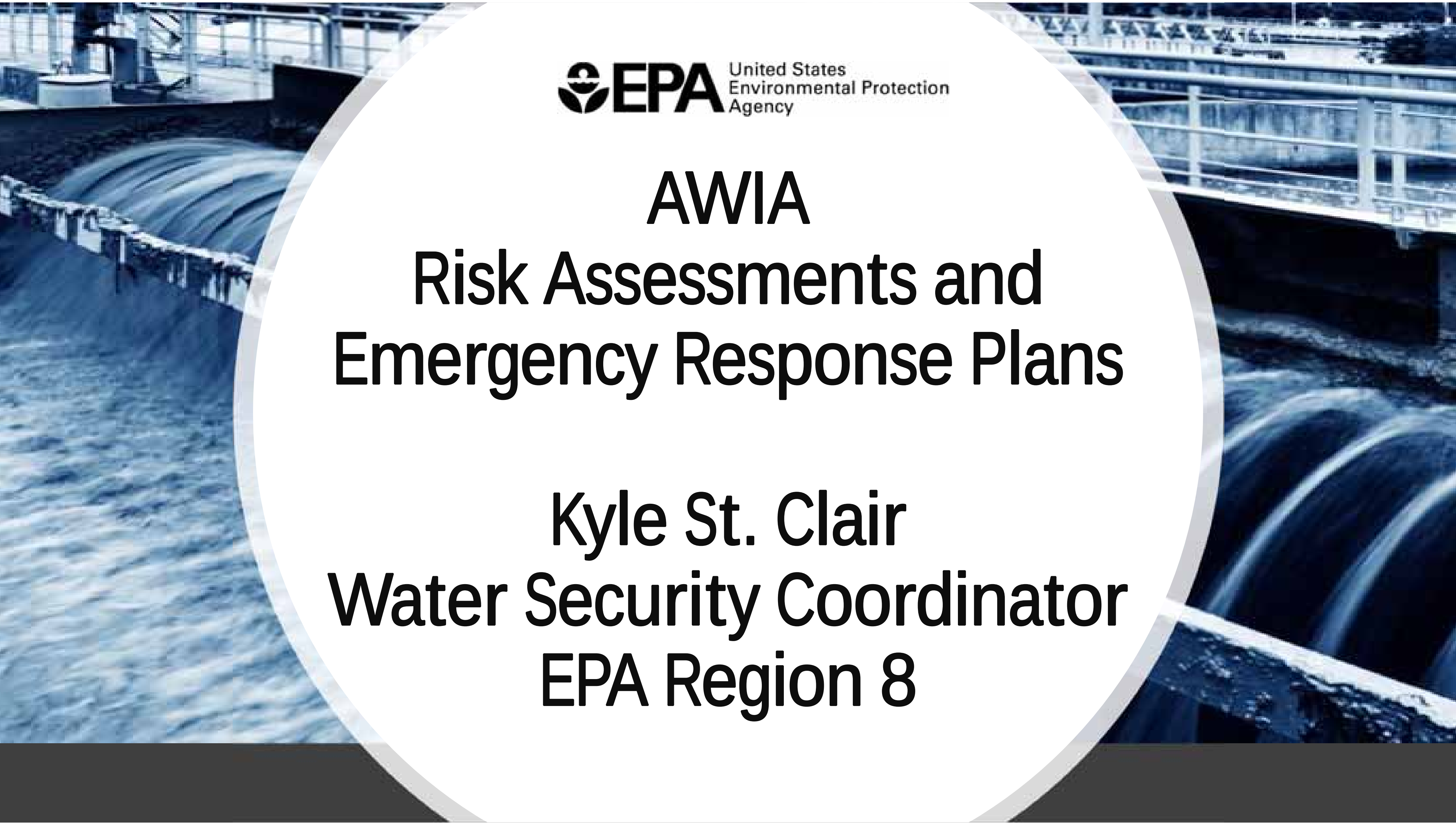


EPA United States Environmental Protection Agency

AWIA
Risk Assessments and Emergency Response Plans

Kyle St. Clair
Water Security Coordinator
EPA Region 8

Agenda

- AWIA Section 2013 Overview
- Risk and Resilience Assessment Requirements
- Vulnerability Self-Assessment Tool
- Emergency Response Plan Requirements
- Emergency Response Plan Guidance and Template
- Online Certification System
- In-Person Training Opportunities
- Exercise: Fill Out an Emergency Response Plan

Overview

AWIA Section 2013 (a) – (f)

Replaces SDWA Section 1433 (from 2002 Bioterrorism Act)

Applies to all community water systems serving more than 3,300 people

Conduct Risk and Resilience Assessments and update Emergency Response Plans (ERP)

