Via DelaFile
October 30, 2024

Malika Davis, Deputy Director
Delaware Public Service Commission
861 Silver Lake Boulevard
Cannon Building, Suite 100
Dover, Delaware 19904

RE: PSC Docket Nos. 16-0659 – Artesian Water Company
Responses to Cybersecurity Questions - 2024

Dear Ms. Davis:

Please accept this letter and the attachment as compliance with Delaware Public Service Commission Order No. 8955 in the above referenced docket. Artesian Water Company, Inc. ("Artesian") has reviewed the list of questions pertaining to cybersecurity which are currently posted on the Commission's website and has no suggested changes to those questions. Attached hereto is a copy of the cybersecurity questions and Artesian's responses.

Please feel free to contact Michael Christopher at (302) 453-7108 should you have any questions regarding this filing.

Respectfully Submitted,

David B. Spacht
Artesian Water Company, Inc.
Chief Financial Officer

Planning/Risk Management

- Is your cybersecurity plan regularly reviewed and audited? If yes, is it audited internally or externally?
  Response:
  Yes. Both.

- How often is the cybersecurity plan reviewed?
  Response:
  At least yearly and as risks are identified.

- Do you assess vulnerabilities and threats to your system and assets?
  Response:
  Yes.

- Do you have a documented risks assessment and management program?
  Response:
  Yes.

- Is cybersecurity addressed differently for IT and OT systems?
  Response:
  Yes.

- Does your company include in its procurement contract language cybersecurity requirements for IT and OT assets?
  Response:
  Yes.

- Do you have a documented records retention policy?
  Response:
  No.

Personnel and Policies

- Are background checks being conducted upon hire for those with access to critical systems and assets?

  Response:

  Yes.

- Do you provide internal cyber security training for all employees?

  Response:

  Yes.

- Do you provide enhanced internal cyber security training for those that are actually in the utility's information technology (IT) and operations technology (OT) networks?

  Response:

  Yes.

- Are there structural and/or organizational policies and procedures in place that allow the utility to be able to address cybersecurity issues?

  Response:
  Yes.

- Are there managerial and operational controls in place to ensure compliance with the company's cybersecurity policies and procedures?

  Response:
  Yes.

- How quickly is access terminated for personnel who leave the company?

  Response:

  Promptly.

- Do you have certain employees who are assigned as cybersecurity personnel? Or is the function outsourced?

  Response

  Yes. Both.

- Do you have specific practices and policies in place about how your private customer data should be handled? Contingency plans for breach of data?

  Response:

  Yes.

- Are recovery activities communicated to internal stakeholders and executive management teams?

  Response:

  Yes.

- Do you screen vendors and third parties that have access to cyber control systems?

  Response:

  Yes.

- Have you implemented processes and procedures for identifying and tracking suspicious cyber activity?
  Response:
  Yes.

Standards and Guidelines for Reporting

- Do you have a disaster recovery plan? (The plan itself should not be made public.)

  Response:

  Yes.

- Do you have separate plans for separate business units in the company?

  Response:
  Yes.

- Are you reporting to the necessary state and/or federal agencies in regards to your plan?

  Response:

  Yes

- Are response and recovery plans regularly tested?

  Response:
  Yes.

- Are legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations, understood and managed?

  Response:
  Yes.

- Do you have a list of contacts for cybersecurity information sharing? (i.e. Federal and state emergency management, law enforcement, National Security, or Any others?)

  Response:
  Yes.

- Should the Commission create guidelines or regulations to ensure utilities are properly managing cyber security issues?

  Response:
  No.

- Does your utility use multi-factor identification for system sign-on purposes?

Response:
Yes, for remote access and supported third-party hosted systems.

- Do you keep audit logs for all remote connection protocols?

  Response:
  Yes.

- Do you have the capability to identify and suspend access of users exhibiting unusual computer activity?

  Response:
  Yes.

- Have you worked with, or used resources provided by, a federal agency (e.g., ICS-CERT/CSET, DHS C3 Program, FERC Architectural Reviews) to conduct a cybersecurity assessment?
  Response:
  Yes.