Cybersecurity 102

Understanding OT Cybersecurity

United States Environmental Protection Agency

Office of Water

About the Speaker

- **Cameron Burden, Cybersecurity Analyst**

- **EPA's Office of Water**
  - **Office of Ground Water and Drinking Water**
  - **Water Infrastructure and Cyber Resilience Division**
  - **Cybersecurity Branch**

- **B.S. Information Technology**
- **CompTIA Security+**

- **Email: Burden.Cameron@epa.gov**

Webinar Logistics and Continuing Education

- Troubleshooting
  - If you have having audio or visual trouble, please exit the webinar and rejoin
  - If you continue to have trouble, please send a private chat to Paige Bateman (GDIT)
- Ways to Interact
  - Submit questions in the chat
  - Respond to poll questions
- Wrap Up and CEUs
  - At the end of the training, please complete the course evaluation
  - Continuing education is tracked by attendance and poll responses

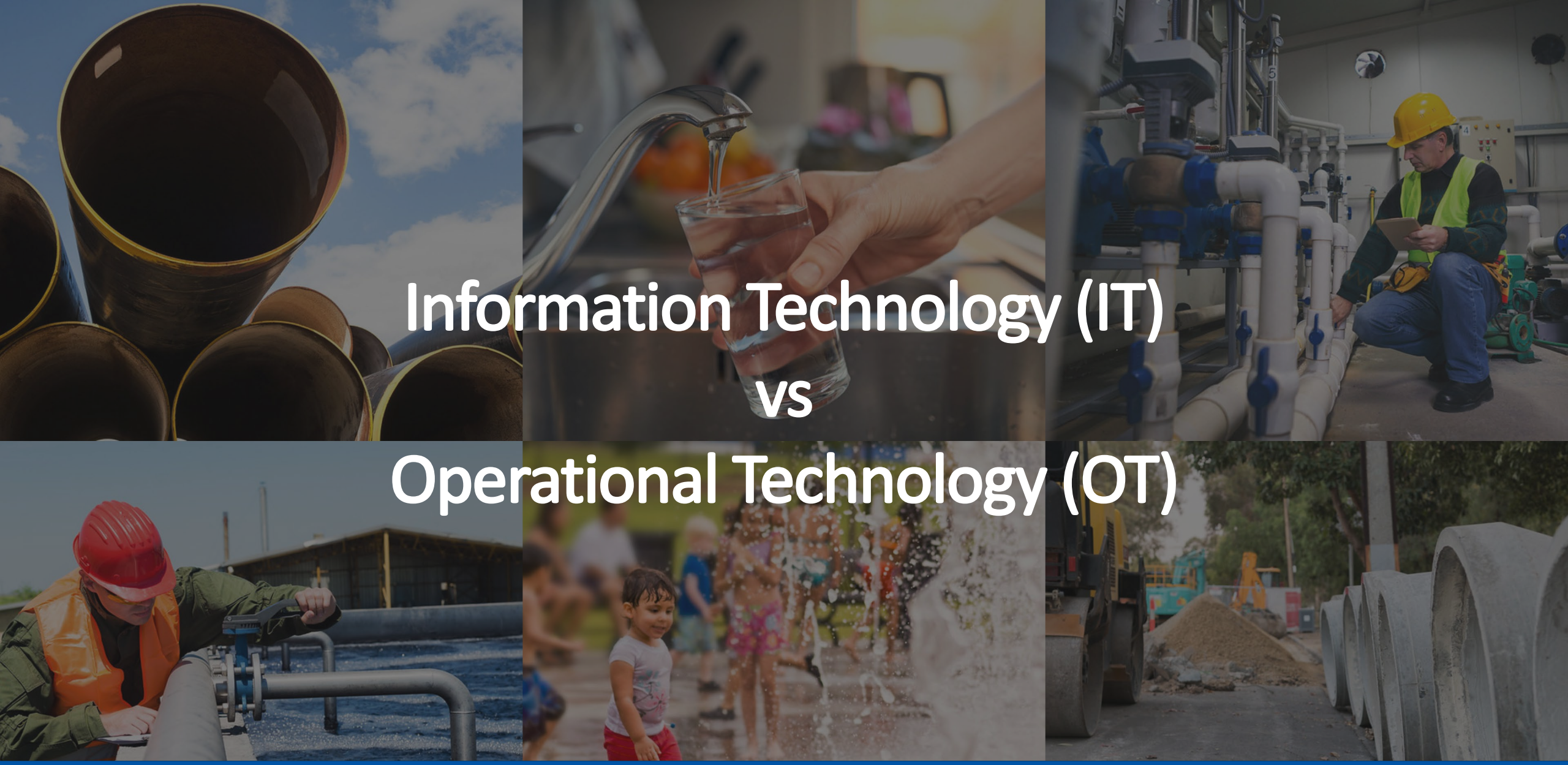
Continuing Education Units

- **You must answer ALL poll questions during this training to receive credit for the CEUs**

- **The final poll question is at the END of the training**

Agenda

- IT vs OT
- Common OT devices/systems
- OT myths
- Common OT Threats
- 5-Minute Break
- Cyber Incidents Impact OT at Water Systems
- Protecting OT systems
- Incident Reporting/Response
- Recovery
- Q&A



Information Technology (IT) vs Operational Technology (OT)

United States Environmental Protection Agency

Poll 3

Office of Water

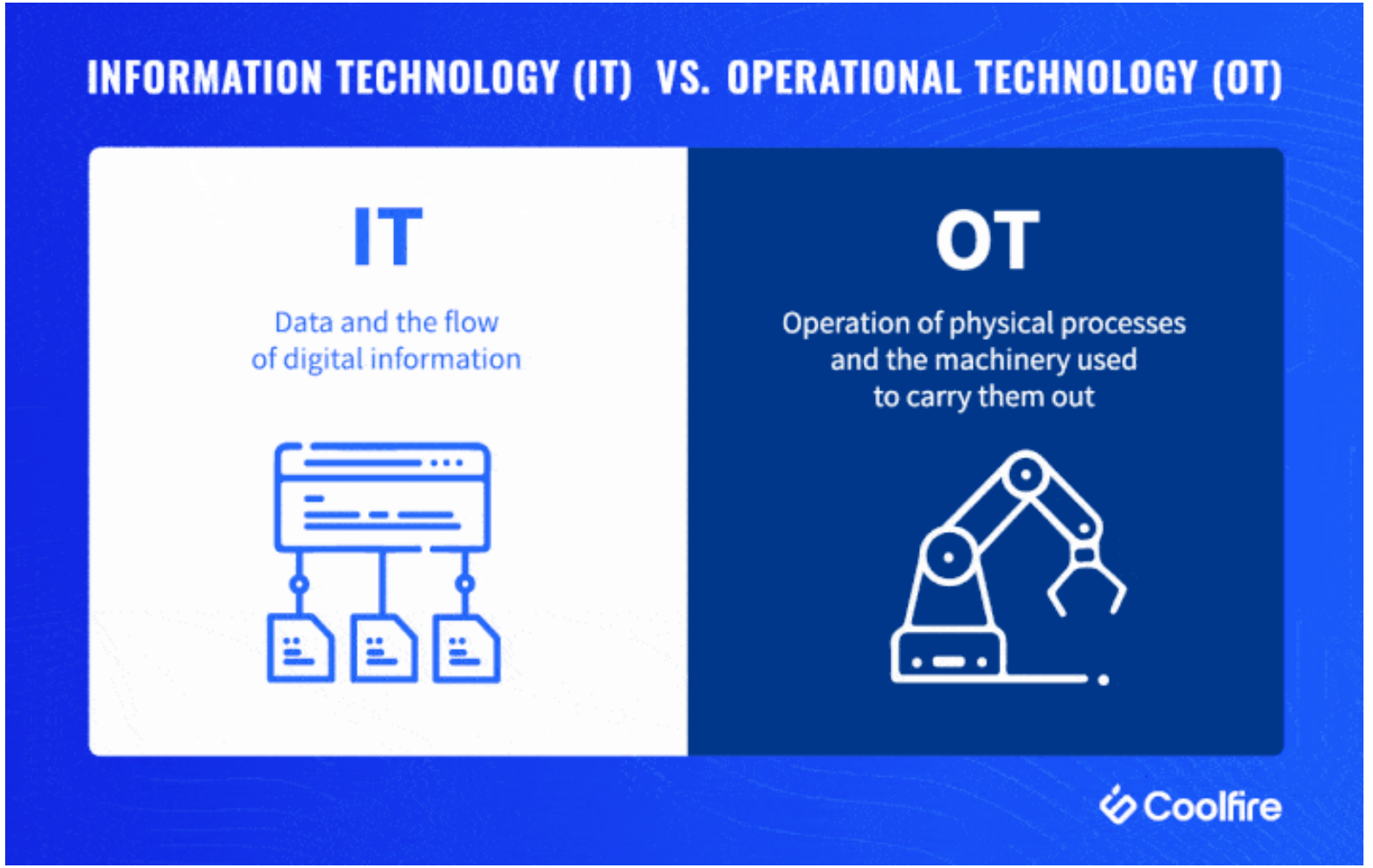
What is Information Technology?