Submit **certifications to EPA** by specified deadlines

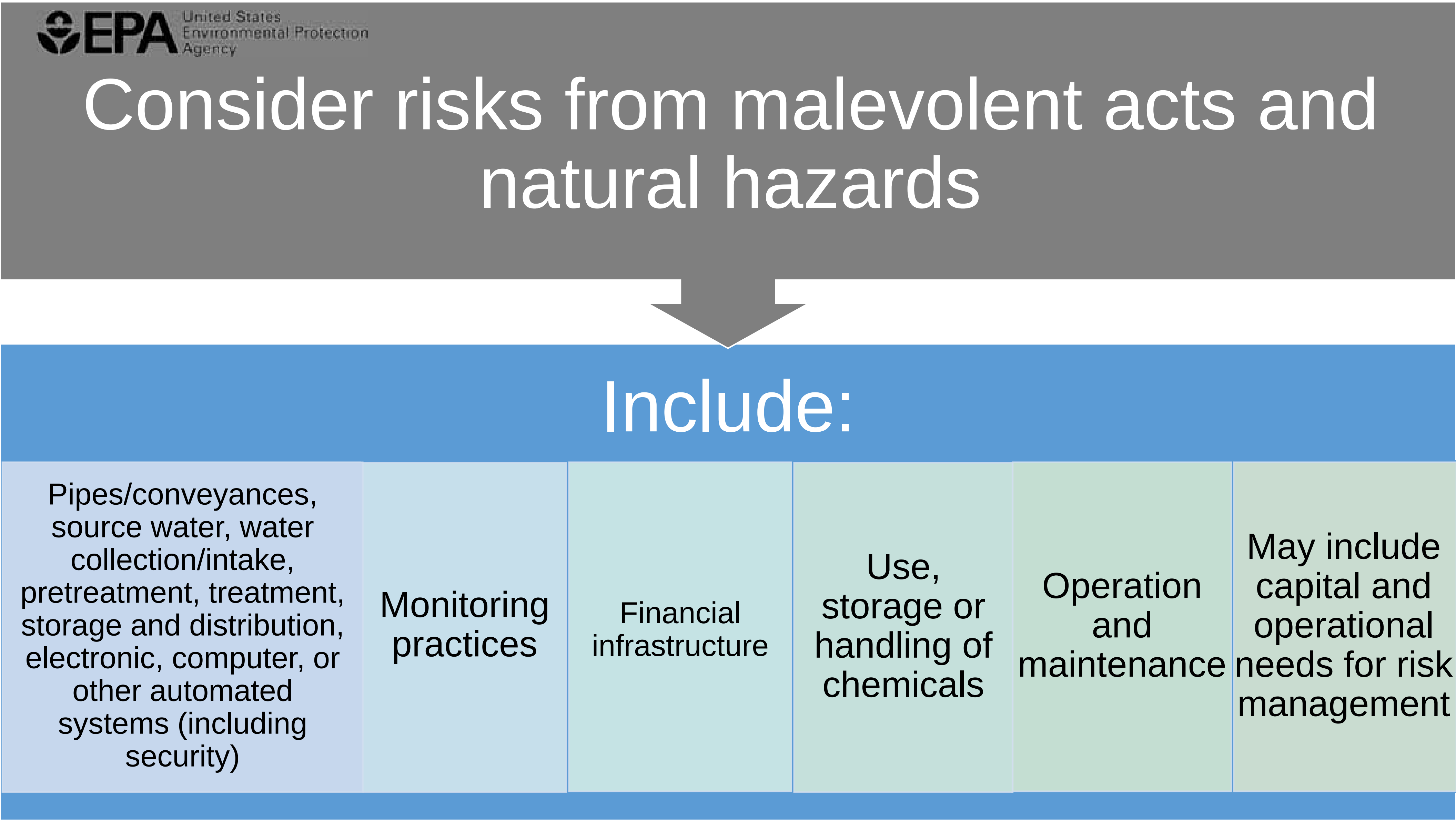
Review risk assessments and ERPs every five years

Coordinate with local emergency planning committees

Maintain records

Risk and Resilience Assessments (RA)

EPA United States Environmental Protection Agency



Consider risks from malevolent acts and natural hazards

Include:

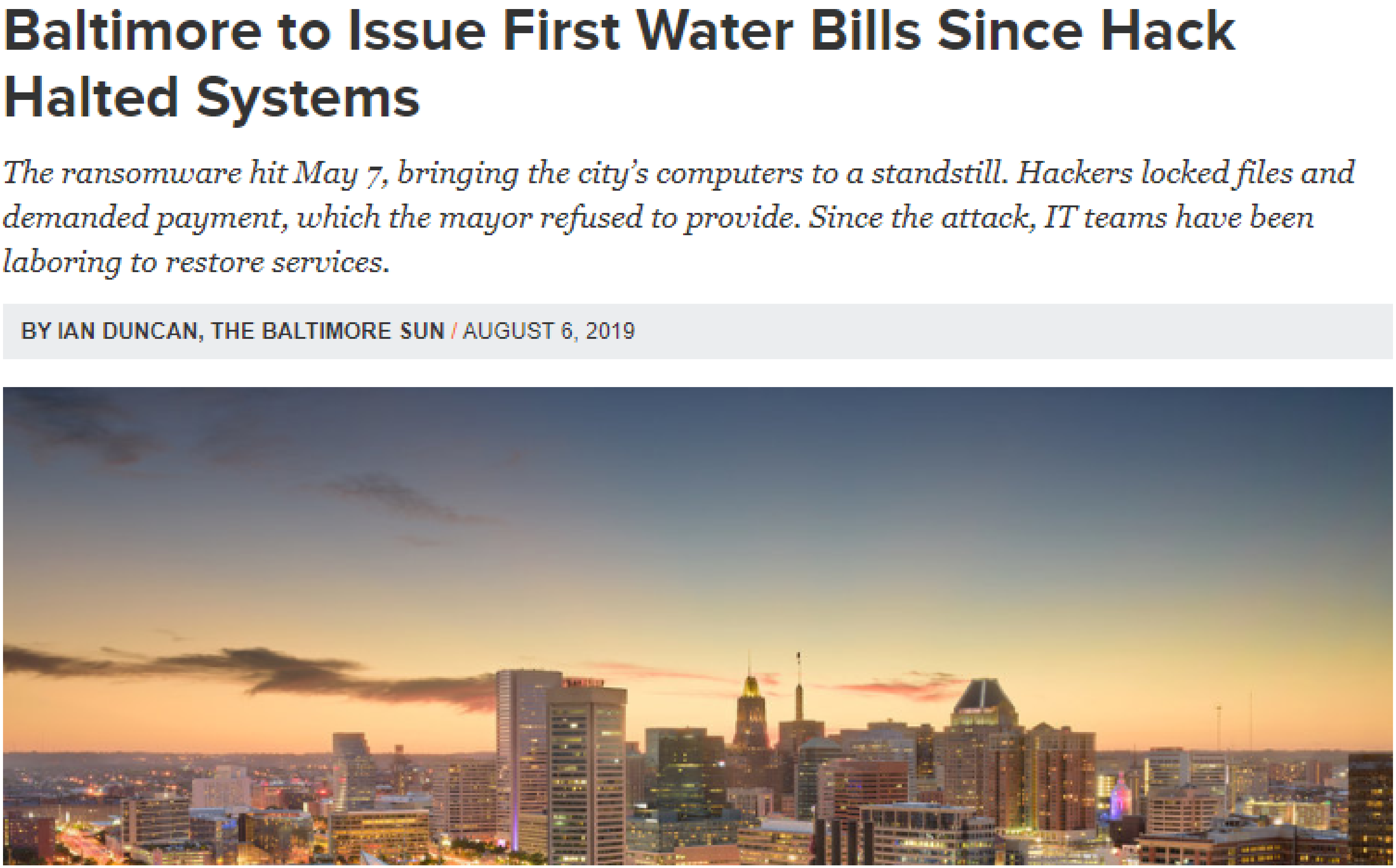
- Pipes/conveyances, source water, water collection/intake, pretreatment, treatment, storage and distribution, electronic, computer, or other automated systems (including security)
- Monitoring practices
- Financial infrastructure
- Use, storage or handling of chemicals
- Operation and maintenance
- May include capital and operational needs for risk management

