You may leave and re-enter the survey to update your response at any time until the deadline of 11:59 PM on Friday, October 29, as long as you use the same computer and have not yet submitted your response.

Questions with an asterisk (*) require an answer.

* 1. What will WaterISAC do with your response?

Only WaterISAC staff will see your response. Staff will aggregate the information you submit with that of other respondents, providing numerical totals and details of incidents and suspicious activities that have occurred at water and wastewater utilities nationwide and internationally to be presented in its analyses and products, including the upcoming Quarterly Water Sector Incident Summary and Threat Analysis. When presenting a specific piece of information provided by a utility in WaterISAC's analyses and products, staff will maintain the confidentiality of the utility. Staff will not divulge the utility's name, the names of its personnel, its location, or other details that could be used to clearly attribute the information to the utility. The following is an example of how staff might share a specific piece of information provided by a utility: "A large drinking water utility reported its website was defaced by possible supporters of the Islamic State."

The analyses and products WaterISAC develops using the information will be marked TLP:AMBER. Recipients may only share TLP:AMBER information with members of their own organization, and with clients or customers who need to know the information to protect themselves or prevent further harm. For more information on the Traffic Light Protocol (TLP), visit this Cybersecurity and Infrastructure Security Agency webpage: https://www.cisa.gov/tlp

WaterISAC will share the analyses and products it develops using the information provided via the survey with its members and partners, which include federal (e.g., EPA and DHS), state, and local government entities and sector associations. For all entities it shares its analyses and products with, WaterISAC will maintain the confidentiality of the utilities who provided information. This policy applies regardless of whether the utility is a member or non-member. What’s more, as a private organization, WaterISAC is not subject to public disclosure laws.

May WaterISAC have your permission to use the information you provide in an aggregated and confidential format in upcoming analyses and products to be shared with other members and partners?

- ○ Yes
- ○ No

* 2. **Your Information**

Your Name	
Your Role/Title	
Utility Name	
City	
State/Province	
Phone Number	
Email Address	

* 3. **Utility Type**

- ○ Drinking Water
- ○ Wastewater
- ○ Combined

* 4. **Utility Size by Population Served**

- ○ Small (<3,300)
- ○ Medium (3,301 - 10,000)
- ○ Large (10,001 to 100,000)
- ○ Very Large (>100,000)

PHYSICAL SECURITY INCIDENTS

Provide information on physical security incidents - successful or attempted - between July 1 and September 30, 2021.

* 5. **Did your organization experience any successful or attempted physical security incidents that did or that had the potential to cause:**

- Harm to employees or customers;

- Public health impacts;

- Significant harm to the environment;

- Impacts to the operations of your utility;

- A significant security breach for your utility; or

- Financial losses to your utility of $10,000 or more (per instance)?

- ○ Yes
- ○ No
- ○ Can't answer - my responsibilities do not include tracking these kinds of incidents

* 6. **Intentional water supply contamination. (Definition: Introduction of an unwanted substance into raw or potable water supplies for the purpose of harming human health or utility assets.)**

Did your organization experience any successful or attempted incidents of water supply contamination?

- Yes
- No

Please describe any notable incidents.

* 7. **Intentional wastewater contamination (Definition: Introduction of an unwanted substance into wastewater or wastewater effluent for the purpose harming human health, the environment, or utility assets.)**

Did your organization experience successful or attempted incidents of wastewater contamination?

- Yes
- No

Please describe any notable incidents.

* 8. **Sabotage/tampering (Definition: Deliberately damaging or manipulating part of a facility to obstruct, disrupt, or destroy operations; it is more than just vandalism.)**

Did your organization experience successful or attempted incidents of sabotage/tampering?

- Yes
- No

Please describe any notable incidents.

* 9. **Breach/Intrusion (Definition: Unauthorized personnel entering a restricted area, secured protected site, or nonpublic area where harm could be done to facilities, equipment, operations, or personnel. It does not include relatively minor cases of trespassing.)**

Did your organization experience successful or attempted breaches/intrusions?