- The study or use of systems (especially computers and telecommunications) for storing, retrieving, and sending information
- The organizations FRONT-END
  - Servers
  - Computers
  - Operating systems
  - Firewalls

What is Operational Technology?

- **Hardware and software that detects or causes a change, through the direct monitoring and/or control of industrial equipment, assets, processes and events**
- **The organizations BACK-END**
  - **Industrial Control Systems (ICS)**
  - **Programmable Logic Controllers (PLC)**
  - **Supervisory control and data acquisition (SCADA) systems**

IT vs OT


INFORMATION TECHNOLOGY (IT) VS. OPERATIONAL TECHNOLOGY (OT)
IT
Data and the flow of digital information
OT
Operation of physical processes and the machinery used to carry them out
Coolfire

Common OT Devices and Systems

United States Environmental Protection Agency

Poll 4

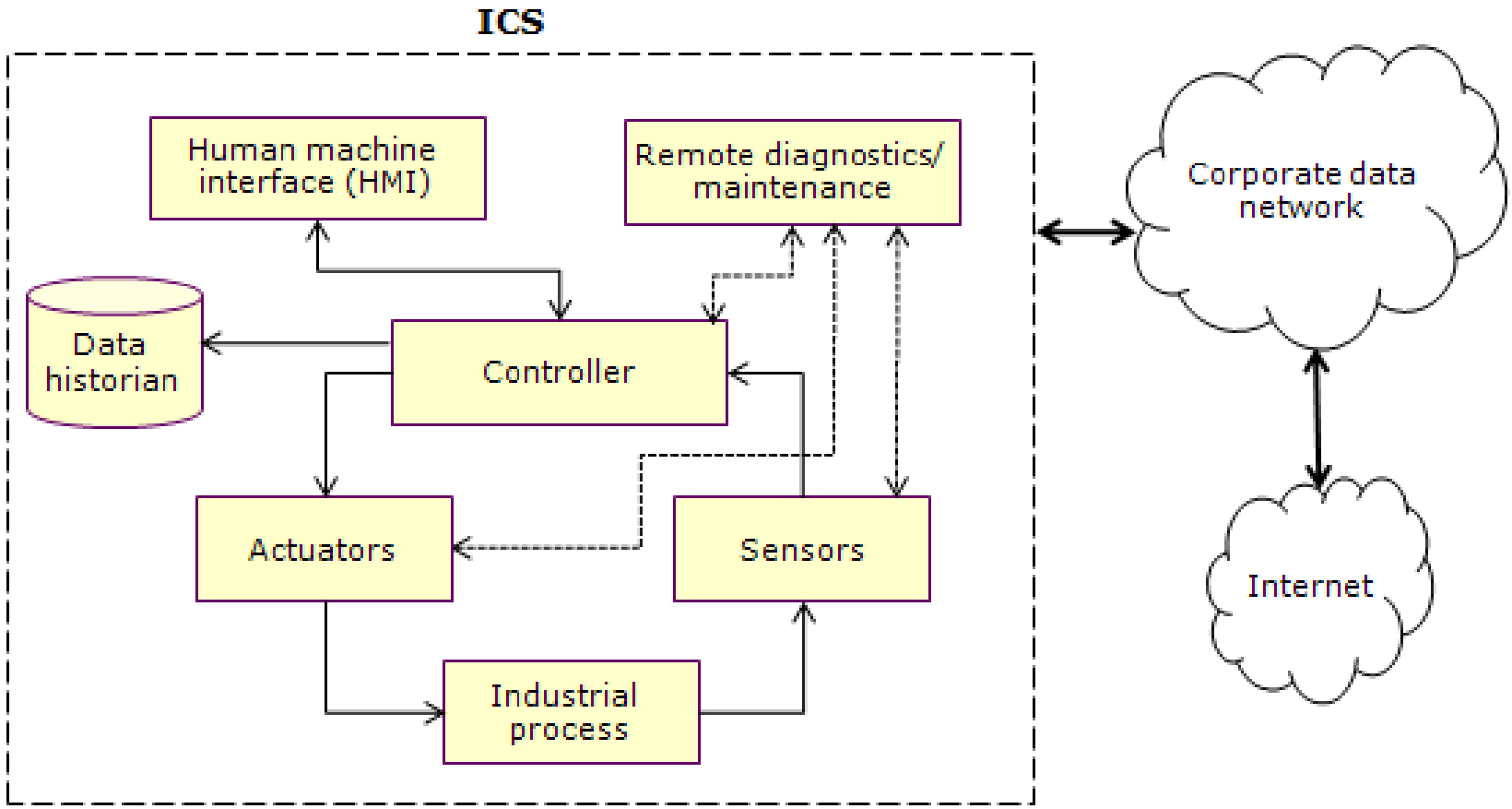
Office of Water

Industrial Control Systems (ICS)

- **A collection of control systems and other hardware that work together to automate or operate industrial processes**

- **The goal of ICSs is to make daily operations more efficient and autonomous, with minimal input from human workers**

