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

TRANSMITTED ELECTRONICALLY

September 29, 2023

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

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

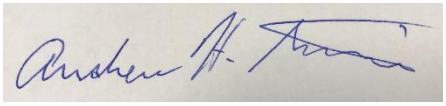
To Deputy Director Davis:

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 in accordance with the list of questions provided on the Commission's website (i.e., https://depsc.delaware.gov/cybersecurity).

Included in VWDE's response are the responses to the additional five (5) questions added to the list of questions by Commission Staff on July 19, 2023, and the revised eleven (11) controls from the previous years' submissions to reflect these recent changes.

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

Best regards,



Andrew H. Stravitz, CISSP, CISM & ITIL
Regional BISO of Municipal Water

CC Malika Davis, Deputy Director, malika.davis@delaware.gov
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, VWDE is subject to both internal controls audits based on COBIT/COSO type frameworks. In addition, the regulated utility is subject to an Independent Systems and Organizational Controls 1 type II ("SOC1 Type II") audit conducted by Ernst & Young.
2. How often is the cybersecurity plan reviewed?	VWDE reviews its cybersecurity plan annually.
3. Do you assess vulnerabilities and threats to your system and assets?	VWDE has a vulnerability management program, which performs monthly scans with commercially supported products. VWDE also is a member of CISA dot Gov, which provides both threat intelligence and independent external vulnerability scanning. VWDE has an enterprise license to Water ISAC for threat intelligence.
4. Do you have a documented risks assessment and management program?	The following process are implemented in our IT Risk & Security Program: • Monthly External Vulnerability Scans are performed. • On demand Internal Vulnerability Scans are performed on new builds. • Pre-implementation Security/Risk Assessments for approved Projects. • Quarterly Payment Card Industry ("PCI") Security Scans for any websites which process credit card data. • Monthly security metrics are provided in a report to management. • All NIST controls are mapped to our policy framework. • A risk register is maintained to capture and track significant risks in accordance with the National Institute of Standards and Technology ("NIST") cybersecurity framework (e.g., 800-53 rev. 5).

	• Annual Tabletop simulation exercise to test incident response procedures.
Personnel and Policies	
5. Are background checks being conducted upon hire for those with access to critical systems and assets?	Yes, VWDE's standard human resource onboarding policy includes background checks.
6. Do you provide internal cyber security training for all employees?	Yes, all employees are subject to monthly cyber awareness training on various cybersecurity topics. Additionally, VWDE conducts internal quarterly phishing campaigns.
7. 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?	VWDE is in the process of rebranding (due to the merger), the specialized OT training curriculum. Employees at the Delaware Utility are required to attend specialized OT/SCADA security training on an annual basis.
8. Are there structural and/or organizational policies and procedures in place that allow the utility to be able to address cybersecurity issues?	Yes, VWDE has an information security policy framework based on NIST 800-53, NIST 800-82, ISA/IEC 62443 and NIST framework for improving critical infrastructure cybersecurity. There are both an Incident Response ("IR") Policy and IR Procedures, which are tested at least annually in a tabletop exercise for the Regulated Utility.
9. Are there managerial and operational controls in place to ensure compliance with the company's cybersecurity policies and procedures?	Yes, our cybersecurity policy framework has been approved by the Veolia North America's corporate Policy Review Committee ("PRC") and published on the Veolia North America intranet site for all company personnel to view and follow. All cybersecurity policies are reviewed on an annual basis in light of changes to industry standards and applicable cybersecurity laws. The respective IT teams conduct several self-assessments on an annual basis in alignment with internal policies and procedures.

10. How quickly is access terminated for personnel who leave the company?	Access is terminated at the time of termination.
11. Do you have certain employees who are assigned as cybersecurity personnel? Or is the function outsourced?	Yes, there is a dedicated North America Chief Information Security Officer who reports to the Chief Information Officer. The Business Information Security Officer embedded in the Regulated Water / Utility is CISSP, CISM and ITIL certified. • VWDE has a dedicated IT Risk & Security team in place. • VWDE uses an external Managed Services Security Provider ("MSSP") to provide 24/7 Security Monitoring via Security Intrusion Event Management ("SIEM").
12. 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, there is a dedicated "Privacy Counsel" who is responsible for training all personnel, and provides training for the handling of PII data. The annual privacy training covers escalation procedures. Our incident response procedures provide detailed processes for escalation, including regulatory and law enforcement contacts.
13. Are recovery activities communicated to internal stakeholders and executive management teams?	Yes, VWDE performs annual tabletop simulation exercises to test cybersecurity resiliency, which include stakeholders and executives.
14. Do you screen vendors and third parties that have access to cyber control systems?	Yes, VWDE has a vendor risk management ("VRM") program in place.
15. Do you have a disaster recovery plan?	Yes, VWDE's Environmental Health and Safety Department mandates a disaster recovery plan covering all utility sites.
16. Do you have separate plans for separate business units in the company?	Yes, all business units ("BU") are required to have an updated recovery plan.
17. Are you reporting to the necessary state and/or federal agencies in regard to your plan?	Yes, we report to both state and federal levels as required by law.
18. Are response and recovery plans regularly tested?	Yes, VWDE annually tests its recovery plans via tabletop simulation exercises.

19. Are legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations, understood and managed?	Yes, Veolia North America, including VWDE, conducts specialized data privacy training for all employees, as well as monthly security awareness training that includes data privacy modules.
20. 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?)	Yes, Veolia North America and its subsidiaries, including VWDE, has an appendix embedded in the "Incident Response Procedures" which covers both state and federal emergency contacts for both regulatory and law enforcement.
21. Should the Commission create guidelines or regulations to ensure utilities are properly managing cyber security issues?	VWDE has proactively used the Environmental Protection Agency's cybersecurity assessment tool to measure our control compliance in the OT/ICS/SCADA environments. As such, we do not believe a
22. Does your utility use multi-factor identification for system sign on purposes?	Yes, multi-factor authentication across VWDE systems is enabled as per our NIST based "Identification and Authentication Policy."
23. Do you keep audit logs for all remote connection protocols?	Yes, all security logs are centrally ingested in our SIEM system.
24. Do you have the capacity to identify and suspend access of users exhibiting unusual computer activity?	Yes, we run Endpoint Detection and Response ("EDR") with centralized monitoring.
25. Is cybersecurity addressed differently for IT and OT systems?	Yes, the approach is specific to each area.
26. Does your company include in its procurement contract language cybersecurity requirements for IT and OT assets?	Yes.
27. Do you have a documented records retention policy?	Yes.
28. Have you implemented processes and procedures for identifying and tracking suspicious cyber activity?	Yes, we have Incident Response Procedures and Security Operations Center (SOC) runbooks.
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, we participated in tabletop exercises which included resources from the DHS, FBI, State Agencies and Waster ISAC. VWDE leverages available resources from CISA dot Gov.

Prepared by:
Andrew H. Stravitz, CISSP, CISM & ITIL
Veolia North America BISO