**FACILITY NAME RISK AND RESILIENCe ASSESSMENT**

**\*\*THIS DOCUMENT IS EXEMPT FROM FOIA\*\***

**\*\*DO NOT SHARE UNDER FOIA OR ANY OTHER REQUEST\*\***

5 ILCS 140/7 (From Ch. 116, par. 207)

Sec. 7. Exemptions.

1. When a request is made to inspect or copy a public record that contains information that is exempt from disclosure under this Section, but also contains information that is not exempt from disclosure, the public body may elect to redact the information that is exempt. The public body shall make the remaining information available for inspection and copying. Subject to this requirement, the following shall be exempt from inspection and copying:

(v) Vulnerability assessments, security measures, and response policies or plans that are designed to identify, prevent, or respond to potential attacks upon a community's population or systems, facilities, or installations, the destruction or contamination of which would constitute a clear and present danger to the health or safety of the community, but only to the extent that disclosure could reasonably be expected to jeopardize the effectiveness of the measures or the safety of the personnel who implement them or the public. Information exempt under this item may include such things as details pertaining to the mobilization or deployment of personnel or equipment, to the operation of communication systems or protocols, or to tactical operations.

(w) (Blank).

(x) Maps and other records regarding the location or security of generation, transmission, distribution, storage, gathering, treatment, or switching facilities owned by a utility, by a power generator, or by the Illinois Power Agency.

**PURPOSE**

The purpose of this Risk and Resilience Assessment (RRA) is to fulfill the requirements of Section 2013 of the America's Water Infrastructure Act (AWIA). AWIA requires water systems serving more than 3,300 people to develop, or update, risk and resiliency assessments (RRA) and emergency response plans (ERPs). It further establishes components that the RRAs and ERPs must address and creates deadlines by which water systems must certify to the United States (US) Environmental Protection Agency (EPA) completion of the RRA and ERP.

**INTRODUCTION**

To aid in continuing the water system’s mission of providingsafe water of adequate quantity to meet the needs of our customers, this RRA contains the required six elements outlined in the AWIA. Specifically, this plan contains:

* Risk to the system from malevolent acts and natural hazards;
* The financial infrastructure of the system;
* Resilience of the pipes and constructed conveyances, physical barriers, source water, water collection and intake, pretreatment, treatment, storage and distribution facilities, electronic, computer, or other automated systems (including the security of such systems) which are utilized by the system;
* The monitoring practices of the system;
* The use, storage, or handling of various chemicals by the system; and
* the operation and maintenance of the system.

**PLAN TRACKING INFORMATION**

| **Plan Distribution** | | |
| --- | --- | --- |
| **Recipient/Title** | **Distributed By** | **Date** |
| Fill in each recipient’s name and title, the person who gave them the plan and on what date. |  |  |
|  |  |  |
|  |  |  |

| **Change History** | | |
| --- | --- | --- |
| **Description of Change** | **Name/Title** | **Date** |
| Describe the changes made to this plan since its original development, who made the changes and on what date the changes were incorporated into this plan. (e.g., Update contact and added cyber security.) |  |  |
|  |  |  |
|  |  |  |

To accomplish this planning and documentation process, the attributes of the water supply have been systematically analyzed leading to the development of a comprehensive assessment.

**SYSTEM INFORMATION**

**Water System ID:**   
**Water System Name:**   
**County Served:**   
**Population Served:**   
**Address:**   
**City State Zip:**   
**Phone:**   
**Fax:**   
**Email:**