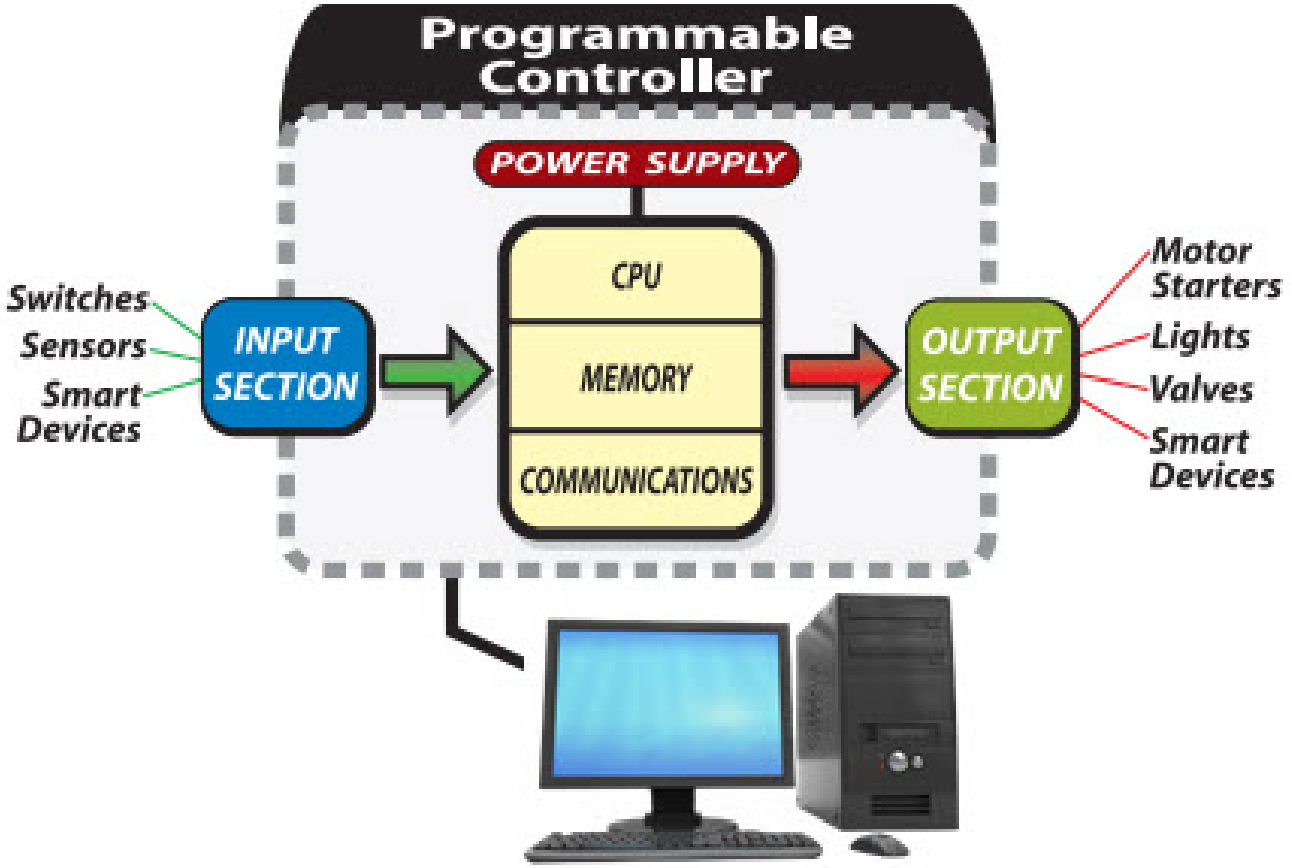
Industrial Control Systems (ICS)



Programmable Logic Controller (PLC)

- **An industrial-grade digital computer designed to perform control functions commonly used for commercial and industrial applications**

Programmable Logic Controller (PLC)



What are some everyday Items that have PLCs?

- **Traffic Lights**
- **Elevators**
- **Automatic doors**
- **Automatic Car Wash**

Supervisory Control and Data Acquisition (SCADA)

- A computerized system that uses software and hardware to monitor and control industrial processes and equipment
- Allows operator to supervise the equipment and control them remotely
- Examines, collects, and processes data in real time

SCADA vs PLC – What's the difference?

SCADA vs ICS Security – What's the difference?

SCADA Security	ICS Security
Centers on real-time data & control	Focus on industrial machinery control
Involves risk & compliance management	Ensures data integrity & machinery safety
Essential for national security	Links to physical safety
Focuses on public safety & service continuity	Utilizes preventative & responsive defenses

Remote Terminal Units (RTUs)

- **A microprocessor-based industrial device that collects and processes data from sensors, actuators, and other devices at remote sites**

How are RTUs used in commercial and industrial systems?

- **Water and wastewater treatment**

  Monitor and control processes such as pumping, filtration, and disinfection to help maintain water quality, prevent equipment failures, and ensure compliance with environmental regulations

- **Intrusion alarms**

  Monitor whether doors, windows, and other access points are open or closed. More advanced systems can also control door access, allowing you to determine who, when, and which door can be entered

Distributed Control System (DCS)

- A computerized system that uses control loops across a factory, machine, or control area to automate industrial equipment
- Helps to manage and control water resources through:
  - Treatment
  - Distribution
  - Disposal

How are DCSs used in commercial and industrial systems?

- **Water treatment**

  Responsible for controlling and monitoring processes, such as coagulation, flocculation, sedimentation, filtration, and disinfection. The goal of using these systems is the consistent production of high-quality potable water

- **Wastewater treatment**

  Employed to control and monitor primary settling, biological treatment, secondary settling, and disinfection. Enables the plants to minimize energy consumption, reduce the generation of waste products, and ensure compliance with effluent discharge regulations.

Common OT Myths

United States Environmental Protection Agency

Poll 5

Office of Water

Air-gapping the system is 100% safe

- False, while air-gapping works, it is not 100% effective
- Systems are still susceptible to insider threats
  - Employees
  - Vendors
  - Contractors
  - Custodians
- These threats can be either intentional or accidental. If they have access, then the threat exists

OT systems are always secure

- **Not true! It would be nice if all OT systems were 100% secure by default; unfortunately, that's just not the case**

- **OT systems often have outdated legacy components and were often designed with reliability and functionality in mind, rather than security**

- **OT systems were designed to function exactly how the utility intended and not to detect any misuse**

OT systems don’t need regular updates and patches.

- **The exact opposite is true – regular updates and patches are critical for closing vulnerabilities.**
- **But the challenge here lies in implementing updates without disrupting crucial industrial processes. So, it’s vital to plan carefully to prevent any interruptions from happening.**

Incident response is not essential for OT environments

- **What's a surefire way to let a cyberattack on industrial processes get out of hand? Not having incident response to quickly detect and respond to a threat.**

- **So having incident response is crucial in OT environments, because the quicker your system can identify and react to a threat, the less damage a cyberattack can cause.**

Common OT Threats

United States Environmental Protection Agency

Poll 6

Office of Water

Supply Chain Threats

- **Vulnerabilities can exist before the equipment is even installed at your utility**
  - **Third-party vulnerabilities: Third-party vendors and partners can be a primary source of cyber risk. Cyber attackers can gain access through open-source repositories, public source code, and login credentials**
  - **Software vulnerabilities: Software vulnerabilities can also be a weakness**
  - **Vendor data storage: How vendor data is stored can also be a vulnerability**

Phishing

- **Form of social engineering and a scam where attackers deceive people into revealing sensitive information or installing malware such as viruses, worms, adware, or ransomware.**
  - **Reveal sensitive information – Pump locations, chemical information**
  - **Install Malware – downloading fake updates**
    - **Can happen on IT network and migrate to OT network**

Insider Threats

- **What is an insider?**
  - **An insider is any person who has or had authorized access to or knowledge of an organization's resources, including personnel, facilities, information, equipment, networks, and systems.**
- **Examples**
  - **Person with:**
    - **Access to sensitive information (Chemical values, Room with SCADA Systems)**
    - **A badge or access device (SCADA contractor, vendor, custodian)**
    - **A computer from the utility or network access to the utility**
    - **Knowledge about the organization's fundamentals (distribution pricing, chemical costs, and organizational structure)**
    - **Knowledge of organizations business strategy and goals**

Insider Threats cont.

