ORDER NO. 88827

IN THE MATTER OF CYBER-SECURITY REPORTING OF MARYLAND UTILITIES	* * * * * * * *	BEFORE THE PUBLIC SERVICE COMMISSION OF MARYLAND _____ Case No. 9492 _____

Issued: September 11, 2018

NOTICE OF INITIATING A PROCEEDING AND REQUEST FOR COMMENTS

To: Service Lists for Case Nos. 9207, 9208, 9294, and 9378 and Interested Persons

On April 6, 2018, the Final Report of the Cyber-Security Reporting Work Group ("CSRWG") ("Final Report") was filed in compliance with Commission Order No. 88499 in Case Nos. 9207 and 9208. The Final Report made recommendations addressing cyber-security definitions, reporting applicability, reporting agenda, reporting certification, briefing parties, briefing frequency, breach reporting, and information handling protocols. The Commission hereby initiates a new docketed proceeding, Case No.9492, and requests comments regarding the Final Report and recommendations contained therein, with the modification to cyber-security reporting discussed below.

Procedural History

In Case Nos. 9207 and 9208, Baltimore Gas and Electric Company ("BGE"), Potomac Electric Power Company ("Pepco"), and Delmarva Power & Light Company

("Delmarva") (collectively, "the Exelon Companies") requested authorization to deploy their Advanced Metering Infrastructure ("AMI") initiatives. In order to identify, monitor, and remediate risks to the confidentiality, integrity, and availability of AMI systems and data, the Exelon Companies filed a Revised Cyber-Security Reporting Process, as well as individual cyber-security plans.[1] Subsequent to these filings, the Exelon Companies consulted with the smart grid working group to develop a methodology for reporting cyber-security issues to the Commission. On June 21, 2013, the Commission issued Order No. 85680, approving the Exelon Companies' cyber-security plans.

Since the issuance of Order No. 85680, metering infrastructure has continued to advance and cyber-security issues have become increasingly complex. Nevertheless, Maryland utilities are not currently subject to uniform cyber-security reporting requirements. For example, Choptank Electric Cooperative, Inc. ("Choptank") filed notice of the implementation of its AMI system, which the Commission approved on March 27, 2015.[2] However, Choptank is not currently required to file an AMI cyber-security plan or cyber-security reporting plan. On January 23, 2017, Southern Maryland Electric Cooperative, Inc. ("SMECO") filed its proposed AMI Metrics Reporting Plan and its proposed Smart Grid Cyber Security Plan.[3] The Commission approved those plans on February 24, 2017. SMECO does not currently have any periodic cyber-security reporting requirements. Likewise, Washington Gas Light Company ("WGL") is not

[1] Case Nos. 9207 and 9208, MailLog No. 145602.

[2] Case No. 9378, *In the Matter of Choptank Electric Cooperative, Inc.'s Implementation of Advanced Metering Infrastructure System;* MailLog No. 165846.

[3] Case No. 9294, *In the Matter of the Request of Southern Maryland Electric Cooperative, Inc. for Authorization to Proceed with Implementation of an Advanced Metering Infrastructure System.*

currently required to file a cyber-security plan or related cyber-security reporting plan. The Potomac Edison Company has not announced any plans to pursue a Smart Grid Initiative, and it accordingly is not subject to periodic cyber-security reporting requirements. However, it provided a confidential briefing on its cyber-security initiatives to the Commission in 2016.[4]

On December 11, 2017, the Commission issued Order No. 88499, which provides guidance related to a potential framework for future cyber-security reporting. The Order observed that because additional Maryland utilities have undertaken smart grid infrastructure deployments since the issuance of Order No. 85680, extension of the existing cyber-security reporting plan requirements should be considered.[5] Accordingly, the Commission directed its Technical Staff to convene a work group for purposes of recommending a framework for future cyber-security reporting. The Order further directed that the revised reporting framework should address cyber-security threats to more than just the smart grid systems, but also consider the application of cyber-security to information technology ("IT") systems, operations technology ("OT"), and control systems.[6]

On April 6, 2018, after holding several meetings, the CSRWG provided its Final Report.[7] The Report provides consensus recommendations on (i) cyber-security definitions, (ii) Maryland utilities periodic cyber-security reporting applicability,

[4] WGL and Columbia have also provided confidential briefings on their respective cyber-security initiatives.