United States Environmental Protection Agency

Baseline Information on Malevolent Acts

- Helps the water system identify malevolent acts to include in their risk assessments.
- Help water systems estimate the threat likelihood for malevolent acts
- Estimating three parameters
  1. Threat Likelihood: the annual probability that a perpetrator will attempt to carry out the malevolent act against the facility.
  2. Vulnerability: the probability that the malevolent act will have an adverse impact on the facility; and
  3. Consequences: the public health and economic consequences resulting from the impact of the malevolent act on the facility.

This is the most difficult risk parameter to estimate because it requires projecting the actions of the perpetrator



Baltimore to Issue First Water Bills Since Hack Halted Systems

The ransomware hit May 7, bringing the city's computers to a standstill. Hackers locked files and demanded payment, which the mayor refused to provide. Since the attack, IT teams have been laboring to restore services.

BY IAN DUNCAN, THE BALTIMORE SUN / AUGUST 6, 2019

EPA United States Environmental Protection Agency
VSAT Web
Vulnerability Self Assessment Tool

Vulnerability Self-Assessment Tool Web 2.0

- VSAT Web 2.0 can be used to conduct an AWIA Section 2013- compliant risk assessment
- Designed for computers and mobile devices like tablets and iPads (not phones)
- Complies with risk assessment standards, and offers liability protection under the Department of Homeland Security's Support Anti-Terrorism by Fostering Effective Technologies (SAFETY) Act program

New Version Available

EPA United States Environmental Protection Agency

Use of Previous Risk Assessment and ERP

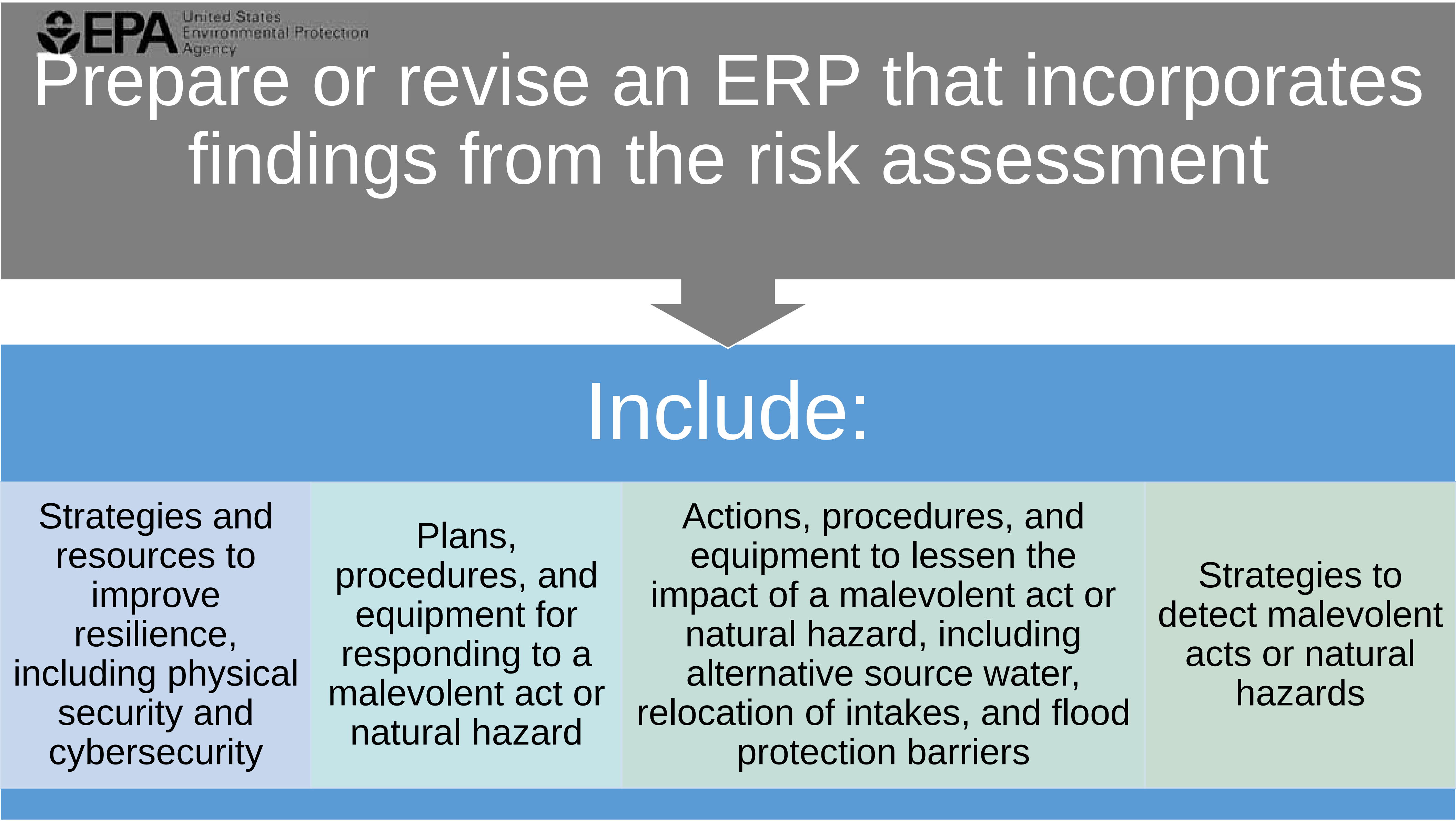
- A CWS may use a risk assessment or ERP developed prior to enactment of the AWIA
- To meet certification requirements, a previous risk assessment or ERP must:
  - ❑ Include all assessment or response components listed in the law; and
  - ❑ Reflect the current condition of the CWS.
- If required assessment or response components have been omitted, the CWS may add those components
- If the CWS has undergone modifications, the CWS may update the risk assessment or ERP where needed