- What is an insider threat?
  - The potential for an insider to use their authorized access or understanding of an organization to harm that organization
- Examples
  - Shadow IT
    - Charging your phone/tablet
  - Terrorism
  - Unauthorized disclosure of information
  - Corruption
  - Sabotage
  - Workplace violence
  - Intentional or unintentional loss of degredation of resources or capabilities

Physical tampering

- **The intentional and unauthorized alteration of a system, device, or process**
  - **Turning off pumps**
  - **Changing chemical levels**
  - **Adjusting sensors**
  - **Turning off cameras**

Misconfigured Devices

- **Occurs when system or application configuration settings are missing or are erroneously implemented, allowing unauthorized access**
  - **Document the configuration**
  - **Update the configurations as equipment is installed, replaced, retired**
  - **Update inventory for devices after installation/configuration**

Ransomware

- **Prevents users from accessing their system or personal files and demands ransom payment in order to regain access**
- **Comes from social engineering or “tricking users”**
- **Ransom payments are demanded as cryptocurrency or credit card payments**

United States Environmental Protection Agency

Office of Water

Cyber Incidents Impact OT at Water Systems

United States Environmental Protection Agency

Office of Water

Recent Headlines

CYBERCRIME

Former Contractor Employee Charged for Hacking California Water Treatment Facility

Former contractor employee charged with hacking for accessing the systems of a water treatment facility in California to delete critical software.

By Eduard Kovacs
July 7, 2023

A 53-year-old man from Tracy, California, has been charged for allegedly hacking into the systems of a water treatment facility in an attempt to delete critical software.

The suspect, Rambler Gallo, has been charged with "transmitting a program, information, code, and command to cause damage to a protected computer", but this is a case of unauthorized access rather than actual hacking.

TRENDING

1. Google Warns of Chrome Browser Zero-Day Being Exploited
2. List Containing Millions of Credentials Distributed on Hacking Forum, but Passwords Old
3. Remotely Exploitable 'PixieFail' Flaws Found in Tianocore EDK II PXE Implementation
4. Vulnerabilities Expose PAX Payment Terminals to Hacking
5. Mr. Cooper Data Breach Impacts 14.7 Million Individuals
6. GitLab Patches Critical Password Reset Vulnerability
7. AI Data Exposed to 'LeftoverLocals' Attack via Vulnerable AMD, Apple, Qualcomm GPUs
8. Oleria Secures $33M Series A Investment

Daily Briefing Newsletter
Subscribe to the SecurityWeek

CNN politics SCOTUS Congress Facts First 2024 Elections

Federal investigators confirm multiple US water utilities hit by hackers

By Sean Lyngaas, CNN
3 minute read · Updated 10:48 PM EST, Fri December 1, 2023

Chrissy Suttles/Beaver County Tr/USA Today Network

Municipal Water Authority of Aliquippa tower in Aliquippa

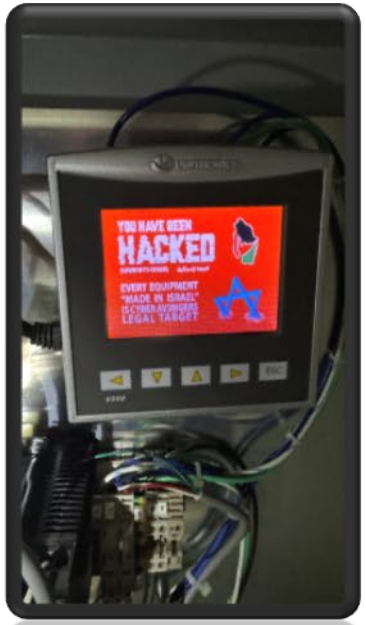
Former Contractor Employee

- A contractor was able to install remote access software onto their personal computer to gain access to Water Treatment Facility.
- After contractor resigned from their company, they remotely accessed Water Treatment Facility and was able to uninstall the software responsible for protecting the water treatment system.
- Vulnerability
  - Remote Access
- Mitigation
  - Multi-Factor Authentication
  - Role-Based Access Control

Multiple US Water Utilities Hit By CyberAv3ngers

- Threat actors were able to hack into Programmable Logic Controllers (PLCs) and display an image
- Vulnerability
  - Default Passwords
- Mitigation
  - Change Default Passwords

Exploitation of PLCs at Water and Wastewater Utilities By Iranian CyberAv3ngers



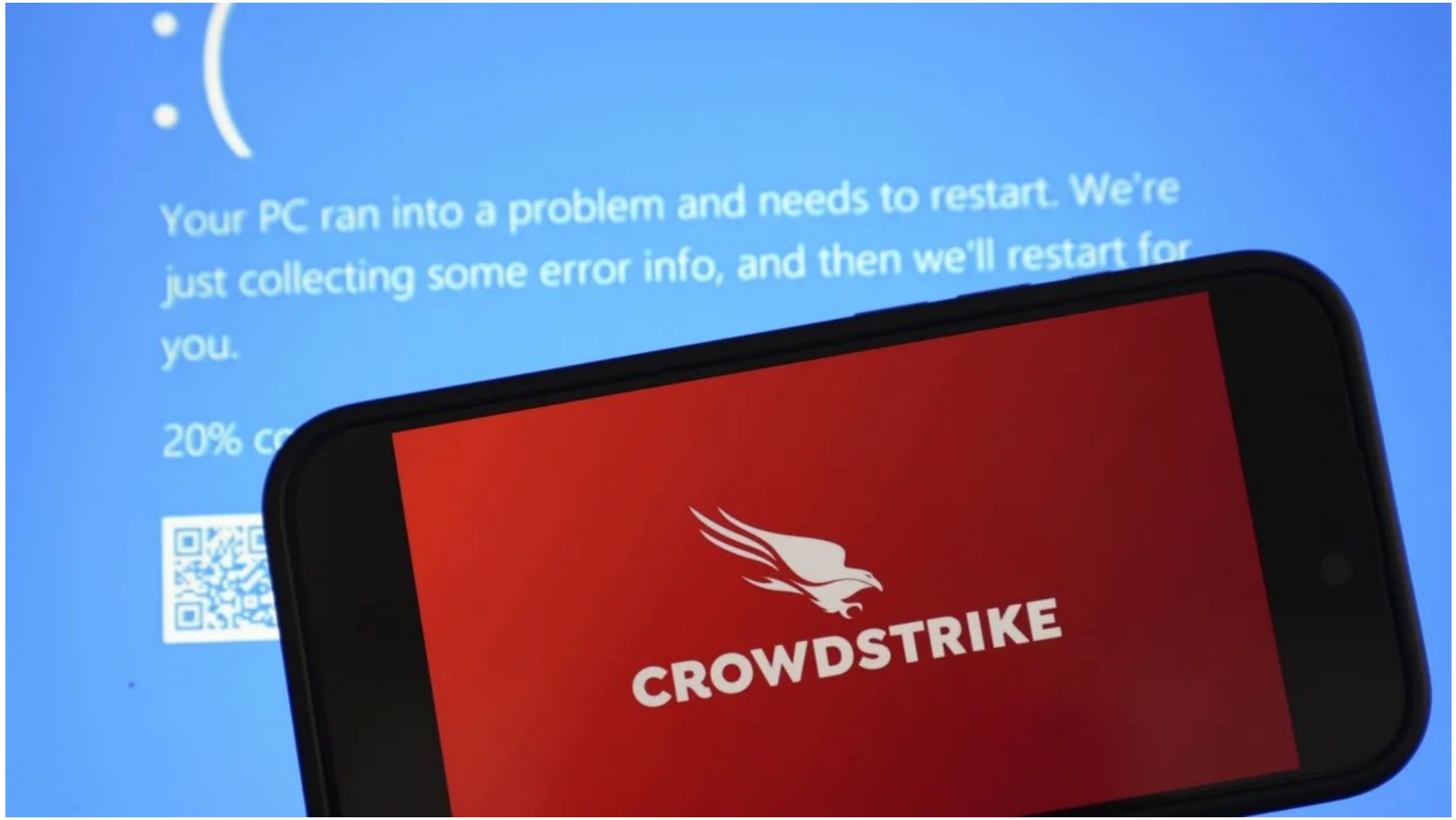
CYBERSECURITY

Bad Password May Have Led to Pennsylvania Water System Hack

Opportunistic Hacktivists Target PLCs at US Water Facility

Team82 / November 30th, 2023

CrowdStrike



CrowdStrike

- **An update containing "incorrect code" affected systems running Windows 10 or later**
  - **Caused systems to crash, leading to multiple services unavailable**
- **Impacted utility SCADA systems and various utility computers taking them offline**
  - **Utilities were able to address issue in a timely manner and maintain operations**

