TIDEWATER
UTILITIES, INC.
A Middlesex Water Company Affiliate

September 29, 2023

Electronic Delivery via DelaFile
Crystal Beenick, Commission Secretary
Delaware Public Service Commission
861 Silver Lake Boulevard
Cannon Building, Suite 100
Dover, DE 19904

Re: PSC Docket No. 16-0659
2023 Annual Cybersecurity Filing – Tidewater Utilities, Inc.

Dear Ms. Beenick:

In compliance with Delaware Public Service Commission (PSC) Order No. 8955 in the above referenced docket, Tidewater Utilities, Inc. (Tidewater) respectfully submits that it has reviewed the list of questions pertaining to cybersecurity posted on the PSC's website and finds that no revisions at this time are recommended. Furthermore, Tidewater's responses to the cybersecurity questions are attached hereto.

If you have any questions regarding the changes to this application, please contact me at (302) 747-1325.

`

Sincerely,

Kirsten Higgins

Kirsten Higgins
Vice President, Development & Contract
Administration

Enclosures
cc: A. Bruce O'Connor, Tidewater Utilities, Inc.
Georgia Simpson, Tidewater Utilities, Inc.

PSC Docket No. 16-0659

Tidewater Utilities Inc. Cybersecurity Responses

Planning/Risk Management

1. Question: Is your cybersecurity plan regularly reviewed and audited? If yes, it is audited internally or externally?

   Response: Yes. It is reviewed both internally and externally.

2. Question: How often is the cybersecurity plan reviewed?

   Response: The cybersecurity plan is reviewed at least annually or more frequently as needed.

3. Question: Do you assess vulnerabilities and threats to your system and assets?

   Response: Yes.

4. Question: Do you have a documented risks assessment and management program?

   Response: Yes.

5. Question: Is cybersecurity addressed differently for IT and OT systems?

   Response: Yes.

6. Question: Does your company include in its procurement contract language cybersecurity requirements for IT and OT assets?

   Response: The Company doesn't currently differentiate procurement contract language for cybersecurity requirements between IT and OT. But, the Company is currently assessing the impact of a breakout of that type on its existing contracts.

7. Question: Do you have a documented records retention policy?

   Response: Yes.

Personnel and Policies

8. Question: Are background checks being conducted upon hire for those with access to critical system and assets?

   Response: Yes.

9. Question: Do you provide internal cyber security training for all employees?

   Response: Yes.

10. Question: 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.

11. Question: Are there structural and/or organizational policies and procedures in place that allow the utility to able to address cybersecurity issues?

    Response: Yes.

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

    Response: Yes.

13. Question: How quickly is access terminated for personnel who leave the company?

    Response: Less than 24 hours.

14. Question: Do you have certain employees who are assigned as cybersecurity personnel? Or is the function outsourced?

    Response: Both.

15. Question: 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.

16. Question: Are recovery activities communicated to internal stakeholders and executive and management teams?

    Response: Yes.

17. Question: Do you screen vendors and third parties that have access to cyber control systems?

    Response: Yes.

18. Question: Have you implemented processes and procedures for identifying and tracking suspicious cyber activity?

    Response: Yes.

Standards and Guidelines for Reporting

19. Question: Do you have a disaster recovery plan?

    Response: Yes.

20. Question: Do you have separate plans for separate business units in the company?

    Response: N/A as Tidewater does not have separate business units.

21. Question: Are you reporting to the necessary state and/or federal agencies in regard to your plan?

    Response: Yes.

22. Question: Are response and recovery plans regularly tested?

    Response: Yes.

23. Question: Are legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations, understood and managed?

    Response: Yes.

24. Question: 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.

25. Question: Should the commission create guidelines or regulations to ensure utilities are properly managing cyber security issues?

    Response: No.

26. Question: Does your utility use multi-factor identification for system sign on purposes?

    Response: Yes.

27. Question: Do you keep audit logs for all remote connection protocols?

    Response: Yes.

28. Question: Do you the capability to identify and suspend access of users exhibiting unusual computer activity?

    Response: Yes.

29. Question: 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.