[5] Order No. 88499 at 2.

[6] Order No. 88499 at 2-3.

[7] The CSRWG consisted of representatives from BGE, Choptank, Exelon, Office of People's Counsel, Potomac Edison / FirstEnergy, Pepco Holding, Inc. (PHI), Technical Staff of the Commission, SMECO, and WGL.

(iii) cyber-security reporting agenda, (iv) cyber-security reporting certification, (v) cyber-security briefing parties, (vi) cyber-security report briefing frequency, (vii) cyber-security breach reporting, and (viii) cyber-security briefing information handling protocols.

Discussion

The Commission finds that it is appropriate to establish a new utility cyber-security reporting framework in Maryland that creates a uniform set of reporting requirements for Maryland utilities of a certain size, not just for the Exelon Companies. The Commission seeks comments on the recommendations of the CSRWG regarding the elements of a new utility cyber-security reporting framework, as discussed below.

First, the CSRWG proposed several definitions that would be applicable to an expanded cyber-security reporting framework in Maryland. Specifically, the workgroup proposed definitions for Information Technology System,[8] Operations Technology System,[9] Smart Grid System,[10] and Security Breach.[11] The Commission proposes to accept these definitions for use in future cyber-security reports.

Second, the CSRWG recommended that the requirement to periodically file cyber-security reports be applicable broadly to "any Maryland electric, gas, or water

[8] The CSRWG proposed that Information Technology System be defined as "a utility business process system or network that contains personally identifiable customer information."

[9] The CSRWG proposed that an Operations Technology System be defined as "a system or network that monitors or controls electric, gas or water system infrastructure used for utility operations."

[10] The CSRWG proposed that a Smart Grid System be defined as "a system or network that enables a utility to gather and store personally identifiable customer information from customer devices or allows for the control of customer devices."

[11] The CSRWG proposed that a Security Breach be defined as "any unauthorized act that has been confirmed to result in access to, acquisition, control, destruction, disclosure, or modification of a utility's IT Systems, OT Systems or Smart Grid Systems."

utility exceeding a customer count of 40,000 customers." The workgroup chose the 40,000 customer threshold to include Choptank, but to exclude smaller Maryland cooperative and municipal utilities, for which the reporting obligation could be burdensome. The CSRWG also expanded the reporting requirement to include gas and water utilities, given that cyber-security threats are not confined to electric utilities.

The Commission proposes that cyber-security reporting requirements should be applicable to all Maryland utilities of a certain size, including gas and water, and should not be confined to electric utilities, and seeks comment thereon. In that regard, the Commission notes that WGL was an active participant in the CSRWG and has agreed to adopt the CSRWG recommended periodic cyber-security reporting framework.[12] The Commission proposes to lower the utility customer threshold from 40,000 to 30,000 customers. This modification would extend the reporting requirement to Columbia Gas of Maryland, Inc., which provides retail gas distribution services to approximately 33,000 customers in Maryland. The Commission believes that it would benefit from receiving cyber-security reports from utilities of this size including all Maryland electric, gas, and water utilities exceeding a customer count of 30,000 customers and seeks comment thereon.

Third, the CSRWG recommended against an overly proscriptive list of standardized questions for periodic cyber-security reporting. The CSRWG observed that in January 2017, the National Association of Regulatory Utility Commissioners ("NARUC") Research Lab published "Cybersecurity Primer for State Utility Regulators

[12] CSRWG Final Report at 7.