**PRIMARY EMERGENCY CONTACT INFORMATION**

**Contact Name:**   
**Contact Title:**   
**Daytime Phone:**   
**Cell Phone:**   
**Email:**

**SECONDARY EMERGENCY CONTACT INFORMATION**

**Contact Name:**   
**Contact Title:**   
**Daytime Phone:**   
**Cell Phone:**   
**Email:**

**RISK TO SYSTEM ASSETS AND POTENTIAL FINANCIAL IMPACT**

Community Water Supply (CWS) officials have developed the following asset risk assessment including relevant financial information. The following table summarizes this information.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **State and Local ID** | **Description/Location** | **Insurance Value** | **List All Identified \*** | **Relative Priority High/Medium/Low** |
| *(List all sources of water) (e.g. wells, intakes)* |  |  |  |  |
| *e.g. Well 100 (99999)* | *e.g., Located at WTP, 100 N. Main St.* | *e.g., $1.5 million* | *e.g., Tornado, Earthquake, Malevolent Break in, Cyberattack, Sabotage* | *e.g., High* |
| *(Indicate Treatment plant with appropriate level of specificity) (e.g., Consider referencing at level of insurance appraisal)* |  |  |  |  |
|  |  |  |  |  |
| *IL2050100* | *e.g., Ion Exchange Treatment Plant located at 100 N. Main St.* | *e.g., $20.0 Million* | *e.g., Tornado, Earthquake, Malevolent Break in, Cyberattack, Sabotage* | *e.g., High* |
| *(Indicate storage and distribution system components to the appropriate level of specificity) (e.g., pipes, storage tanks, high/low service pumps, etc.)* |  |  |  |  |
| *e.g., Elevated Storage* | *e.g, 500,000 gallon welded steel tower located at 100 Merchant Street* | *e.g, $1.5 million* | *e.g., Malevolent Break in, Cyberattack, Sabotage* | *e.g., High* |
|  |  |  |  |  |
| *Other (Consider listing other assets listed for insurance purposes)* |  |  |  |  |
| *e.g., Stationary Generator* | *e.g., 600 kw located at water plant* | *e.g., $250,000* | *e.g., Malevolent Break in, Cyberattack, Sabotage* | *e.g., Medium* |
|  |  |  |  |  |

**\*e.g., Flood, Tornado, Earthquake, Ice Storm, Fire, Cyberattack, Malevolent Break-in (Physical Assault), Theft, Sabotage, Intentional Contamination of Source Water, Intentional Contamination of Finished Water, Other**

**Resilience of assets**

To aid in the development of emergency planning documents, water supply officials evaluated the preceding assets to determine the system’s ability to prevent or respond to damage that could inhibit or prevent the provision of adequate quantities of potable water to customers of the system.

Prior to the evaluation of specific asset resilience, the water supply noted the following general precautions that aid in the security of staff and equipment:

* Per Illinois Law (Public Water Supply Operations Act, 415 ILCS 45), water supply operators must be properly licensed and receive continuing education to renew their license. Further, properly credentialed individuals cannot have a civil or criminal record that could pose a risk to the provision of safe water.
* Access to critical components (e.g., wells, water treatment plant, storage tanks, operational technology, etc.) of the water supply is restricted to operational staff. Access to the critical components is controlled by various means including physical and electronic security systems.
* Operational staff control locked portions of the system including wells, water treatment plant and storage facilities. As necessary, the water superintendent restricts access to keys for the system. When staff leave the employment of the water system, they must return keys to eliminate their ability to gain entry to components of the water supply. Additionally, depending on the employee separation cause/reason, water supply officials may re-key facilities as needed.
* Water supply operational officials inspect critical components of the water system daily and often more frequently. The local police department is familiar with the water system and operational staff.
* Operational staff maintain the grounds surrounding critical components of the system and can react to security vulnerabilities. Staff have been advised to report security vulnerabilities to the responsible operator in charge and to report potential security breaches to the local police department.
* Operation staff will use all means available for the early detection and reaction to malevolent threats/acts, cyber intrusions, natural disasters or other emergency conditions. Water supply official will diligently monitor facilities for unauthorized entry, cyber threats, and extreme weather forecasts from the National Weather Service or Army Corps of Engineers.
* Wells are maintained in accordance with state regulation (35 Il Adm Code 604.240) including, but not limited to, sanitary seals, vents, screens and source water monitoring. In addition, water supply officials conduct monthly bacteria monitoring to ensure the sanitary safety of the source water.
* &/OR Surface water intake structures are constructed/maintained in accordance with state regulation (35 Il Adm Code 604.215), including, but not limited to, the ability to draw water from various depths, protection from icing (particularly frazzle ice) and protection from physical damage.
* In compliance with 35 Il Adm Code 604.105(d), the water supply has sufficient redundant equipment to replace faulty/inoperable apparatus in an emergency;
* The water system has sufficient capacity to overcome a substantial emergency in various components of its source and water treatment facility. 35 Il Adm Code Section 604.105(a) requires the water supply to be designed to produce at least 20 percent greater than the maximum average daily demand of consumers.
* The water system complies with electrical control and standby power requirements in 35 IL Adm Code 604.155. Standby power is available to safely produce an adequate water supply to customers and electrical controls are secure.
* In compliance with 35 Il Adm Code 604.1415(a), the water supply distribution system maintains a minimum pressure of 20 psi. If pressure drops below 20 psi for any reason, immediate emergency procedures are instituted, including issuance of a boil order.
* The water system has an Illinois EPA approved cross-connection control program and completes a triennial survey of its distribution system (per 35 IL Adm Code 604, Subpart O).
* The water system complies with stored water requirements and fire flow requirements in 35 IL Adm Code 604.1340 and 604.1300, respectively. The water system has roughly one day of stored water.
* Water system staff, with assistance of local fire department staff, control the use of hydrants and valves.
* Security sensitive records including, but not limited to, Emergency Response Planning documents, maps and plans of the distribution system, and statutorily required reports are maintained in a secure location. Generally, this information is secured at the water plant or city hall. Employees follow the Freedom of Information Act requirements and consult corporate counsel, as necessary.
* To the extent possible, Supervisory Control and Data Acquisition (SCADA) and business computer software and hardware are protected from cyber-attack. Cybersecurity has been evaluated using the U.S. EPA Checklist of Priority Cybersecurity Practices for Water Systems, see Appendix A. Generally, upon detection of a cyber threat to one of the system assets, compromised computers will be disconnected, and breached components will be isolated to prevent further damage or the spreading of malware. Notification of the incident will be made to the United States Cybersecurity and Infrastructure Security Agency (CISA), the Illinois Emergency Management Agency (IEMA), the local Federal Bureau of Investigation (FBI) and the appropriate Illinois EPA Regional Office.