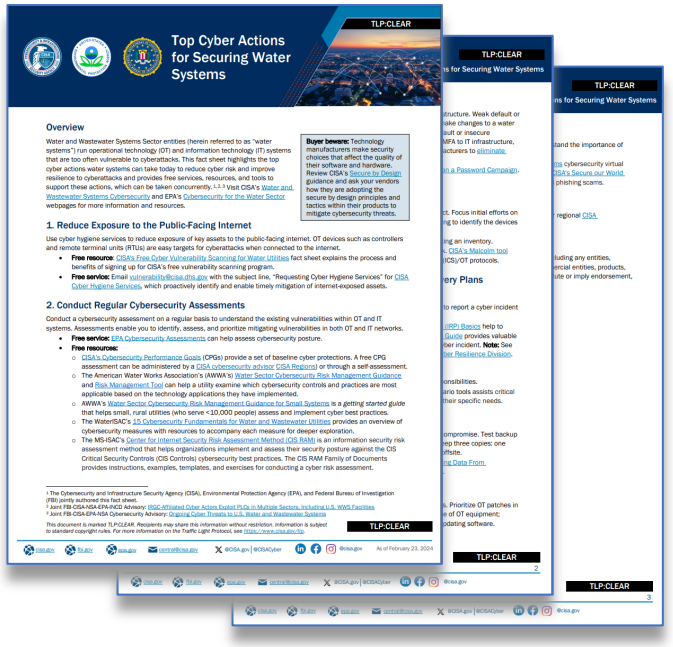
Protecting OT Systems

United States Environmental Protection Agency

Office of Water

Top Cyber Actions for Securing Water Systems OT

1. Reduce exposure to the public-facing internet
2. Conduct regular cybersecurity assessments
3. Change default passwords
4. Conduct an inventory of OT/IT assets
5. Develop and exercise cybersecurity incident response and recovery plans
6. Back up OT/IT systems
7. Reduce exposure to vulnerabilities
8. Conduct cybersecurity awareness training



1. Reduce Exposure to the Public-Facing Internet

- **Without cybersecurity controls, unauthorized users can exploit exposed Human Machine Interfaces (HMIs) in Water and Wastewater Systems to:**
  - **View the contents of the HMI (including the graphical user interface, distribution system maps, event logs, and security settings).**
  - **Make unauthorized changes and disrupt water and/or wastewater treatment process.**
- **OT devices, such as controllers and remote terminal units (RTUs), are easy targets for cyberattacks when connected to the internet.**
- **Use cyber hygiene services to reduce exposure of key assets to the public-facing internet.**

Free Resources

- **CISA Cyber Vulnerability Scanning for Water Utilities**
- **EPA Proactive Vulnerability Identification**

CISA's Free Cyber Vulnerability Scanning for Water Utilities

- **Benefits of this service include:**
  - **Identifying internet-accessible assets.**
  - **Identifying vulnerabilities in internet-connected assets.**
  - **Weekly reports on scanning status and recommended mitigations.**
  - **Ongoing detection and reporting with continuous scanning for new vulnerabilities.**

Email vulnerability@cisa.dhs.gov with the subject line "Requesting Vulnerability Scanning Services" to request this service.

Figure 1: Sample Page in Weekly Report

EPA's Proactive Vulnerability Identification and Follow-up Program

Objective: Identify internet-exposed Operational Technology (OT) devices at drinking water and wastewater systems, perform follow-ups to notify utilities of their vulnerability, and provide mitigation resources.

Goal: Identify and mitigate 500 vulnerabilities at drinking water and wastewater systems by the end of FY25.

Impact: Decrease cybersecurity risk at drinking water and wastewater systems

2. Conduct Regular Cybersecurity Assessments

- **Assessments enable utilities to identify, assess, and prioritize mitigating vulnerabilities in both OT and IT networks.**

Free Resources

- **EPA Cybersecurity Assessments**
- **CISA Cybersecurity Performance Goals (CPGs)**
- **AWWA Water Sector Cybersecurity Risk Management Guidance and Risk Management Tool**
- **AWWA Water Sector Cybersecurity Risk Management Guidance for Small Systems**
- **WaterISAC 15 Cybersecurity Fundamentals for Water and Wastewater Utilities**
- **MS-ISAC's Center for Internet Security Risk Assessment Method (CIS RAM)**

EPA's Water Sector Cybersecurity Evaluation Program

- **Free third-party cybersecurity assessments provided by EPA for Water and Wastewater Systems to evaluate cybersecurity practices.**
- **The program uses the EPA Cybersecurity Checklist which is derived from CISA's Cross-Sector Cybersecurity Performance Goals (CPGs).**
- **Utilities receive an Assessment Report and a Risk Mitigation Plan template.**

Scan this QR Code to Register for a Free Cybersecurity Assessment

EPA's Water Cybersecurity Assessment Tool (WCAT)

- **Cybersecurity Self-Assessment Tool to evaluate cybersecurity practices at water and wastewater systems.**

- **The Tool Features:**
  - **Assessment Workbook**
  - **Assessment Report**
  - **Risk Mitigation Plan**

EPA Water Cybersecurity Assessment Tool (WCAT)

EPA

EPA Cybersecurity Checklist for Drinking Water and Wastewater Systems

What is the purpose of this checklist assessment?

This assessment tool uses the EPA Cybersecurity Checklist for Drinking Water and Wastewater Systems. The purpose of this checklist assessment is to provide a method to evaluate cybersecurity at a water or wastewater system (WWS). When a WWS uses operational technology (OT)[1], such as an industrial control system (ICS)[2], as part of its equipment or operation, then the adequacy of the cybersecurity of that OT for producing and distributing safe water should be evaluated. A commonly used OT at a WWS is a Supervisory Control and Data Acquisition (SCADA) system.

The checklist assessment questions and recommended actions to address the questions are extracted directly from the Cybersecurity and Infrastructure Agency (CISA) Cross-Sector Cybersecurity Performance Goals. In this checklist assessment, the Cybersecurity Performance Goals are written in a more simplified question format to facilitate their use in evaluating a WWS.

Link to Cybersecurity and Infrastructure Agency (CISA) Cross-Sector Cybersecurity Performance Goals below:
https://www.cisa.gov/cpg

Alternatives to the cybersecurity evaluation checklist include those from CISA[3], NIST[4], AWWA[5], ISO[6], and ISA/IEC[7].

How should this checklist assessment be used?