Preparing for a ERP Development

1. Conduct a risk and resilience assessment.
2. Identify state regulatory requirements.
3. Identify and integrate local plans.
4. Coordinate with Local Emergency Planning Committees (LEPCs) and response partners.
5. Plan for resources.

Emergency Response Plans (ERP)

EPA United States Environmental Protection Agency



EPA United States Environmental Protection Agency

Prepare or revise an ERP that incorporates findings from the risk assessment

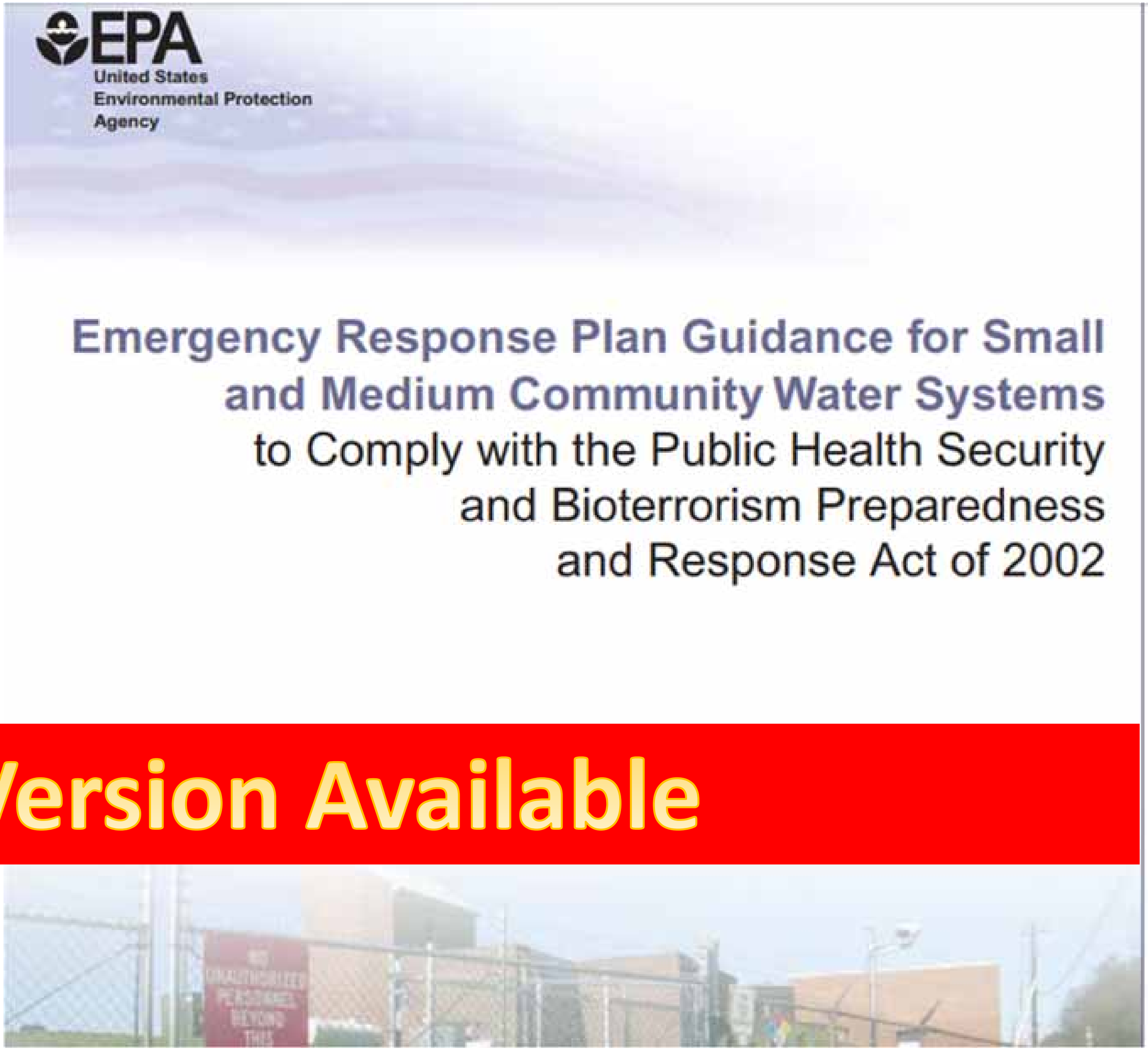
Include:

