October 22, 2022

Eric F. Mease, Public Utilities Analyst I
Delaware Public Service Commission
861 Silver Lake Boulevard
Cannon Building, Suite 100
Dover, Delaware 19904

Re: PSC Docket No. 16-0659; Cybersecurity Annual Questionnaire

Dear Mr. Mease:

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

If you have any further questions regarding this filing, I can be reached at +1 (201) 494-5872.

Best regards,

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

Enclosure

ANNUAL CYBERSECURITY QUESTIONS
PSC Docket No. 16-0659

<u>Planning/Risk Management</u>

Is your cybersecurity plan regularly reviewed and audited?	Yes
Internally or externally?	Both

Has your plan been reviewed recently?	Yes
If not, how often is it reviewed?	Annually

Do you assess vulnerabilities to your system and assets?   Yes

- Veolia has vulnerability reporting agents deployed on laptops/desktops and perform scheduled scans against the server environment.

Do you assess threats to your system and assets?   Yes

Do you prioritize risks?   Yes
And what processes do you use?

The following process are implemented in our IT Risk & Security Program:
- Quarterly External Vulnerability Scans are performed.
- On demand Internal Vulnerability Scans are performed on new builds.
- Pre-implementation Security/Risk Assessments for approved Projects.
- Quarterly PCI Security Scans for any websites which process credit card data.
- Documenting process outcomes in the IT Risk and Security Register.
- Monthly security metrics are provided in a report to management.
- An IT-GRC (governance risk & compliance) tool is used to map all NIST controls to our policy framework.
- A risk register is maintained to capture and track significant risks.
- Tabletop simulation exercise to test incident response procedures.

<u>Personnel and Policies</u>

Are background checks being conducted upon hire?   Yes

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

- Veolia regularly trains employees with a variety of "Security Awareness" training including phishing campaigns and online CBT courses.

Do you provide enhanced internal cyber security training for those that are actually in the utilities operating network?   Yes

Are there structural and/or organizational policies and procedures in place that allows the utility to able to address or think through these things (cybersecurity issues)? Yes

- Veolia has an information security policy framework based on NIST 800-53.

Are there managerial and operational controls in place? Yes

How quickly is access to those personnel who quit/fired eliminated? At time of termination

Do you have certain employees that are assigned as cybersecurity personnel? Yes
Or outsourced? Yes

- Veolia has a dedicated IT Risk & Security team in place.
- Veolia uses external MSSP to provide 24/7 Security Monitoring via SIEM.

Do you have specific practices and policies in place about how your private customer data should be handled? Yes

- Veolia engages an independent auditor to produce a SOC1 Type I report on the customer care and billing system on an annual basis.

Contingency plans for breach of data? Yes

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

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

- Veolia has a vendor risk management (VRM) program in place.

Standards and Guidelines for Reporting

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

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

Are you reporting to the necessary agencies in regards to your plan? Yes

Are response and recovery plans regularly tested? As required

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

- Membership to Water ISAC Security & Resilience Updates.

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

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

- Veolia is available to participate and comment.

- Veolia provides a high level of cyber security coverage, both for systems and customer data, and will strive to comply with any guidelines or regulations set fourth by the regulators for the locations in which we operate.

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

- Our NIST based policy mandates any remote connectivity over a public network uses MFA.

Do you keep audit logs for all remote connection protocols?...Yes

- All cybersecurity events are collected in a central SIEM

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

- Veolia monitors for anomaly behaviors and has EDR isolation capabilities.

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