You may leave and re-enter the survey to update your response at any time until the deadline of 11:59 PM on Friday, July 31, 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?

WaterISAC requests your permission to aggregate the information you provide with that of other respondents and to anonymize details of any reported incidents for use in the upcoming Water Sector Incident Summary, Threat Analysis, and similar products. Numerical information will be presented only as nationwide totals. Details of incidents, if used, would be presented in complete anonymity such as: "In November, one water utility reported its website had been defaced by possible supporters of the Islamic State."

Confidentiality: As with any incident information provided by a utility to WaterISAC, only WaterISAC staff will see your survey responses. WaterISAC's policy is to never share details of a utility's security incidents or related information with any other entity except with the utility's express permission. 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 anonymized format in the upcoming Water Sector Incident Summary, Threat Analysis, and similar products?

- ◯ 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 April 1 and June 30, 2020.

* 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

* 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

* 14. **Did your utility experience any acts of surveillance or suspicious questioning or threats?**

- ◯ Yes
- ◯ No

* 15. **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.

* 16. **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

Provide information on incidences of disinformation and misinformation that impacted your utility between April 1 and June 30, 2020.

Note the following:

Disinformation is inaccurate information that is spread deliberately to create disruptive or adverse effects. It differs from **misinformation** (inaccurate information such as rumors) because it is intentionally inaccurate and spread with malicious intent.

* 17. **Did your organization experience any disinformation or misinformation?**

- Yes
- No

* 18. **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

Please describe any notable incidents.

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

Did your organization experience misinformation?

Yes No

Please describe any notable incidents.

CYBERSECURITY INCIDENTS

Provide information on cybersecurity incidents against your utility between April 1 and June 30, 2020.

* 20. **Did your organization experience any cybersecurity incidents that involved:**

- A successful or unsuccessful attack involving its industrial control systems; or

- A successful or unsuccessful but significant attack 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

* 21. **Did your organization experience successful or unsuccessful attacks involving its industrial control systems?**

Yes

No

Please describe any notable incidents.

* 22. **Did your organization experience successful or unsuccessful but significant attacks involving its business/enterprise information systems?**

Yes

No

Please describe any notable incidents.

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

CONCLUSION

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

* 25. Would you answer three additional questions regarding the COVID-19 pandemic?

- Yes
- No

26. What impacts has your utility experienced as a result of the COVID-19 pandemic?

- [ ] Confirmed cases among employees
- [ ] Supply chain disruptions
- [ ] Service disruptions due to employee absences and/or lack of essential supplies
- [ ] Revenue losses
- [ ] Infrastructure damage (from restarted construction activity)
- [ ] Other

Please use this space to describe impacts.

27. Which of the following statements best describes your organization's remote work policy going forward?

- [ ] Continuing for a significant part of the organization
- [ ] Continuing but limited, such as for high risk individuals
- [ ] Ceasing entirely
- [ ] Other
- [ ] Does not apply

Please use this space to describe your organization's remote work policy.

28. What measures has your utility implemented to reduce the risk of COVID-19 transmission among employees?

- [ ] Engineering controls, which involve isolating hazards from employees and require no actions or different behavior on their part (e.g., installing plexiglass barriers and ensuring ventilation and water systems operate properly)
- [ ] Administrative controls, which require action by employees and typically necessitate changes in work policies (e.g., encouraging sick employees to stay at home, implementing health screenings, and promoting personal hygiene)
- [ ] PPE distribution, such as for face masks and gloves
- [ ] Other
- [ ] None

Please use this space to describe measures your organization has implemented.

29. How prepared does your utility believe it is for future waves of COVID-19 or other pandemics?

- ( ) Very Prepared
- ( ) Somewhat Prepared
- ( ) Not Prepared

Please use this space to describe your organization's level of preparedness.

30. Does your organization have any lessons learned from its response to COVID-19 that it would be willing to share with WaterISAC?

- ( ) Yes
- ( ) No