The following table provides an evaluation of the existing and needed enhancement to the resilience of the specific assets of the water system:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **State and Local ID** | **Existing Security Countermeasures** | **Existing protection against Natural Disasters** | **High Priority Countermeasure/ Disaster Protection Enhancements\*** | **Moderate Priority Countermeasure/ Disaster Protection Enhancements\*\*** |
| *(List all sources of water-should mirror table above* | *(e.g., fencing, locks, cameras, lighting, warning signs, motion sensors, alarms)* | *(e.g., berms, levees, redundancy, generators, etc.)* | *(e.g., Install locks on the water plant door.)* | *(e.g., construction of a levee)* |
| *e.g. Well 100 (99999)* | *e.g., Well is contained within the water treatment plant property perimeter fence. Security lighting is provided and Local PD patrols after hours.* | *e.g., The well is located 2 ft. above the 100 year flood and can be supplied electricity through a back-up generator.* | *e.g., The well house door lock has been compromised and needs to replaced.* | *e.g., Moderate - Additional Cyber risk reduction through consultant evaluation and mitigation.* |
|  |  |  |  |  |
| *(Indicate Treatment plant with appropriate level of specificity) -should mirror table above* | *(e.g., SCADA/Computer systems are properly password protected, business systems are physically separate from SCADA, & an active firewall protects critical systems)* | *(e.g., water treatment plant can be bypassed and water piped directly to distribution system from wells sources.)* | *e.g., Perimeter gate needs to be repaired such that the facility can be secured at all times.* | *e.g., Camera and alarm system needs to be installed to monitor treatment plant when staff not present.* |
|  |  |  |  |  |
| *(Indicate storage and distribution system components to the appropriate level of specificity) -should mirror table above* | *e.g., perimeter fencing and ladder locking system* | *(e.g., distribution system has redundant elevated storage tanks)* | *e.g., None identified.* | *e.g., Alarm system needs to be installed to indicate security breach.* |
|  |  |  |  |  |
|  |  |  |  |  |

**\*High priority countermeasures/protection need to be acted upon regardless of cost considerations.**

**\*\*Moderate priority countermeasures/protection need to be acted upon as funds become available.**

**Monitoring Practices**

In evaluating the potential risk of pathogens or chemical contaminant to the Community Water Supply (CWS), officials recognizes the importance of routine monitoring to detect the possibility of contamination of source water, treatment chemicals/process or the distribution system. The importance of monitoring water quality is demonstrated by the fact that a CWS in Illinois must comply with the Illinois Environmental Protection Act (415 ILCS 5/) and regulations found in 35 Il Adm Code. These state laws and regulations are generally more stringent (they must be at least as stringent) than the federal Safe Drinking Water Act (40 CFR).