- Strategies and resources to improve resilience, including physical security and cybersecurity
- Plans, procedures, and equipment for responding to a malevolent act or natural hazard
- Actions, procedures, and equipment to lessen the impact of a malevolent act or natural hazard, including alternative source water, relocation of intakes, and flood protection barriers
- Strategies to detect malevolent acts or natural hazards

EPA United States Environmental Protection Agency

Emergency Response Plan Guidance

- Utilities should not use the previous version of the ERP to develop an ERP because it is missing new requirements.
- 4 sections organized around the requirements.



EPA
United States
Environmental Protection
Agency

Emergency Response Plan Guidance for Small and Medium Community Water Systems
to Comply with the Public Health Security and Bioterrorism Preparedness and Response Act of 2002

New Version Available

United States Environmental Protection Agency

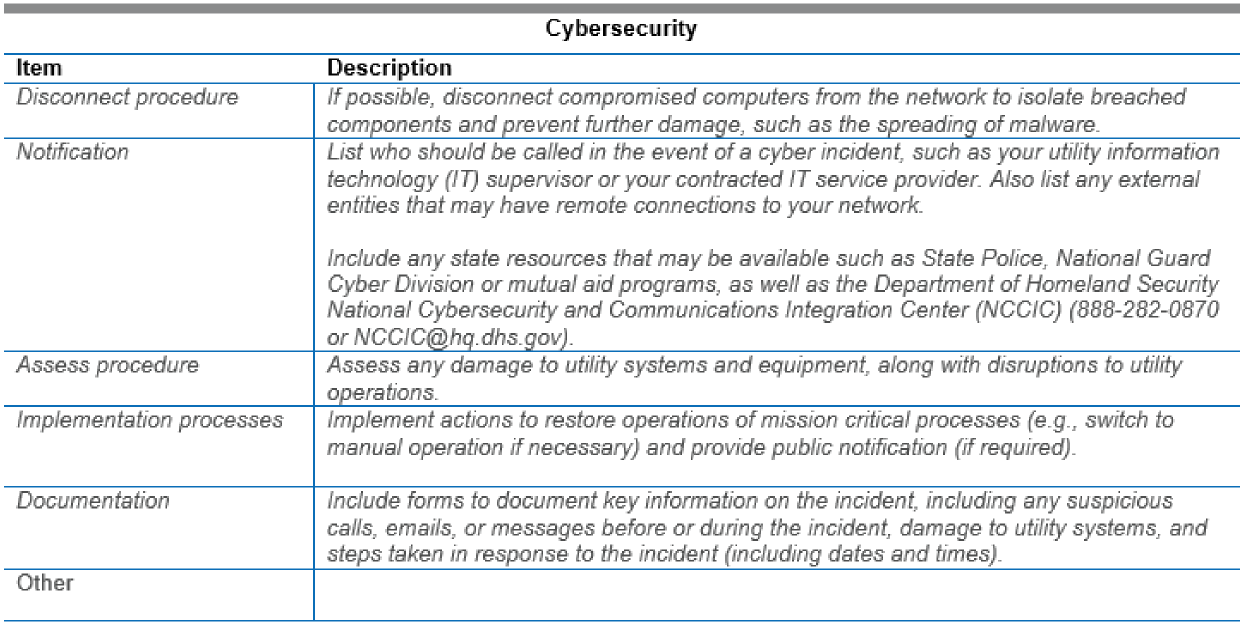
Sections of the Emergency Response Plan

- Utility Overview
- Resilience Strategies
- Emergency Plan & Procedures
  - Core Procedures
  - Incident Procedures
- Mitigation Actions
- Detection Strategies

Core Response Procedures

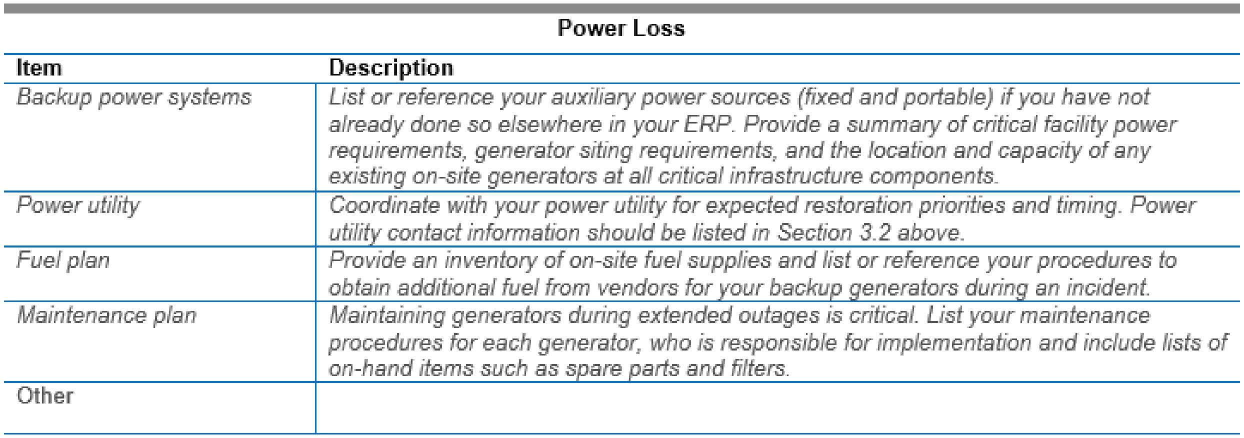
- Core procedures are the “building blocks” for incident-specific procedures, since the apply across a broad variety of incidents.
  - Core procedures include:
    - Access
    - Physical Security
    - Cybersecurity
    - Power Loss
    - Emergency Alternate Drinking Water Supplies
    - Sampling and Analysis
    - Family and Utility Personnel Well Being

