Building Cyber Resilience Using EPA's Water and Wastewater Cybersecurity Incident Response Plan Template

Training Date and time 2026:

- April 30th
- 1:00-2:30pm ET

Introduction & General Description:

- EPA invites water sector professionals to learn about its new Drinking Water and Wastewater Systems Cybersecurity Incident Response Plan Template. This fully customizable template is designed to help all utilities prepare for, respond to, and recover from cybersecurity incidents affecting both information technology (IT) and operational technology (OT) systems.

- This webinar will introduce EPA's Incident Response Plan Template and accompanying instructions including how utility personnel can access, tailor, and operationalize the plan to meet system-specific needs.

- Participants will learn how the template is structured, how it supports utility preparedness, and how it aligns with SDWA Section 1433 requirements to incorporate cybersecurity into Emergency Response Plans (ERPs). The session will also highlight practical steps unities can take to adapt the template to their own operations.

- Intended audience: Drinking water and wastewater utility managers and operators; IT and OT staff; emergency response planners; and state and local partners.

Course Objectives:

- After attending this webinar, participants will be able to:
    - Understand the purpose and the structure of the EPA Incident Response Plan Template.
    - Apply the template to their own operational environment to identify planning gaps or opportunities for improvement.
    - Identify core elements of an effective incident response plan.

Course Format and Procedures:

- Format: Virtual Training (Instructor Led)
- Duration: 1:30:00
- Procedures:
    - Attend Training via training link (MS Teams or Zoom)
    - Answer all poll questions (9)
    - Remain in training for entire duration.
        - Final poll question is at the end of training session.

Course Agenda:

1.) **Introduction (5 minutes)**
2.) **Background (5 minutes)**

3.) **Why incident response planning matters (5 minutes)**
4.) **Overview of the Template (10 minutes)**
    a. **Steps to take before using the template**
    b. **How to use the template**
5.) **Key components of the template (25 minutes)**
6.) **Applying the template to your utility (10 minutes)**
7.) **Additional resources to support the development and implementation of the template (10 minutes)**
8.) **Next Steps (5 minutes)**
9.) **Q & A (10 minutes)**
10.) **Closing (5 minutes)**

Presenter Biographies:

- Brandon M. Carter: Sr. Cybersecurity Specialist with USEPA. (**MAIN**)
    - Brandon M. Carter is a member of EPA's Office of Water Emergency Response and Cybersecurity (OWERC). *He holds a master's degree in Information Systems Management from Bowie State University, as well as industry-standard cybersecurity certifications from CompTIA and (ISC)2.*

- Cameron Burden: Cybersecurity Specialist with USEPA **(ALTERNATE)**
    - Cameron Burden is a member of EPA's Office of Water Emergency Response and Cybersecurity (OWERC). Having earned a Bachelors in Information Technology, he now applies his knowledge in the Water Sector of EPA with the mission to inform U.S. Public Water Systems about cybersecurity best practices that will help improve the overall cyber posture in the water sector.

- Vijal Pancholi: Cybersecurity Specialist with USEPA **(ALTERNATE)**
    - Vijal Pancholi is a member of EPA's Office of Water Emergency Response and Cybersecurity (OWERC). He currently holds a bachelor's degree in Computer Networks and Cybersecurity and uses his knowledge to help the Water Sector increase their cyber resilience through webinars and outreach.

- Cole Dutton: Cybersecurity Specialist with USEPA. **(ALTERNATE)**
    - *Cole Dutton is a member of EPA's* Office of Water Emergency Response and Cybersecurity (OWERC)*. He holds a master's degree in Information Security from James Madison University, as well as industry-standard cybersecurity certifications from CompTIA and (ISC)2.*

Attendance Verification and Retention of Attendance Records (Same as Course Completion):