The checklist assessment questions are intended to identify gaps or potential vulnerabilities in current cybersecurity practices. WWSs are encouraged to use the resources and technical assistance described in EPA guidance (link below) to address these gaps and reduce the risk that a cyberattack may

3. Change Default Passwords Immediately

- **Require unique, strong, and complex passwords for all water systems, including connected infrastructure.**
- **Change default or insecure passwords.**
- **Implement multifactor authentication (MFA).**
- **Focus on deploying MFA to IT infrastructure, such as email, to make it difficult for threat actors to access OT systems.**
- **Consider asking manufacturers to eliminate default passwords.**

Free Resources

- **CISA Secure our World: Use Strong Passwords and More than a Password Campaign**
- **CISA Cyber Guidance for Small Businesses**

4. Conduct an Inventory of IT/OT Assets

- **Create an inventory of software and hardware assets to help understand what you need to protect.**
- **Focus initial efforts on internet-connected devices and devices where manual operations are not possible.**
- **Use monitoring to identify the devices communicating on your network.**

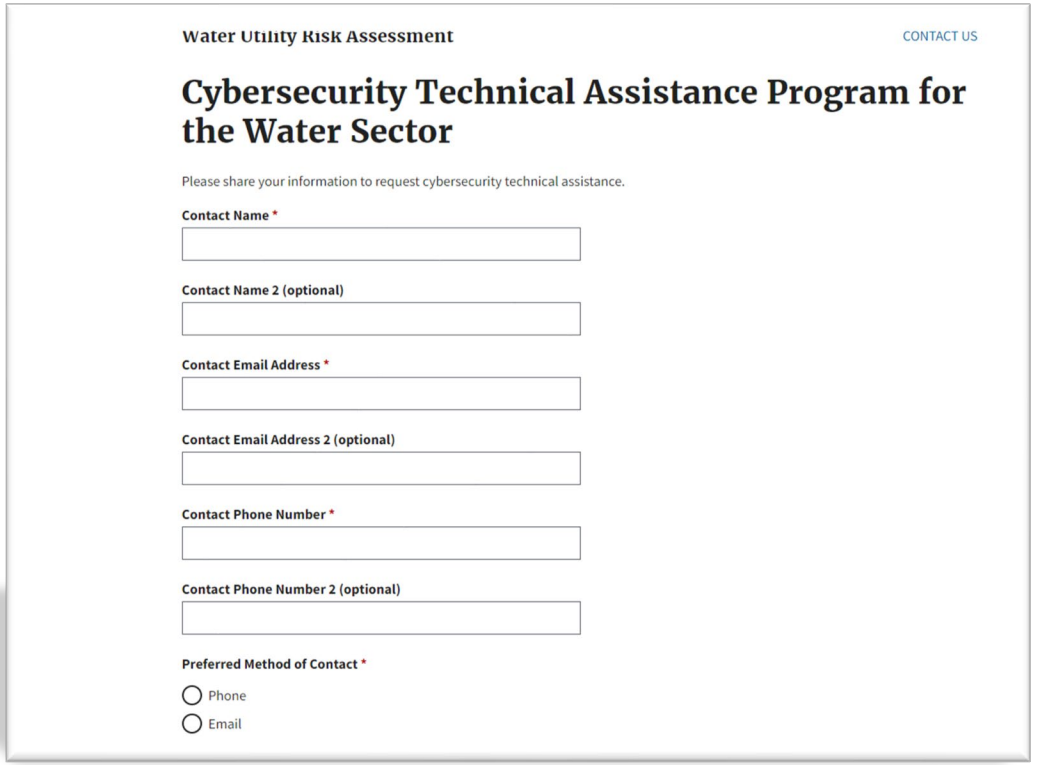
Free Resources

- **EPA Cybersecurity Technical Assistance Program**
- **CISA Malcolm (network traffic analysis tool)**

Cybersecurity Technical Assistance Program for the Water Sector (Cybersecurity Help Desk)

- **EPA provides direct cybersecurity technical assistance for members of the Water Sector, including:**
  - **Utilities**
  - **Primacy Agencies**
  - **Technical Assistance Providers**
  - **Others**

- **Cybersecurity Subject Matter Experts respond to requests for technical assistance by phone or email within two business days.**



https://www.epa.gov/waterresilience/forms/cybersecurity-technical-assistance-program-water-sector

CISA Malcolm

- Free network traffic analysis tool
- Why use it?
  - Network Visibility
  - Threat Detection & Hunting
  - User-Friendly Visualization
  - Scalability
  - Compliance

5. Develop and Exercise Cybersecurity Incident Response and Recovery Plans

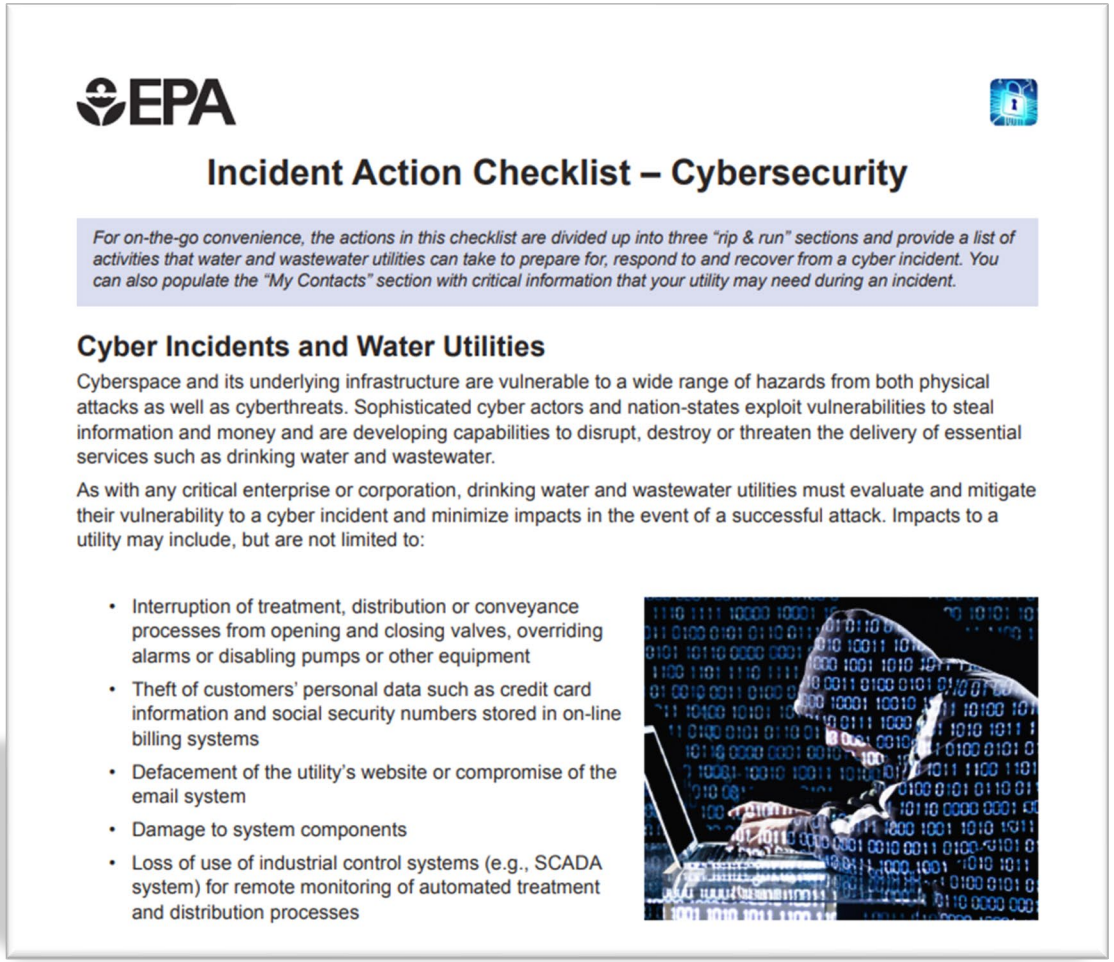
- **Understand incident response actions, roles, and responsibilities, as well as who to contact and how to report a cyber incident before one occurs to ensure readiness against potential targeting.**
- **Test/exercise your incident response plan annually to ensure all operators are familiar with roles and responsibilities.**

Free Resources

- **EPA Cybersecurity Incident Action Checklist**
- **CISA Incident Response Plan (IRP) Basics**
- **CISA-FBI-EPA Water Incident Response Guide**
- **CISA Tabletop Exercise Package (CTEP)**
- **EPA Tabletop Exercise (TTX) Tool for Drinking Water and Wastewater Utilities**