Core Response Procedure Examples



Cybersecurity

Item	Description
Disconnect procedure	*If possible, disconnect compromised computers from the network to isolate breached components and prevent further damage, such as the spreading of malware.*
Notification	*List who should be called in the event of a cyber incident, such as your utility information technology (IT) supervisor or your contracted IT service provider. Also list any external entities that may have remote connections to your network.* *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 National Cybersecurity and Communications Integration Center (NCCIC) (888-282-0870 or NCCIC@hq.dhs.gov).*
Assess procedure	*Assess any damage to utility systems and equipment, along with disruptions to utility operations.*
Implementation processes	*Implement actions to restore operations of mission critical processes (e.g., switch to manual operation if necessary) and provide public notification (if required).*
Documentation	*Include forms to 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).*
Other	



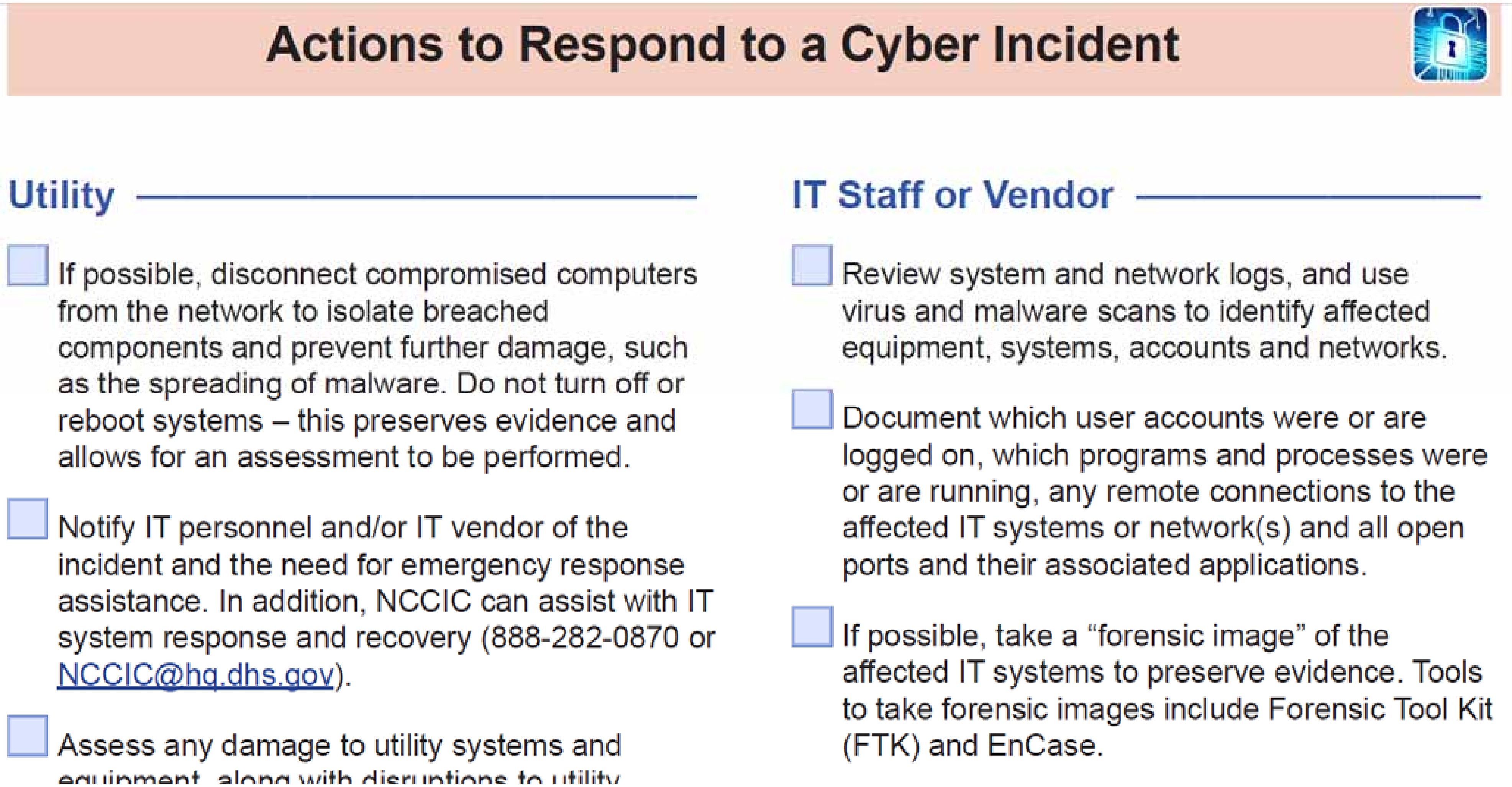
Power Loss

Item	Description
Backup power systems	*List or reference your auxiliary power sources (fixed and portable) if you have not already done so elsewhere in your ERP. Provide a summary of critical facility power requirements, generator siting requirements, and the location and capacity of any existing on-site generators at all critical infrastructure components.*
Power utility	*Coordinate with your power utility for expected restoration priorities and timing. Power utility contact information should be listed in Section 3.2 above.*
Fuel plan	*Provide an inventory of on-site fuel supplies and list or reference your procedures to obtain additional fuel from vendors for your backup generators during an incident.*
Maintenance plan	*Maintaining generators during extended outages is critical. List your maintenance procedures for each generator, who is responsible for implementation and include lists of on-hand items such as spare parts and filters.*
Other	