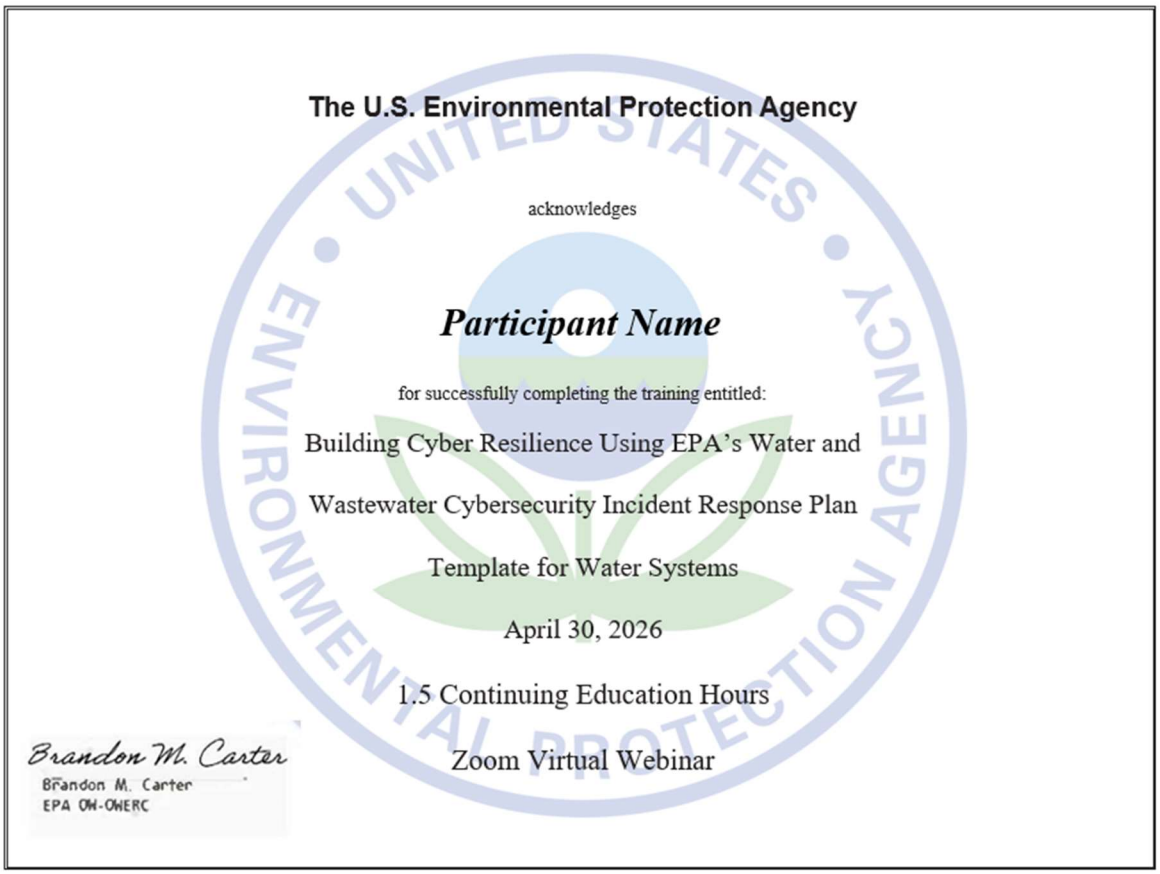
- Attend Virtual Webinar Course (instructor Led)
    - Answer Poll Questions (9)
    - Final Poll Question is at the end of the training to ensure participant attendance.
    - Attendee must register with the following information:
        - Name (first and last)

        - Email
        - Utility Name
        - State
    - Attendance records are kept by training date.

Criteria of Course Completion (Same as Attendance Verification):

- Attend Virtual Webinar Course (instructor Led)
    - Answer Poll Questions (9)
        - Final Poll Question is at the end of the training to ensure participant attendance.
        - Attendee must register with the following information:
            - Name (first and last)
            - Email
            - Utility Name
            - State
        - Attendance records are kept by training date.

Sample Certificate of Completion:



Polling Questions:

1. **What is your affiliation**?
    a. Drinking Water
    b. Wastewater
    c. Combined Utility
    d. Primacy Agency
    e. Technical Assistance Provider
    f. Other
2. **Does your utility have an established Cybersecurity Incident Response Plan (CIRP)?**
    a. Yes, a formal documented plan
    b. Yes, but it is informal or incomplete
    c. No plan in place
    d. I don't know
    e. I am not a utility
3. **What type of incident concerns you or your organization the most:**
    a. Cybersecurity Incident
    b. Water contamination event
    c. Natural disaster
    d. Other (please feel free to place in the chat)
4. **What type of CYBER incident concerns you or your organization the most?**
    a. Foreign State-sponsored attack
    b. Ransomware attack
    c. Insider threat
    d. Unauthorized systems access
    e. Other (please feel free to place in the chat)
    f. I don't know
5. **How often does your organization exercise, test, or review your CIRP?**
    a. Every year (or more frequently)
    b. Every two years (or less frequently)
    c. Other (please feel free to place in the chat)
    d. I don't know
    e. We do not currently have a CIRP
6. **Has your organization conducted cybersecurity tabletop exercise (TTX)?**
    a. Yes
    b. No
    c. I don't know
7. **Please rate the quality, relevance, and usefulness of EPA's presentation:**
    a. Excellent
    b. Great
    c. Average
    d. Fair
    e. Poor
8. **Do you have a process in place to report incidents to the federal level, whether it's to FBI, CISA,**

and/or EPA?

a. Yes
b. No
c. I don't know
d. I am not a utility

9. **After today's exercise what single step will you take to strengthen your utility's cybersecurity posture?**
    a. Create a Cybersecurity Incident Response Plan
    b. Undergo a Cybersecurity Assessment
    c. Review, Update, and Test Cybersecurity Incident Response Plan
    d. Check System Back-up Procedures
    e. Educate Employees on Basic Cybersecurity Practices
    f. Other (please feel free to type into the chat)