The monitoring for contaminants of concern make up a substantial portion of the regulations adopted within the Federal/Illinois Registers. In fact, the U.S. EPA has established protective drinking water standards for more than 90 contaminants, including drinking water regulations issued since the 1996 amendments to the Safe Drinking Water Act that strengthen public health protection.

Specifically, the Illinois EPA enforces the drinking water standards that include monitoring requirements found in 35 Il Adm Code Part 611 (Primary Drinking Water Standards) for treated water and 35 Il Adm Code Part 620 for groundwater. To ensure that water systems properly monitor for various contaminants, the Illinois EPA routinely issues sample demand letters, establishes special exception permits (see 35 IL Adm Code Part 604) and posts monitoring schedules on their Drinking Water Watch Website (<http://water.epa.state.il.us/dww/>).

Additionally, the Illinois EPA enforces 35 Il Adm Code 604.130 regarding routine operational testing and 604.165 that establishes routine testing parameters for monthly operating reporting. These parameters can be utilized in the detection of anomalies that could be viewed as early warning signals of a water quality concern resulting from natural or nefarious causes.

At the current time, the FACILITY NAME complies with Illinois drinking water monitoring requirements.

Further, during an emergency, water supply staff will monitor the situation through treatment plant and distribution system controls (e.g., process control testing, chemical usage, tower elevations, system pressures and disinfectant residuals will give an indication of the status of the safety and capacity of the water system). The water system maintains adequate testing equipment to evaluate these areas of concern and the safety of the water supply. Upon resolution of the emergency condition and repair to the affected asset(s), the responsible operator in charge will conduct an evaluation of the water system. Should water quality monitoring be necessary, the operational staff will coordinate with the Illinois EPA and County Health Department as well as its contractual laboratory to ensure the safety of the water.

**Chemical Use, Storage and Handling**

Chemical use, storage and handling is also regulated by the Illinois EPA under 35 IL Adm Code. At the current time, the FACILITY NAME complies with Illinois regulations governing use, storage and handling of chemicals under this regulation. Specifically, all chemicals are stored in a secure location and are properly isolated. Additionally, chemical usage is evaluated on an ongoing basis by the Illinois EPA through monthly operational reporting as required by 35 IL Adm Code Part 604. Should it be necessary to employ a “new” chemical or modify chemical addition practices, the Illinois EPA requires that a licensed professional engineer obtain a construction permit and subsequent operating permit for NSF 60 certified chemical per 35 IL Adm Code Part 602.

With respect to additional chemical handling practices, chemical deliveries are made in the presence of operational staff and controlled accordingly. Further, chemical suppliers have a longstanding relationship with the CWS and understand operational procedures. Material Safety Data Sheets (MSDS) are maintained in the water treatment plant for all hazardous chemicals and operational staff are afforded proper personal protective equipment (PPE) for their safety. Finally, the Illinois Department of Labor routinely inspects the CWS to ensure worker safety concerns are addressed.

**Operation/Maintenance of the System**

The operation and maintenance of CWSs is regulated by the Illinois EPA under 35 IL Adm Code. Routine inspections of the water system are made by the Illinois EPA to confirm compliance with 35 IL Adm Code Part 604. The most recent inspection report is maintained at the water treatment plant/city hall. This report identified points of concern with respect to compliance with the regulations as well as recommendations to enhance the design, operation and maintenance of the water system. Also, of importance, the Illinois EPA documentation includes an inventory of critical resources.

At the time of the last inspection (and subsequent follow-up action by the water system), the FACILITY NAME has taken all necessary action to comply with Illinois regulations governing the design, operation and maintenance of the CWS. (Note: the Illinois EPA has confirmed that the inspections conducted by their staff conform to the guidelines for Sanitary Surveys. Illinois EPA’s primary enforcement authority is routinely reviewed by the U.S. EPA Region 5 for conformity with Safe Drinking Water Act requirements.)

To further ensure the safety of the water system, the water supply provides annual consumer confidence reports to its customers, triennial cross-connection control surveys, flushing notice and other periodic educational materials through news media and direct mailings. Through these materials, customers should be aware where their water originates, how it is treated and its expected quality.