United States
Environmental Protection
Agency

Incident-Specific Response Procedures (ISRPs)

- Incidents include but are not limited to the following:
  - Cyber-Attack
  - Tornado
  - Tsunami
  - Volcanic Activity
  - Wildfire
  - Source Water Contamination
  - Distribution System Contamination
  - Hurricane
  - Drought
  - Earthquake
  - Extreme Cold and Winter Storms
  - Extreme Heat
  - Harmful Algal Bloom
  - Flooding



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, NCCIC can assist with IT system response and recovery (888-282-0870 or NCCIC@hq.dhs.gov).

□ Assess any damage to utility systems and equipment, along with disruptions to utility

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.

https://www.epa.gov/waterutilityresponse/incident-action-checklists-water-utilities

EPA United States Environmental Protection Agency

Certification Due Dates

Risk Assessment

Population served
≥100,000

March 31, 2020

DUE

Population served
50,000-99,999

December 31, 2020

DUE

Population served
3,301-49,999

June 30, 2021

DUE

ERP

Certify ERP not later than 6 months after completion of the risk assessment

United States Environmental Protection Agency

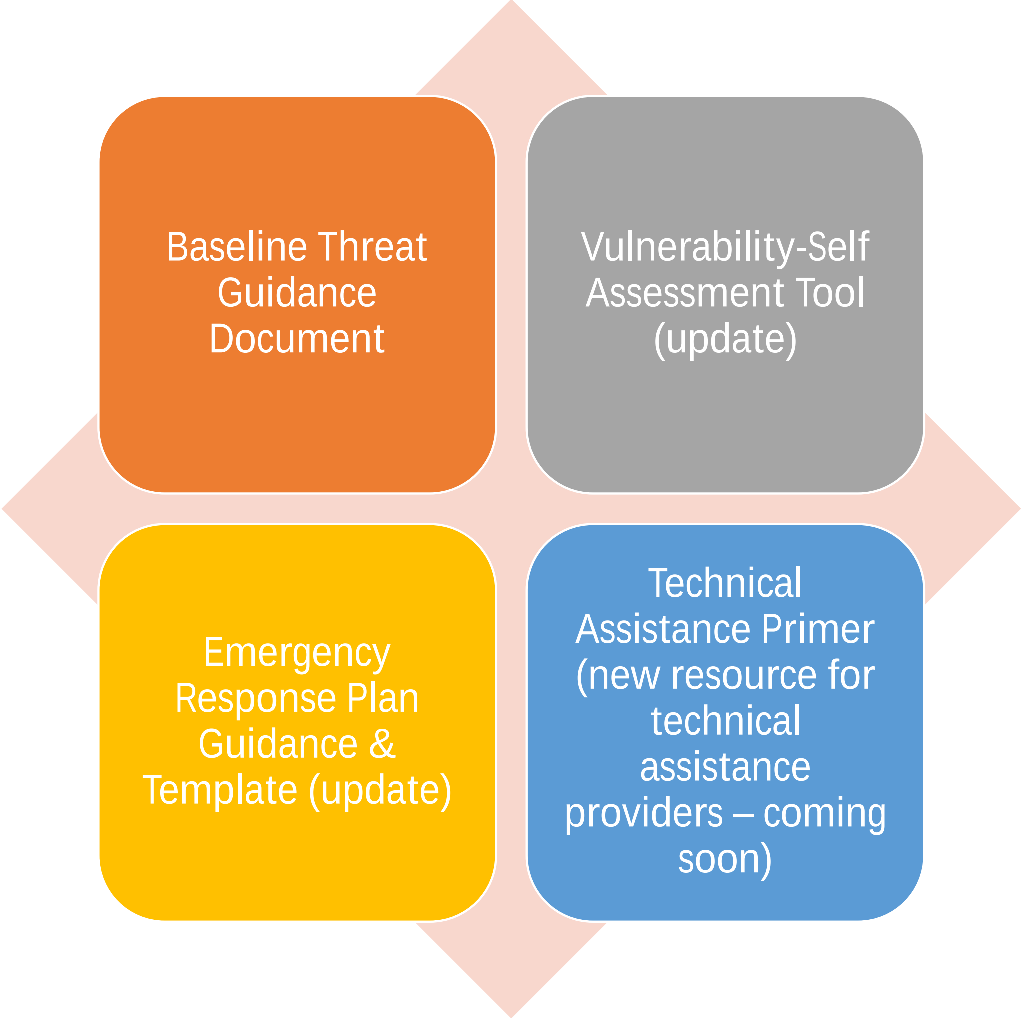
Certification Submission

EPA has three options for submittal:

- Regular mail (standard form)
- Email (standard form)
- **Secure online portal:**
    - Will provide online receipt & notifications

United States Environmental Protection Agency

Compliance Resources



Baseline Threat Guidance Document

Vulnerability-Self Assessment Tool (update)

Emergency Response Plan Guidance & Template (update)

Technical Assistance Primer (new resource for technical assistance providers – coming soon)

