Veolia Water Delaware, Inc.
2000 First State Boulevard
Wilmington, DE 19804
Tel.: (302) 252-3035
Fax: (303) 633-5910

TRANSMITTED ELECTRONICALLY VIA DELAFILE

October 30, 2025

Crystal Beenick
Commission Secretary Delaware Public Service Commission
861 Silver Lake Boulevard
Cannon Building, Suite 100
Dover, Delaware 19904

Re: Delaware Public Service Commission Docket No. 16-0659 - Annual Cybersecurity Questionnaire (2025)

Dear Deputy Director Davis,

In accordance with the Delaware Public Service Commission ("Commission") Order No. 8955 in Docket No. 16-0659 ("Order"), Veolia Water Delaware, Inc. ("VWDE") hereby reports that we have reviewed and updated our responses for 2025 in accordance with the list of questions provided on the Commission's website (i.e., https://depsc.delaware.gov/cybersecurity).

We remain available If you have any further questions regarding this filing.

Best regards,

Larry Finnicum, Regional President - Delaware
Veolia Water Delaware, Inc
Regional President - Delaware

CC

Matt Hartigan, Executive Director, matthew.hartigan@delaware.gov
Patricia Gannon, Senior Regulatory Policy Administrator, patricia.gannon@delaware.gov

Enclosures: Planning/Risk Management

ANNUAL CYBERSECURITY QUESTIONS
PSC Docket No. 16-0659

Planning/Risk Management

Control Question	Response
1. Is your cybersecurity plan regularly reviewed and audited? If yes, is it audited internally or externally?	Yes, internally
2. How often is the cybersecurity plan reviewed?	Annually.
3. Do you assess vulnerabilities and threats to your system and assets?	Yes
4. Do you have a documented risk assessment and management program?	Yes
5. Is Cybersecurity addressed differently for IT and OT systems?	Yes
6. Does your company include in its procurement contract language cybersecurity requirements for It and OT assets?	Yes
7. Do you have a documented records retention policy?	Yes
Personnel and Policies	
8. Are background checks being conducted upon hire for those with access to critical systems and assets?	Yes
9. Do you provide internal cyber security training for all employees?	Yes
10. 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?	Yes
11. Are there structural and/or organizational policies and procedures in place that allow the utility to be able to address cybersecurity issues?	Yes

Control Question	Response
12. Are there managerial and operational controls in place to ensure compliance with the company's cybersecurity policies and procedures?	Yes
13. How quickly is access terminated for personnel who leave the company?	Access is removed at the time of termination.
14. Do you have certain employees who are assigned as cybersecurity personnel? Or is the function outsourced?	Yes, internally and externally supported.
15. Do you have specific practices and policies in place about how your private customer data should be handled? Contingency plans for breach of data?	Yes
16. Are recovery activities communicated to internal stakeholders and executive management teams?	Yes
17. Do you screen vendors and third parties that have access to cyber control systems?	Yes
18. Have you implemented processes and procedures for identifying and tracking suspicious cyber activity?	Yes
19.. Do you have a disaster recovery plan?	Yes
20.. Do you have separate plans for separate business units in the company?	Yes
21. Are you reporting to the necessary state and/or federal agencies in regard to your plan?	Yes
22. Are response and recovery plans regularly tested?	Yes
23. Are legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations, understood and managed?	Yes
24.. Do you have a list of contacts for cybersecurity information sharing? (i.e. Federal	Yes

Control Question	Response
and state emergency management, law enforcement, national security or any others?)	
25. Should the Commission create guidelines or regulations to ensure utilities are properly managing cyber security issues?	No, per Delaware Public Service Commission's decision in this docket, per Order No. 8955, adopted on October 18, 2016
26. Does your utility use multi-factor identification for system sign on purposes?	Yes
27. Do you keep audit logs for all remote connection protocols?	Yes
28. Do you have the capacity to identify and suspend access of users exhibiting unusual computer activity?	Yes
29. Have you worked with, or used resources provided by, a federal agency (e.g., ICSCERT/ CSET, DHS C3 Program, FERC Architectural Reviews) to conduct a cybersecurity assessment?	Yes

Prepared by:
Laura Whitt-Vinyard, CISSP, CISA,CISM, CRISC
Veolia North America, Inc.
Chief Information Security Officer

(on behalf of Veolia Water Delaware, Inc.)