CHESAPEAKE UTILITIES

September 24, 2021

Ms. Donna Nickerson, Secretary
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 Ms. Nickerson:

In accordance with PSC Order No. 8955 in Docket No. 16-0659 (Oct. 18, 2016), Chesapeake Utilities Corporation ("Chesapeake") hereby reports that it has reviewed the previously provided list of cybersecurity questions posted on the Commission website and acknowledges that three additional questions were added to the list in April 2021. Attached hereto is a copy of the cybersecurity questions and Chesapeake's responses.

If you have any questions with respect to the above, please do not hesitate to contact me at 302.734.6727.

Sincerely,

/s/ Marie E. Kozel
Marie E. Kozel, Regulatory Analyst III

Enclosure

Cc: Andrew Slater, Public Advocate (via email)
Regina A. Iorii, Esq., Deputy Attorney General (via email)
Andrea Maucher, Public Utilities Analyst (via email)
Matthew Hartigan, Executive Director (via email)
Thomas Walsh, Esq., Deputy Attorney General (via email)
Malika Davis, Regulatory Policy Administrator (via email)

Annual Cybersecurity Questions

PSC Docket No. 16-0659

Planning/Risk Management

1. Is your cybersecurity plan regularly reviewed and audited? Internally or externally? **Yes, the Company's cybersecurity plan is regularly reviewed and audited both internally and externally.**

2. Has your plan been reviewed recently? If not how often is it reviewed? **Yes, the plan has been reviewed recently.**

3. Do you assess vulnerabilities to your system and assets? **The company utilizes multiple National Institute of Standards and Technology ("NIST") approved vulnerability management solutions and partners with third-parties to perform penetration testing.**

4. Do you assess threats to your system and assets? **The company utilizes multiple NIST approved vulnerability management solutions and partners with third-parties to perform penetration testing**.

5. Do you prioritize risks and what processes do you use? **The Company's Board maintains an oversight role with respect to risk management and is ultimately responsible for ensuring that the Company's risk management framework is sufficient given the Company's business activities. Risks are considered in virtually every business decision and process. The Company's risk management framework includes the following components: risk identification, risk assessment, risk management and monitoring, and communication.**

Personnel and Policies

6. Are background checks being conducted upon hire? **Routine and customary background checks are performed for potential new hires.**

7. Do you provide internal cyber security training for all employees? **Employees receive periodic cybersecurity awareness education.**

8. Do you provide enhanced internal cyber security training for those that are actually in the utilities operating network? **Employees receive periodic cybersecurity awareness education. Certain employees involved with the Company's operating network also actively participate in the Company's internal cybersecurity committees.**

9. 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)? **In 2015, the Company took the following actions, among others, to further protect our business from potential cyber or physical security risk: i) added additional key members to our team, ii) added new security mechanisms to further protect key assets, iii) developed strong relationships among the private sector and government agencies, iv) participated in an industry specific symposium, v) established several security teams comprised of select members of management that collectively review best practices, recent security events, and respond to security inquires, and vi) adopted several policies, controls and procedures to further enhance our security posture.**

10. Are there managerial and operational controls in place? **In 2015, the Company took the following actions, among others, to further protect our business from potential cyber or physical security risk: i) added additional key members to our team, ii) added new security mechanisms to further protect key assets, iii) developed strong relationships among the private sector and government agencies, iv) participated in an industry specific symposium, v) established several security teams comprised of select members of management that collectively review best practices, recent security events, and respond to security inquires, and vi) adopted several policies, controls and procedures to further enhance our security posture.**

11. How quickly is access to those personnel who quit/fired eliminated? **The Company has a process in place that ensures prompt notification to appropriate individuals when changes to access is required.**

12. Do you have certain employees that are assigned as cybersecurity personnel? **Or outsourced? The company has dedicated cybersecurity personnel on staff. In 2019, the company contracted with a Managed Security Service Provider (MSSP) to provide 24/7 monitor, detect and respond (MDR) capabilities.**

13. Do you have specific practices and policies in place about how your private customer data should be handled? Contingency plans for breach of data? **The Company has several security teams comprised of select members of management that collectively review best practices, recent security events, and respond to security inquiries. The Company has developed strong relationships among the private sector and government agencies. The Company also engages third-parties when appropriate and necessary.**

14. Are recovery activities communicated to internal stakeholders and executive and management teams? **The Company has open lines of communication with all relevant internal stakeholders, executive and management teams.**

15. Do you screen vendors and third parties that have access to cyber control systems? **The Company has a process in place to vet vendors and third parties.**

Standards and Guidelines for Reporting

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

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

18. Are you reporting to the necessary agencies in regards to your plan? **Yes, as necessary and appropriate.**

19. Are response and recovery plans regularly tested? **Plans are reviewed and tested.**

20. Are legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations, understood and managed? **The Company's security teams remain abreast of legal and regulatory requirements and periodically receive presentations from third-parties.**

21. 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?) **The Company has developed strong relationships among the private sector and government agencies. In addition, members of the Company's security teams hold an active security clearance.**

22. Should the Commission create guidelines or regulations to ensure utilities are properly managing cyber security issues? **The Company currently provides cyber related disclosures in its Form 10-K and Proxy Statements filed with the Securities and Exchange Commission. The Company will continue to work with the Commission in its cyber related initiatives.**

23. Does your utility use multi-factor identification for system sign on purposes? **Yes, the company utilizes multi-factor authentication.**

24. Do you keep audit logs for all remote connection protocols? **All logs are stored with our Managed Security Service.**

25. Do you have the capacity to identify and suspend access of users exhibiting unusual computer activity? **Yes, the company utilizes an advanced endpoint and detection response (EDR) solution which can isolate assets.**