuit Riders and Technical Assistance Providers**

- **Regional Workshops for Primacy Agencies:**

- Region 1 – September 21, 2023

- Region 2 – Completed

- Region 3 – Completed

- Region 4 – Completed

- Region 5 – Completed

- Region 6 – Completed

- Region 7 – Completed

- Region 8 – October 2, 2023

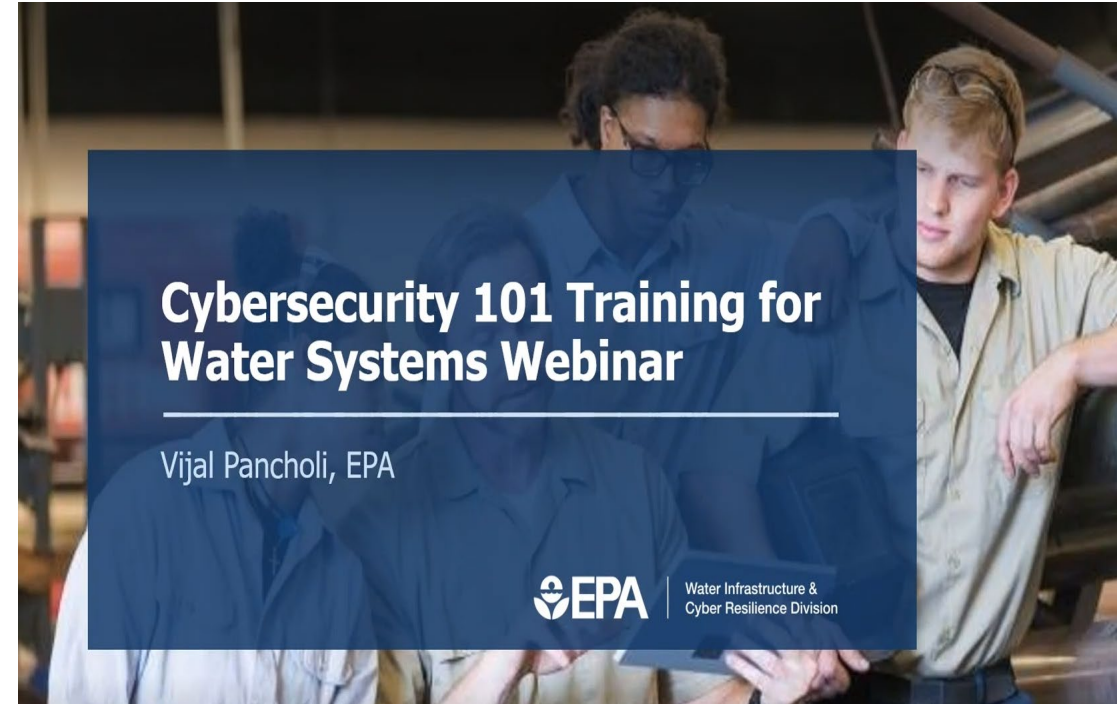
- Region 9 - Completed

- Region 10 – September 18, 2023

Cybersecurity 101 Webinar for Water Systems

- This webinar reviews basic cybersecurity topics including:
- Account security
- Device security
- Data security
- Training, and more.

Water system staff can benefit from this webinar by being introduced to baseline cybersecurity concepts from subject matter experts.



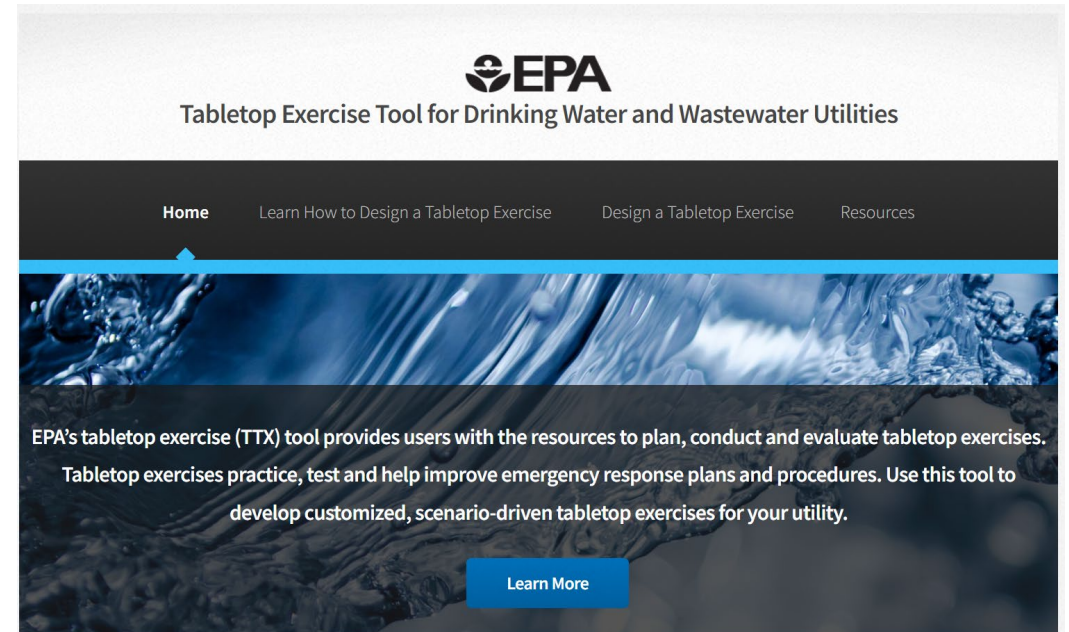
Link: <https://www.youtube.com/watch?v=e2QDbgrojb0>

EPA Tabletop Exercise Tool for Utilities

- You can download the TTX tool here:

<https://www.epa.gov/waterresiliencetraining/develop-and-conduct-water-resilience-tabletop-exercise-water-utilities>

If you are interested in having a TTX in your state, please contact us at watercyberta@epa.gov



Link to our Website

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