This customer education should provide a sound platform for the additional surveillance of water quality changes in the distribution system. Customer concerns in this regard are investigated immediately. When necessary, operational staff contact the Illinois EPA, Illinois Rural Water Association, consulting engineers, and other technical service providers in addressing these consumer concerns. In the event that a contaminant of concern is discovered, operational staff immediately coordinate with Illinois EPA to ensure that State regulations are followed with proper public notification of contamination or suspected contamination. (Note: the regulatory requirement are identified in 35 Il Adm Code Part 611 and the Illinois Sample Collector Handbook, <https://www2.illinois.gov/epa/topics/compliance-enforcement/drinking-water/Pages/sample-collectors-handbook.aspx>)

In the event of an emergency, the water system has identified the following critical customers. These customers will be afforded special attention should a water quality or water quantity emergency occur.

**Critical Customer Inventory**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Customer** | **Contact Name** | **Location** | **Customer Type** | **Phone Number(s)** | **Relative Priority High/Medium** |
|  |  |  | **Hospital** |  |  |
|  |  |  |  |  |  |
|  |  |  | **School** |  |  |
|  |  |  |  |  |  |
|  |  |  | **Day Care** |  |  |
|  |  |  |  |  |  |
|  |  |  | **Nursing Home** |  |  |
|  |  |  |  |  |  |
|  |  |  | **Food Processing** |  |  |
|  |  |  |  |  |  |
|  |  |  | **Health Care** |  |  |

**Appendix A:** Checklist of Priority Cybersecurity Practices for Water Systems

Note: Any items marked “no” should include an explanation

|  | **Question**  Does the CWS… | **Answer**  Mark the appropriate check box (“Yes”, “No”, “In progress”, “Not applicable”) to answer each cybersecurity assessment question. |
| --- | --- | --- |
|  | **Reduce Exposure to Public-Facing Internet** | |
| 1. | Ensure assets connected to the public Internet expose no unnecessary exploitable services (e.g., remote desktop protocol) and eliminates connections between OT assets and the Internet? | Yes  No  In progress  Not applicable  *If “No”, EPA recommends that the CWS take the following action: Eliminate unnecessary exposed ports and services on public-facing assets with regular review and eliminate OT asset connections to the public Internet unless explicitly required for operations.* |
|  | **Conduct Regular Cybersecurity Assessments** | |
| 2. | Conduct regular cybersecurity assessments? | Yes  No  ☐In progress  ☐Not applicable  *If “No”, EPA recommends that the CWS take the following action: Conduct a cybersecurity assessment on a regular basis to understand the existing vulnerabilities within OT and IT systems. Assessments enable you to identify, assess, and prioritize mitigating vulnerabilities in both OT and IT networks.* |
| 3. | Have a named role/position/title that is responsible for planning, resourcing, and executing cybersecurity activities within the CWS? | ☐Yes  ☐No  ☐In progress  ☐Not applicable    *If “No”, EPA recommends that the CWS take the following action: Identify one role/position/title responsible for cybersecurity within the CWS. Whoever fills this role/position/title is then in charge of all CWS cybersecurity activities.* |
|  | **Change Default Passwords Immediately** | |
| 4. | Change default passwords and require a minimum length for passwords? | ☐Yes  ☐No  ☐In progress  ☐Not applicable  *If “No”, EPA recommends that the CWS take the following action: Change all default manufacturer or vendor passwords before equipment or software is put into service and implement a minimum length requirement for passwords through a policy and/or administrative controls set in the system.* |
| 5. | Require multi-factor authentication (MFA) wherever possible, but at a minimum to remotely access CWS/OT/IT networks? | ☐Yes  ☐No  ☐In progress  ☐Not applicable  *If “No”, EPA recommends that the CWS take the following action: Deploy MFA as widely as possible for both operational technology (OT) and information technology (IT) networks. At a minimum, MFA should be used for remote access to the OT network.* |
|  | **Conduct Inventory of OT/IT Assets** | |
| 6. | Maintain an updated inventory of all OT and IT network assets? | Yes  No  ☐In progress  ☐Not applicable  *If “No”, EPA recommends that the CWS take the following action: Regularly review (no less than monthly) and maintain a list of all Operational Technology (OT) and IT assets with an IP address. This includes third-party and legacy (i.e., older) equipment. 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.* |
| 7. | Maintain current documentation detailing the set-up and settings (i.e., configuration) of critical OT and IT assets? | Yes  No  ☐In progress  ☐Not applicable  *If “No”, EPA recommends that the CWS take the following action: Maintain accurate documentation of the original and current configuration of OT and IT assets, including software and firmware version* |

