CHESAPEAKE
UTILITIES CORPORATION

September 27, 2023

Ms. Crystal Beenick, 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. Beenick:

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 list of questions pertaining to cybersecurity posted on the Commission website. Attached, please find Chesapeake's updated responses to those questions.

Should you have any questions with regard to this submission, please contact me at the number or email listed below, or Marie Kozel at 302.734.6727 or mkozel@chpk.com.
hem

/s/ Lindsay Orr Foy
Lindsay Orr Foy (No. 5321)
AVP, Associate General Counsel
Chesapeake Utilities Corporation
114 Sandhill Drive, Suite 105
Middletown, DE 19709
Phone: (302) 314-7026
Email: LFoy@chpk.com

Attachments

Cc: Matthew Hartigan, Executive Director (via email)
Malika Davis, Deputy Director (via email)
Sommer Poppe, Esq., Deputy Attorney General (via email)
Samantha Hajek, Ombudsman (via email)
Ruth Ann Price, Public Advocate (via email)
Regina A. Iorii, Esq., Deputy Attorney General (via email)
Andrea Maucher, Public Utilities Analyst (via email)

Planning/Risk Management

- Is your cybersecurity plan regularly reviewed and audited? If yes, is it audited internally or externally? **Yes, the Company's cybersecurity plan is regularly reviewed and audited both internally and externally.**
- How often is the cybersecurity plan reviewed? **The plan is reviewed annually.**
- Do you assess vulnerabilities and threats 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 regular penetration testing.**
- Do you have a documented risks assessment and management program? **The company utilizes multiple National Institute of Standards and Technology ("NIST") approved vulnerability management solutions and partners with third-parties to perform regular penetration testing.**
- Is cybersecurity addressed differently for IT and OT systems? **OT is protected via dedicated security components, EDR and resides in a separate domain.**
- Does your company include in its procurement contract language cybersecurity requirements for IT and OT assets? **The Company has a Third Party Risk program in place which assesses and *risk ranks* current and prospective vendors. Risk Treatment is applied when appropriate. Vendors must meet minimum Cybersecurity related standards in order to be eligible for access to the company's data and/or environment. Administrative controls include master service agreements with security, privacy and confidentiality provisions.**
- Do you have a documented records retention policy? **The company operates off a formal records retention schedule which dictates the appropriate schedule based on the data type.**

Personnel and Policies

- Are background checks being conducted upon hire for those with access to critical systems and assets? **Routine and customary background checks are performed for potential new hires.**

- Do you provide internal cyber security training for all employees? **Employees receive weekly cyber security testing.**

- 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? **Employees receive weekly cyber security training/testing. Certain employees involved with the Company's Operational Technology (OT) network receive specialized (quarterly) training.**

- Are there structural and/or organizational policies and procedures in place that allow the utility to be able to address cybersecurity issues? **The company has a comprehensive Cybersecurity program which consists of:**

    - **Vulnerability Management**
    - **Adversary Emulation/Red Team**
    - **Digital Forensics and Incident Response**
    - **Security Awareness**
    - **Third Party Risk**
    - **Offensive Security Measures (Threat Hunting)**
    - **Industry leading controls (DLP, EDR, NGFWs, MFA)**
    - **Cyber Threat Intelligence (CTI)**

  Several committees have also been established to review and assess enterprise level cyber risk and to establish and implement policies, controls and procedures. Several members of the Cybersecurity team hold an active DHS/TSA security clearance. MITRE's ATT&CK framework is leveraged for the sharing and ingestion of threat level data.

- Are there managerial and operational controls in place to ensure compliance with the company's cybersecurity policies and procedures? **The company has a comprehensive Cybersecurity program which consists of:**

    - **Vulnerability Management**
    - **Adversary Emulation/Red Team**
    - **Digital Forensics and Incident Response**
    - **Security Awareness**
    - **Third Party Risk**
    - **Offensive Security Measures (Threat Hunting)**
    - **Industry leading controls (DLP, EDR, NGFWs, MFA)**
    - **Cyber Threat Intelligence (CTI)**

  Several committees have also been established to review and assess enterprise level cyber risk and to establish and implement policies, controls and procedures. Several members of the Cybersecurity team hold an active DHS/TSA security clearance. MITRE's ATT&CK framework is leveraged for the sharing and ingestion of threat level data.

- How quickly is access terminated for personnel who leave the company? **The Company operates based on an offboarding policy and has a process in place that ensures prompt notification to appropriate individuals during any access changes.**

- Do you have certain employees who are assigned as cybersecurity personnel? Or is the function outsourced? **The company has a dedicated Cybersecurity team focused on DFIR, vulnerability management, third party risk and security awareness. Additionally, an MDR is used for 24/7 coverage.**

- 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 operates**

based on a Data Classification and Data Protection policy. This policy dictates the appropriate controls and labeling which should be in place for all data types, including private customer data. Additionally, the company has a Critical Incident Response Team (CIRT) which convenes during any potential or confirmed cyber or privacy related incident.

- Are recovery activities communicated to internal stakeholders and executive management teams? **The Company has open lines of communication with all relevant internal stakeholders, executive and management teams.**
- Do you screen vendors and third parties that have access to cyber control systems? **The Company has a Third Party Risk program in place which assesses and *risk ranks* current and prospective vendors. Risk Treatment is applied when appropriate. Vendors must meet minimum Cybersecurity related standards in order to be eligible for access to the company's data and/or environment.**
- Have you implemented processes and procedures for identifying and tracking suspicious cyber activity? **In addition to continuous monitoring, the company utilizes state of the art technology, performs weekly adversary emulation, weekly threat hunting and holds daily Cyber Operations meetings to review relevant alerts and intel.**

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 state and/or federal agencies in regards to your plan? **Yes, as necessary and appropriate.**
- Are response and recovery plans regularly tested? **Plans are reviewed and tested.**
- 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.**
- 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, including membership in several ISACs. In addition, members of the Company's security team hold an active security clearance.**
- 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.**
- Does your utility use multi-factor identification for system sign-on purposes? **Yes**

- Do you keep audit logs for all remote connection protocols? **All logs are stored with our Managed Security Service and on the company's internal SIEM.**
- Do you have the capability 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.**
- 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? **The company interfaces with DHS as necessary for malware sample submission and information sharing. Several members of the Cyber team hold active security clearances with DHS/TSA.**