Outreach and Communications Efforts

Fact Sheet

Posted @ https://www.epa.gov/waterresilience/overview-new-risk-assessment-and-emergency-response-plan-requirements-community

Video

Available in Fall 2019

Training

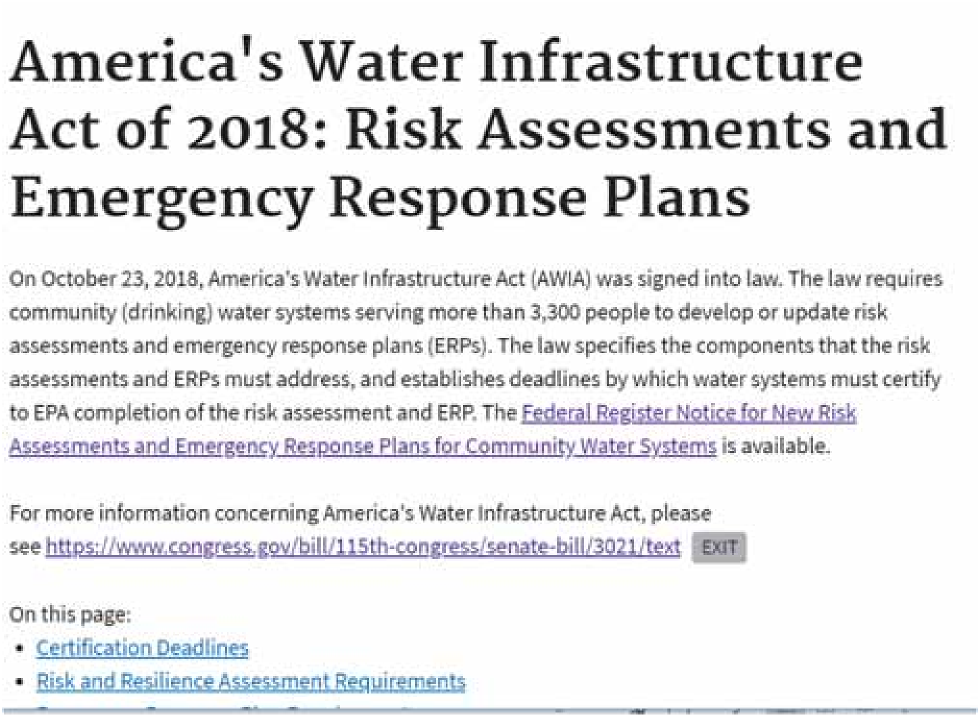
Requirements overview presentation available online now

Detailed in-person and web-accessible full-day training

EPA United States Environmental Protection Agency

Please visit website for updates!

https://www.epa.gov/waterresilience/americas-water-infrastructure-act-2018-risk-assessments-and-emergency-response-plans



America's Water Infrastructure Act of 2018: Risk Assessments and Emergency Response Plans

On October 23, 2018, America's Water Infrastructure Act (AWIA) was signed into law. The law requires community (drinking) water systems serving more than 3,300 people to develop or update risk assessments and emergency response plans (ERPs). The law specifies the components that the risk assessments and ERPs must address, and establishes deadlines by which water systems must certify to EPA completion of the risk assessment and ERP. The Federal Register Notice for New Risk Assessments and Emergency Response Plans for Community Water Systems is available.

For more information concerning America's Water Infrastructure Act, please see https://www.congress.gov/bill/115th-congress/senate-bill/3021/text

On this page:

- Certification Deadlines
- Risk and Resilience Assessment Requirements

United States Environmental Protection Agency

FAQs

1. Can another standard such as PARRE or a state standard be used to comply with the risk assessment requirements?

AWIA does not require the use of any standards, methods or tools for the risk and resilience assessment or emergency response plan. Your utility is responsible for ensuring that the risk and resilience assessment and emergency response plan address all the criteria in AWIA Section 2013(a) and (b), respectively. The U.S. EPA recommends the use of standards, including AWWA J100-10 Risk and Resilience Management of Water and Wastewater Systems, along with the U.S. EPA Vulnerability Self-Assessment Tool and other organizations, to facilitate sound risk and resilience assessments and emergency response plans.

2. How soon can I submit a certification?

Now.

3. Will USEPA still be providing explicit guidance for increased resiliency to these smaller water systems?

(e) Guidance To Small Public Water Systems.—The Administrator shall provide guidance and technical assistance to community water systems serving a population of less than 3,300 persons on how to conduct resilience assessments, prepare emergency response plans, and address threats from malevolent acts and natural hazards that threaten to disrupt the provision of safe drinking water or significantly affect the public health or significantly affect the safety or supply of drinking water provided to communities and individuals.

EPA United States Environmental Protection Agency

FAQs

4. Is there funding available for conducting the risk assessment?

Currently, there is not one stream of funding that is designated specifically to address the new risk assessment requirement. However, the Drinking Water State Revolving Fund program can be used to conduct a risk assessment since it addresses resilience of the system and the risk assessment may yield a project that the utility may want to invest in to improve the overall system resilience. Both parts of the program can be used. Each state will manage this differently. Please check with your state to see if they have set aside funds for this function specifically either with direct contractor or with reimbursements.

5. Who is qualified to certify a risk assessment or emergency response plan?

Any designated utility representative.

6. How are you determining the population sizes for utilities?

U.S. EPA is using the SDWIS database to determine the population size served by each utility and the corresponding deadline.

Contact Information

Kyle St. Clair
Phone: (303) 312-6791
Email: stclair.kyle@epa.gov

Website: www.epa.gov/waterresilience

Join the EPA Water Security Divison mailing list to receive updates and other information

EPA