|  |  |  |
| --- | --- | --- |
|  | **Develop & Exercise Cybersecurity Incident Response & Recovery Plans** | |
| 8. | Have a written cybersecurity incident response (IR) plan for critical threat scenarios (e.g., disabled or manipulated process control systems, the loss or theft of operational or financial data, exposure of sensitive information), which is regularly reviewed, practiced, and updated? | ☐Yes  Date of last IR plan review/update: *[insert month/day/year]*  ☐No  ☐In progress  ☐Not applicable    *If “No”, EPA recommends that the CWS take the following action: Develop, practice, review, and update an IR plan for cybersecurity incidents that could impact CWS operations. Participate in discussion-based (ex. TTX) and operations-based exercises (ex. Drill) to improve responses to potential cyber incidents.* |
| 9. | Have a written procedure for reporting cybersecurity incidents, including how and to whom? (e.g., phone call, internet submission) and to whom (e.g., FBI or other law enforcement, CISA, state regulators, Water Information Sharing & Analysis Center - WaterISAC, cyber insurance provider)? | ☐Yes  ☐No  ☐In progress  ☐Not applicable  *If “No”, EPA recommends that the CWS take the following action: Document the procedure for reporting cybersecurity incidents to better aid law enforcement, receive assistance with response and recovery, and to promote water sector awareness of cybersecurity threats. (See OW factsheet)* |
|  | **Backup OT/IT Systems** | |
| 10. | Backup systems necessary for operations (e.g., network configurations, PLC logic, engineering drawings, personnel records) on a regular schedule, store backups separately from the source systems, and test backups on a regular basis? | ☐Yes  ☐No  ☐In progress  ☐Not applicable  *If “No”, EPA recommends that the CWS take the following action: 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 type*  *1) Store one copy offsite.* |
|  | **Reduce Exposure to Vulnerabilities** | |
| 11. | Patch or otherwise mitigate known vulnerabilities within the recommended time frame? | ☐Yes  ☐No  ☐In progress  ☐Not applicable  *If “No”, EPA recommends that the CWS take the following action: Identify and patch vulnerabilities in a risk-informed manner (e.g., critical assets first) as quickly as possible* |
| 12. | Require unique and separate credentials for users to access OT and IT networks and separate user and privileged (e.g., System Administrator) accounts? | ☐Yes  ☐No  ☐In progress  ☐Not applicable  *If “No”, EPA recommends that the CWS take the following action: Require a single user to have two different usernames and passwords; one account to access the IT network, and the other account to access the OT network to reduce the risk of an attacker being able to move between both networks using a single login and restrict System Administrator privileges to separate user accounts for administrative actions only and evaluate administrative privileges on a recurring basis to ensure accurate information for the individuals who have these privileges.* |
| 13. | Prohibit the connection of unauthorized hardware (e.g., USB devices, removable media, laptops brought in by others) to OT and IT assets? | ☐Yes  ☐No  ☐In progress  ☐Not applicable  *If “No”, EPA recommends that the CWS take the following action: When feasible, remove, disable, or otherwise secure physical ports (e.g., USB ports on a laptop) to prevent unauthorized assets from connecting.* |
| 14. | Immediately disable access to an account or network when access is no longer required due to retirement, change of role, termination, or other factors? | ☐Yes  ☐No  ☐In progress  ☐Not applicable  *If “No”, EPA recommends that the CWS take the following action: Terminate access immediately to accounts or networks upon a change in an individual’s status making access unnecessary (i.e., retirement, change in position, etc.).* |
|  | **Conduct Cybersecurity Awareness Training** | |
| 15. | Provide/conduct annual cybersecurity awareness training for all CWS personnel that covers basic cybersecurity concepts? | ☐Yes  ☐No  ☐In progress  ☐Not applicable  *If “No”, EPA recommends that the CWS take the following action: Conduct cybersecurity awareness training annually, at a minimum, to help all employees understand the importance of cybersecurity and how to prevent and respond to cyberattacks.* |