EPA's Water Sector Incident Action Checklist - Cybersecurity

- **An actionable list of activities you can take during all phases of a cyber incident, including:**
  - **Preparation**
  - **Response**
  - **Recovery**
- **This Checklist can be included in your Incident Response Plans for quick access.**



EPA

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

6. Backup OT/IT Systems

- **Regularly backup OT/IT systems so you can recover to a known and safe state in the event of a compromise.**
- **Test backup procedures and isolate backups from network connections.**
- **Implement the NIST 3-2-1 rule:**
  - **3) Keep three copies: one primary and two backups**
  - **2) Keep the backups on two different media types**
  - **1) Store one copy offsite**
- **Free Resource**
  - **CISA Cyber Essentials Toolkit Chapter 5: Your Data - Make Backups and Avoid the Loss of Information Critical to Operations**
  - **NIST Protecting Data From Ransomware and Other Data Loss Events**

7. Reduce Exposure to Vulnerabilities

- **Mitigate known vulnerabilities.**
- **Keep all systems up to date with patches and security updates.**
- **Prioritize OT patches in accordance with CISA's Known Exploited Vulnerabilities (KEV) catalog during scheduled downtime of OT equipment; prioritize patches in IT, as applicable.**

Free Resources

- **CISA Secure our World (provides guidance on updating software)**
- **CISA KEV catalog**

8. Conduct Cybersecurity Awareness Training

- **Conduct cybersecurity awareness training at least annually to help all employees understand the importance of cybersecurity and how to prevent and respond to cyberattacks.**

Free Resources

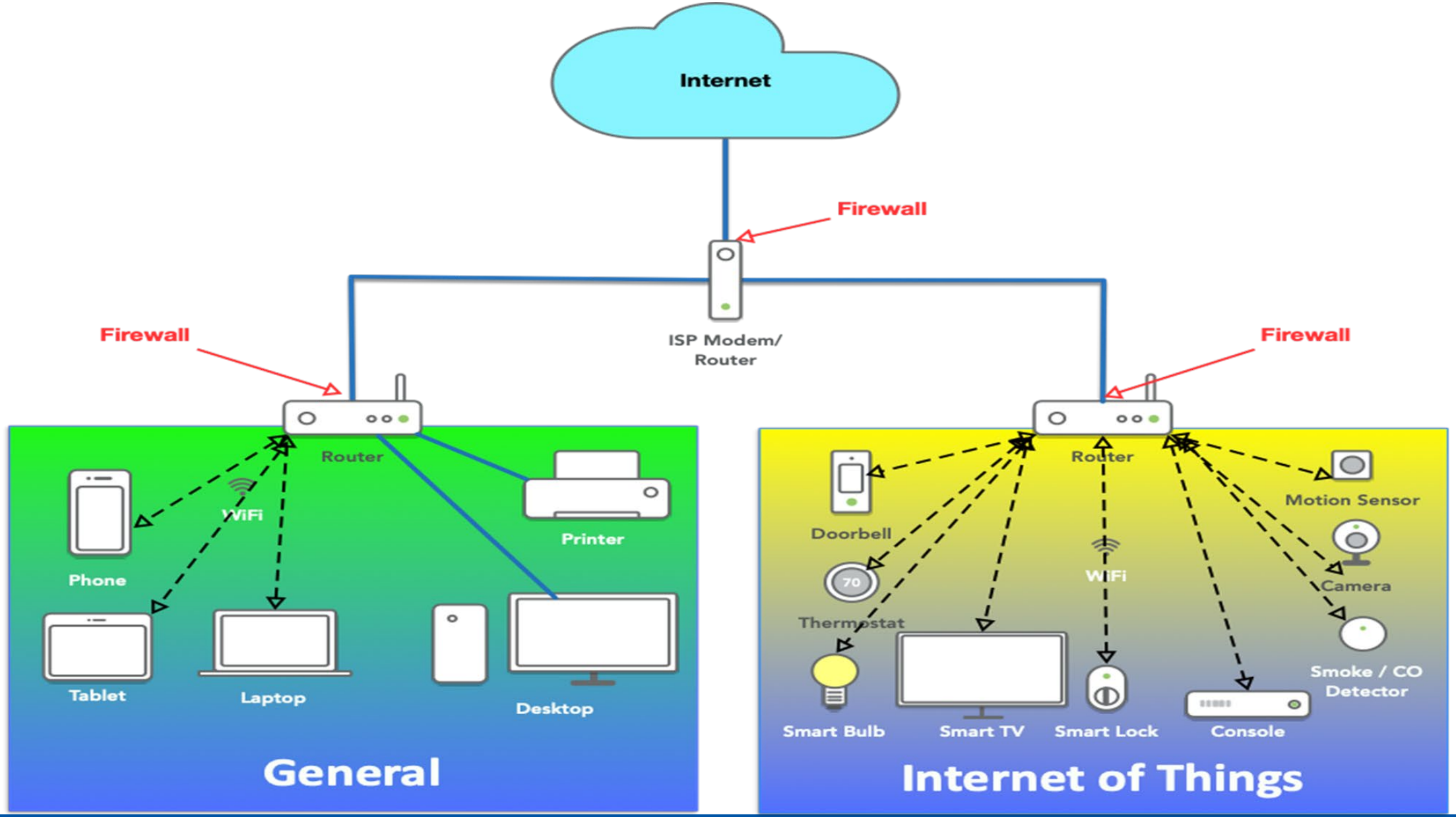
- **EPA Cybersecurity Training**
- **CISA Industrial Control Systems Training**
- **CISA Secure our World Campaign (phishing training)**

Cybersecurity Training for the Water Sector

- **EPA is committed to providing cybersecurity training for the water sector on an ongoing and reoccurring basis.**
- **Trainings include cybersecurity basics for water systems, how to conduct a cybersecurity risk assessment, tabletop exercises, and more.**
- **Visit www.epa.gov/waterresilience/cybersecurity-training to view upcoming and recorded training.**
- **Contact watercyberta@epa.gov to request a cybersecurity training or tabletop exercise.**

Network Segmentation

- **Dividing a network into smaller, more manageable segments, which each act as their own network**
- **Improves performance and security**


Internet
Firewall
ISP Modem/
Router
Firewall
Firewall
Router
Phone
WiFi
Printer
Tablet
Laptop
Desktop
General
Router
Doorbell
Motion Sensor
70
Thermostat
WiFi
Camera
Smoke / CO
Detector
Smart Bulb
Smart TV
Smart Lock
Console
Internet of Things

Incident Reporting & Response

United States Environmental Protection Agency

Poll 9

Office of Water

Incident Response Plan

An incident response plan is a document with detailed procedures on how to respond to a cyber incident which can help minimize response and recovery times.

