ORDER NO. 89015

IN THE MATTER OF CYBER-SECURITY REPORTING OF MARYLAND UTILITIES	*	BEFORE THE PUBLIC SERVICE COMMISSION OF MARYLAND
	*	
	*	CASE NO. 9492

Issue Date: February 4, 2019

On September 11, 2018, the Maryland Public Service Commission ("the Commission") issued a Notice of Initiating a Proceeding and Request for Comments regarding the Final Report of the Cyber-Security Reporting Work Group ("CSRWG") ("Final Report").[1] The Final Report provided consensus recommendations on (i) cyber-security definitions, (ii) Maryland utilities periodic cyber-security reporting applicability, (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.

Timely comments were filed by Commission Staff ("Staff"),[2] the Office of People's Counsel ("OPC"),[3] Washington Gas Light Company ("WGL"),[4] Baltimore Gas and Electric Company, Delmarva Power & Light Company, and

[1] The Final Report can be found at ML 219883.
[2] ML 222443
[3] ML 222445
[4] ML 222440

Potomac Electric Power Company (collectively "the Exelon Utilities"),[5] The Potomac Edison Company ("Potomac Edison"),[6] and Columbia Gas of Maryland, Inc. ("Columbia").[7] In general, all of the filed comments supported the consensus recommendations in the Final Report, although a few recommended minor changes, on which the Commission makes determinations herein.[8]

Discussion

OPC, Potomac Edison, and WGL all support the consensus recommendations in the Final Report as modified by the Commission in the Request for Comments.

Staff and the Exelon Utilities both note that the proposed schedule for reporting/briefings contained in the Final Report needs to be modified due to the date of issuance of this Order. The Commission finds these recommendations to be correct and therefore schedules the first briefings to take place in the second half of 2019.[9]

The Exelon Utilities also suggest that the CSRWG be reconstituted to discuss any changes to the cyber-security requirements contained in this Order if and when changes or additions are needed. In light of the good work of the CSRWG in reaching consensus in their proposals to date, the Commission finds this recommendation reasonable and adopts it.

Columbia suggests that the definition of Information Technology ("IT") System be broadened. Columbia notes that an IT system is "more than a system or network that

[5] ML 222437
[6] ML 222434
[7] ML 222449
[8] The Commission finds that additional experience with the new cyber-security reporting protocols will be helpful before considering promulgating regulations.
[9] The Exelon Utilities request the cyber-security reporting requirements take effect 180 days after this Order. The Commission declines to adopt this suggestion as it would delay the requirement for utilities to report cyber-security breaches.

contains personally identifiable customer information (PII)."[10] The Commission finds that limiting the definition of IT System to systems containing "personally identifiable customer information" would exclude sensitive electronic systems such as internal email in which malware may be planted. Therefore, the Commission adopts Columbia's broadened definition for IT System. Columbia also requests that the utilities be notified of what additional questions may be asked at cyber-security briefings 90 days in advance of the briefing. The Commission finds that the briefings should involve some exchange among the attendees, and this proposal would be too limiting. This suggestion is denied. Finally, Columbia suggests that Cyber-security Reporting Authorized Representatives who attend confidential briefings should be subject to § 2-309 of the Public Utilities Article. That section provides, "Except as directed by the Commission or a court or as authorized by law, an individual subject to § 2-302 of this subtitle may not divulge information learned while inspecting the plant or examining the records of a public service company." The Commission finds this suggestion will help ensure the confidentiality of the cyber-security briefings and therefore adopts it.

IT IS THEREFORE, this 4th day of February in the year Two Thousand Nineteen, by the Public Service Commission of Maryland,

ORDERED: (1) That the following definitions are hereby adopted:

(a) Information Technology System (IT System) – hardware and software related to electronic processing, and storage, retrieval, transmittal and manipulation of data.

(b) Operations Technology System (OT System) – a system or network that monitors or controls electric, gas or water system infrastructure used for utility operations.

[10] Columbia Comments at pp. 3–4.

(c) Smart Grid System – 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.

(d) Security Breach – 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.

(2) That all Maryland electric, gas, or water companies that have 30,000 or more customers in Maryland shall file periodic Cyber-security Reports with the Maryland Public Service Commission as provided herein.

(3) That the periodic Cyber-security Reports shall include 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.

(4) That certification of the accuracy of the periodic Cyber-security Report shall be either by an independent cyber-security consulting firm or by an appropriate and authorized company officer in the format specified in Appendix 3 of the Final Report. All completed self-certifications shall be retained by the company for a period of five years.

(5) That Cyber-security Reporting Authorized Representatives having the authority to receive confidential cyber-security briefings or confidential cyber-security breach information, not requiring government security clearance are:

- The Commissioners;
- The Commission Executive Secretary;
- The Commission's Executive Director;
- The Commission's General Counsel;
- The Commission's Senior Advisors;
- The Commission's Chief Engineer;
- An Office of People's Counsel Designated Representative; and
- Alternatives or Others by Commission Invitation.

(6) That there shall be a three-year audit cycle for Commission cyber-security briefings, with the initial schedule as described below:

	First Maryland Cyber-Security Briefing under New Protocols	**Second Cycle Maryland Cyber-Security Briefing under New Protocols**
BGE	2019	2022
Choptank	2020	2023
Potomac Edison	2021	2024
Pepco and Delmarva	2020	2023
SMECO	2021	2024
WGL	2019	2022
Columbia Gas	2021	2024

(7) That all Maryland electric, gas, and water companies regulated by the Commission, regardless of their number of customers, shall verbally report cyber-security

breaches that impact IT, OT, or Smart Grid Systems to the Commission's Chief Engineer (or designated alternate) within one business day of confirmation, or sooner, unless contrary to law or the recommendation of law enforcement to avoid compromising an investigation. Utilities should report updates to the Chief Engineer after the initial report if material changes occur or are discovered regarding the breach. Breached utilities should also contact the Department of Homeland Security National Cyber-security and Communications Integration Center, and Maryland Fusion Center, as well as the Maryland Attorney General's Office, where appropriate.

(8) Any cyber-security briefing materials reviewed at periodic briefings with the Commission shall be collected at the end of the briefing. Any actions requested by the Commission to the utility shall be recorded by the utility. Briefing materials and recorded actions shall be retained by the utility for a period of no less than five years. No detailed information requiring a government security clearance should be communicated to Cyber-security Reporting Authorized Representatives who do not have appropriate clearance. Cyber-security Reporting Authorized Representatives shall be subject to Section 2-309 of the Public Utilities Article, *Annotated Code of Maryland*.

By Direction of the Commission,

/s/ Terry J. Romine

Terry J. Romine
Executive Secretary