(Version 3.0)" ("Primer"),[13] which contains a detailed list of 108 sample questions.[14] However, the CSRWG cautioned that some of the questions required the divulging of highly sensitive information, and that other questions may not be appropriate for every scenario or region. The CSRWG therefore recommended that each utility report cyber-security issues pursuant to the following ten categories: (i) Cyber-security Plan Overview; (ii) Cyber-security Standards Adopted; (iii) Reporting Cyber Incidents; (iv) Partnerships for Information Sharing, Planning, and Situational Awareness; (v) Procurement Practices to Manage Cyber-security Risks from Vendors; (vi) Personnel and Policies on Hiring, Training, and Separation to Manage Cyber-security Risks; (vii) Risk Management Process to Assess and Prioritize Cyber-security Risk; (viii) Implementation of Cyber-security Strategies; (ix) Response and Recovery to Cyber Incidents; and (x) Cyber-security Process. The Commission proposes that the ten-point standardized cyber-security report agenda developed by the CSRWG may be appropriate at this time, and seeks comments thereon. As provided in the Final Report, the Commission proposes to ask additional questions at cyber-security briefings, including questions contained in the Primer, where the provided information is insufficient.[15]

Fourth, the CSRWG recommended that self-certification be accepted by the Commission as an alternative to the engagement of an independent cyber-security consulting firm ("CCF") for certification of periodic cyber-security reporting. In Order

[13] The Primer may be located at the following address: https://pubs.naruc.org/pub/66D17AE4-A46F-B543-58EF-68B04E8B180F.

[14] See Appendix 2 to CSRWG Final Report at 15 – 21.

[15] CSRWG Final Report at 8.

No. 85680, applicable to the Exelon Companies and related to AMI, the Commission required that a CCF be engaged for independent certification of cyber-security reports. Nevertheless, Order No. 88499 suspended the CCF directive, recognizing that hiring a CCF could present significant costs and that "an acceptable alternative would be the certification of the accuracy of the briefing materials by an appropriate and authorized company officer."[16] During their meetings, the CSRWG developed instructions and a template for utility self-certification. [17] The CSRWG Final Report also concluded that "the cost involved in securing a CCF for an expanded scope beyond AMI into IT Systems and OT Systems would make this very expensive and time consuming for the utilities."[18] The Commission seeks comments on this recommendation.

Fifth, the CSRWG proposed that cyber-security briefing parties be comprised of the same members that are designated as Cyber-Security Reporting Authorized Representatives ("CSRARs"). CSRARs have the authority to receive confidential cyber-security briefings or confidential cyber-security breach information, not requiring a government security clearance. The CSRWG proposed that the cyber-security briefing parties be (i) the Commissioners, (ii) the Commission's Executive Secretary, (iii) the Commission's Executive Director, (iv) the Commission's General Counsel, (v) the Commission's Senior Advisors, (vi) the Commission's Chief Engineer, (vii) an Office of People's Counsel designated representative, and (viii) alternates or others as invited by the Commission. The Commission proposes that the CSRWG's proposed list of cyber-

[16] Order No. 88499 at 3.

[17] CSRWG Final Report at Appendix 3, page 22.

[18] CSRWG Final Report at 8.

security briefing parties may be reasonable, and seeks comment thereon.

Sixth, the CSRWG recommended that cyber-security reporting frequency should align with the three-year audit schedules established by the North American Electric Reliability Corporation's ("NERC") Critical Infrastructure Protection ("CIP"). NERC has determined that a three-year audit cycle is appropriate for Transmission Owners, and the CSRWG likewise proposed a three-year audit cycle for Commission's review. The CSRWG also recommended staggering the cyber-security briefing engagements according to the following schedule:

	First Maryland Cyber-Security Briefing under New Protocols	**Second Cycle Maryland Cyber-Security Briefing under New Protocols**
BGE	2018	2021
Choptank	2019	2022
Potomac Edison	2020	2023
Pepco and Delmarva	2019	2022
SMECO	2020	2023
WGL	2018	2021

The Commission proposes that the periodic cyber-security reporting schedule proposed by the CSRWG may be reasonable, and seeks comments thereon. The Commission also proposes (consistent with the CSRWG's recommendation at 10) that the Commission's Chief Engineer act as a liaison with each utility's authorized

representative as the utility's cyber-security report briefing becomes due to confirm logistics such as available dates and times, desired duration, and location of briefings.