- **Maintain and update IRP after incidents**
  - Lessons learned
  - Process/Contact changes

- **Conduct Tabletop Exercises (TTX) to improve incident response**

Steps in Cybersecurity Incident Response & Handling (R&H)

- Preparation
- Identification
- Containment
- Investigation and forensics
- Communication and Reporting
- Recovery
- Lessons Learned/After Action Report

Incident (R&H) – Preparation

- Developing the processes, procedures, and resources required for efficient event response of a cyber incident
  - Creating a Cyber Incident Response Plan (IRP)
    - Will be different from natural disaster plans
  - Defining roles and duties
  - Identifying important employees
    - IT Vendors, OT Vendors, Cybersecurity Insurance
  - Creating communication routes

Incident (R&H) – Identification

- Next, identify a security event through intrusion detection systems, log monitoring, network monitoring, or user reporting**
- When a cyber event is discovered, the cyber incident response team should investigate it and identify the nature and severity of the issue**

- Please note there should be a different team for a natural disaster vs a cyber incident

** = This step is more for the IT personnel/vendor

Incident (R&H) – Containment

- Once the incident has been identified and confirmed, the emphasis changes to confining the issue to avoid future harm or unwanted access
  - Isolating and stopping impacted systems (segmentation)**
  - Taking other appropriate measures to limit the impact (manual mode)**

- You can implement certain mitigation strategies to minimize the immediate potential harm caused by the incident

** = This step is more for the IT personnel/vendor

Incident (R&H) – Investigation

- Conduct a full investigation to determine the cause, scope, and extent of the occurrence
- This includes:
  - gathering evidence
  - analyzing logs**
  - determining the access point and vulnerabilities exploited**
- The purpose is to collect data that will help prevent such situations in the future

**= This step is more for the IT personnel/vendor

Incident (R&H) – Communication and Reporting

- **Effective communication is critical throughout the incident response process. Management, IT/OT teams, legal counsel, and, if required, law enforcement authorities should all receive regular information**

- **Write a clear and simple report detailing:**
  - **The occurrence**
  - **Actions done**
  - **Lessons learned**

Cybersecurity Incident Reporting

- **Why is incident reporting important?**
  - **Could jeopardize drinking water and wastewater utilities by:**
    - **Exposure of private customer/employee information**
    - **Changing chemical levels in water treatment processes**
    - **Denying access to critical systems**

- **The attacker is a criminal, and reporting an incident allows individuals to look out for suspicious activity and enables them to take steps to protect themselves**

Cyber Incident Reporting Process Factsheet

- **Printable factsheet developed by EPA to help provide guidance on how to respond and report a cyber incident.**
- **Provides information such as what and when to report to the Federal Government**

EPA

CYBER INCIDENT REPORTING PROCESS

WHY IS IT IMPORTANT TO REPORT CYBER INCIDENTS?

A cyber incident could jeopardize drinking water and waste water utilities by allowing access to private customer/employee information, changing chemical levels in water treatment processes, or denying access to critical systems. Cyber incidents resulting in disruptions of operational processes are of particular concern to the Federal Government. The attacker is a criminal, and reporting an incident allows individuals to look out for suspicious activity and enables them to take steps to protect themselves.

WHERE TO REPORT:

REPORT TO THE FBI FOR THREAT RESPONSE

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. The FBI will conduct the investigation.

OR

REPORT TO CISA FOR ASSET RESPONSE

Submit a computer security incident form to the Cybersecurity and Infrastructure Security Agency (CISA) Incident Reporting System at www.us-cert.cisa.gov/forms/report. CISA can be contacted by phone at 888-282-0870 and by email at Central@cisa.gov. CISA will provide technical assets and assistance to mitigate vulnerabilities and reduce the impact of the incident.

OR

CONTACT EPA FOR CENTRALIZED RESPONSE

Please reach out to the U.S. Environmental Protection Agency (EPA) Water Infrastructure and Cyber Resilience Division (WICRD) at WICRD-outreach@epa.gov. 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.

WHEN TO REPORT TO THE FEDERAL GOVERNMENT

Utilities are encouraged to report all cyber incidents when there is any:

- Loss of data, system availability, or control of systems;
- Impact to any number of victims;
- Detection of unauthorized access to, or malicious software present on, critical information technology systems;
- Affected critical infrastructure or core government functions; or
- Impact to national security, economic security, or public health and safety.

WHAT TO REPORT TO THE FEDERAL GOVERNMENT

A cyber incident may be reported at various stages, even when complete information may not be available. Helpful information could include:

- Who you are,
- Who experienced the incident,
- What sort of incident occurred,
- Details of incident impact,
- How and when the incident was initially detected,
- What response actions have already been taken, and
- Who has been notified.

Incident (R&H) – Recovery

- After the event has been controlled and investigated, focus your attention on restoring regular operations
  - Remove any suspicious or malicious presence**
  - Rebuild or restore affected systems (data backups)**
  - Validate their integrity**

- The incident response team along with IT/OT staff is responsible for implementing necessary security patches, updates, or changes to prevent similar or identical incidents from occurring

**= This step is more for the IT personnel/vendor

Incident (R&H) – Lessons Learned

- The final step entails reviewing the occurrence and drawing useful conclusions to enhance security procedures
  - End User Training
  - Implement Firewalls**
  - Develop/Update IRP
  - Communicate Findings (internal/external)

- Organizations may put proactive steps in place to strengthen their defenses, improve incident response skills, and defend against similar occurrences in the future by identifying vulnerabilities, flaws, and gaps in the current systems and networks

**= This step is more for the IT personnel/vendor

Recovery

United States Environmental Protection Agency

Office of Water

Manual Mode

- How long can your utility handle Manual Operations?
- What systems/process are required for manual operations?
- What training is needed for operators to successfully do manual operations?
- How often does training need to be recertified?
- What equipment needs to be monitored?
  - Where is it located?
- What data need to be collected during this process? If so, how?
  - How is collected data protected?

Manual Mode

- **Things to consider:**
  - **Lack of Quality Control**
  - **Time Delays**
  - **Time lost in retrieving/recording data**
  - **Inefficient teamwork**
  - **Redundant efforts**

Wrap-Up

United States Environmental Protection Agency

Office of Water

Recap

- IT vs OT
  - The differences between both
- Common OT devices/systems
  - Identified common devices and how they are used in everyday life
- OT myths
  - What is real and what is not
- Common OT Threats
  - Everyday Incidents

Recap

- Protecting OT systems
  - Simple changes go a long way
- Incident Reporting/Response
  - What to do when things go wrong
- Recovery
  - Manual mode

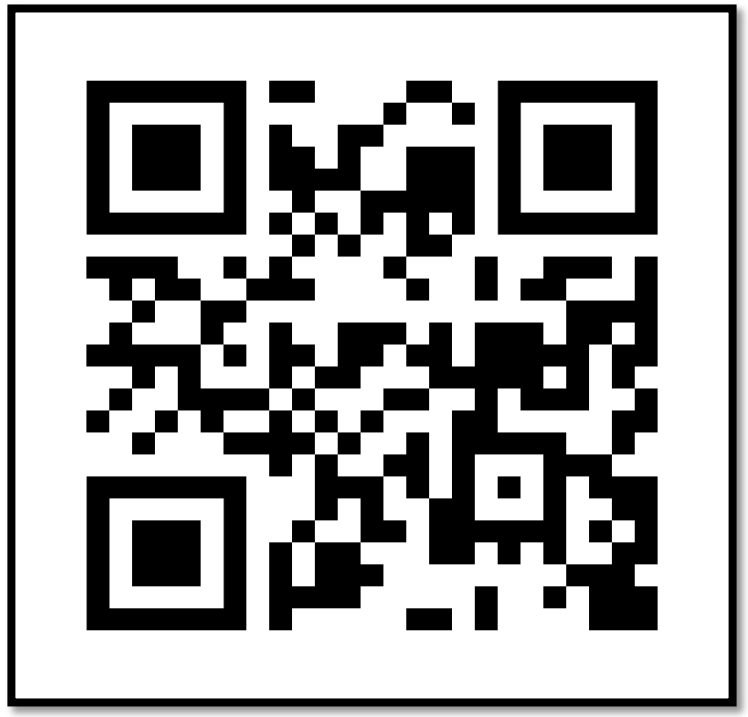
Post Webinar Questionnaire

- **Let us know how we did**

- https://gdit.zoomgov.com/survey/7Mp6wfJvEbbg3NwDtQr_lIEysbmUZg7e0RH25JBpru49K_WHsII.sKFn7RfCOBYzpQ1y/view?id=ZIBBHFOTTNqA7RBPX54DsA#/sharePreview

EPA's Cybersecurity for the Water Sector Website

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



Questions?