- ◯ Yes
- ◯ No

Please describe any notable incidents.

* 10. **Misrepresentation (Definition: Presenting false information or misusing insignia, documents, and/or identification to misrepresent one's affiliation as a means of concealing possible illegal activity. This activity could be directed at utility personnel or customers.)**

Did your organization experience successful or attempted incidents of misrepresentation?

- ◯ Yes
- ◯ No

Please describe any notable incidents.

* 11. **Assault (Definition: A physical attack on an employee or group of employees with the intent to cause bodily harm or on a facility to cause damage.)**

Did your organization experience successful or attempted incidents of assault?

- ◯ Yes
- ◯ No

Please describe any notable incidents.

* 12. **Thefts (Definition: Stealing organization equipment, supplies, chemicals, or funds that amounts to $10,000 or more, per instance.)**

Did your organization experience successful or attempted incidents of theft?

- ○ Yes
- ○ No

Please describe any notable incidents.

13. **Please describe any other notable physical security incidents your organization experienced.**

PHYSICAL SECURITY INCIDENTS - POTENTIAL PREPARATORY ACTIVITIES

Provide information on potential preparatory activities for physical security incidents against your utility between July 1 and September 30, 2021.

* 14. **Surveillance or suspicious questioning (Definition: Collection of information about facilities or personnel and their activities, for possible or confirmed malicious purposes. Surveillance can be conducted in person or remotely, such as through the use of binoculars or drones, and it can involve the perpetrator making notes, drawing maps, or taking photographs. Suspicious questioning can also be done in person or via phone, email, etc.)**

Did your organization experience successful or attempted incidents of surveillance?

- ○ Yes
- ○ No

Please describe any notable incidents.

* 15. **Threats (Definition: Stated intent to inflict pain, injury, damage or other hostile action on someone or something [e.g., bomb threat]. *This does not include threats to contaminate water supplies, which is a separate question posed above.*)**

Did your organization experience threats?

- ○ Yes
- ○ No

Please describe any notable incidents.

DISINFORMATION AND MISINFORMATION

Describe any disinformation and misinformation incidents involving your utility between July 1 and September 30, 2021.

* 16. **Disinformation (Definition: Inaccurate information that is spread deliberately to create disruptive or adverse effects. Disinformation campaigns are also referred to as "influence operations," "information warfare," and "fake news.")**

Did your organization experience disinformation?

- ○ Yes
- ○ No
- ○ Can't answer - my responsibilities do not include tracking these kinds of incidents

Please describe any notable incidents.

* 17. **Misinformation (Definition: Inaccurate information that is spread without malicious intent). *Please only include misinformation that caused or that had the potential to cause disruptive or adverse effects.***

Did your organization experience misinformation?

- ○ Yes
- ○ No
- ○ Can't answer - my responsibilities do not include tracking these kinds of incidents

Please describe any notable incidents.

CYBERSECURITY INCIDENTS

Provide information on cybersecurity incidents against your utility between July 1 and September 30, 2021.

* 18. **Did your organization experience any successful or unsuccessful attacks against its industrial control systems?**

- ○ Yes
- ○ No
- ○ Can't answer - my responsibilities do not include tracking these kinds of incidents.

Please describe any notable incidents.

* 19. **Did your organization experience any successful or unsuccessful but significant attacks involving its business/enterprise information systems?** *(Factors that could contribute to an unsuccessful attack being significant include that it was targeted, revealed previously unknown vulnerabilities, or was nearly successful.)*

- ○ Yes
- ○ No
- ○ Can't answer - my responsibilities do not include tracking these kinds of incidents

Please describe any notable incidents.

20. **Please specifically describe any ransomware, Business Email Compromise (BEC), or other notable cybersecurity incidents your organization experienced.**

CONCLUSION

21. **If you have any questions, comments or suggestions, WaterISAC welcomes them.**