Seventh, the CSRWG recommended that cyber-security breach reporting requirements apply to *all* Maryland electric, gas, and water companies regulated by the Commission, regardless of their number of customers. The CSRWG made this recommendation "due to the potential safety, reliability, financial, and customer privacy impacts of cyber-security breaches."[19] The Commission proposes that this recommendation may be reasonable, and seeks comments thereon. Additionally, the Commission notes that the CSRWG recommended that cyber-security breaches that impact IT, OT, or Smart Grid Systems should be reported verbally to the Commission's Chief Engineer or designated alternate within one business day of confirmation, or sooner, where public release of breach details through media outlets is imminent, unless contrary to law or the recommendation of law enforcement to avoid compromising an investigation.[20] The Chief Engineer (or designated alternate) could act as the point of contact ("POC") after internal Commission discussion. Utilities should report updates to the POC after the initial report if material changes occur or are discovered regarding the breach. The POC would then inform the CSRARs either verbally, by teleconference using the Commission's standing conference bridge, or by the use of the State of Maryland's internal software tool to protect and encrypt email. As detailed in the Final Report, breached utilities should also contact the Department of Homeland Security National Cyber-security and Communications Integration Center, and Maryland Fusion

[19] CSRWG Final Report at 11.

[20] Federal regulations prohibit utilities from divulging Critical Electric Infrastructure Information as defined in 18 C.F.R. 388.113.

Center, as well as the Maryland Attorney General's Office, where appropriate.[21] The Commission seeks comment on these suggestions of the CSRWG Report.

Eighth, the CSRWG recommended that certain cyber-security briefing information handling protocols be established to protect sensitive information. Specifically, the CSRWG recommended that any cyber-security briefing materials reviewed at periodic briefings with the Commission be collected at the end of the meeting. Additionally, any actions requested by the Commission to the utility would be recorded and retained by the utility. The utility would retain and safeguard these briefing materials and recorded actions for a period no less than five years, for potential review at a later date by the Commission or CSRARs. Finally, the CSRWG recommended that no detailed information requiring a government security clearance should be communicated to CSRARs who do not have appropriate clearance. The Commission proposes that the CSRWG protocols represent a good starting point to protect sensitive information, and seeks comments thereon.[22]

Written comments on the Final Report and the proposals herein shall be filed by October 10, 2018. An original and seventeen copies of the comments, together with an electronic copy, shall be addressed to Terry J. Romine, Executive Secretary, Maryland Public Service Commission, William Donald Schaefer Tower, 6 St. Paul Street,

[21] The Commercial Law Article of the Maryland Code § 14-3503(a) requires Maryland companies to protect personal information from unauthorized access, use, modification, or disclosure. Likewise, § 14-3504(h) requires that certain types of personally identifiable data breaches be reported to the Maryland Attorney General's Office.

[22] Although the CSRWG developed a set of proposed COMAR regulations in Appendix 4 to the Final Report, it recommended against adopting them currently. The Commission agrees that it would be helpful to gain additional experience with the new cyber-security reporting framework before promulgating new regulations.

16th Floor, Baltimore, Maryland 21201. Five of the paper copies shall be three-hole punched. The Commission encourages the use of the Commission's e-File system for submission of the electronic coy of the filing. Details of the e-File system are on the Commission's web page, www.psc.state.md.us (Online Services).

By Direction of the Commission,

/s/ Terry J. Romine

Terry J. Romine
Executive Secretary