PUBLIC SERVICE COMMISSION OF MARYLAND

REPORT ON CYBERSECURITY PROTECTIONS FOR UTILITIES

Submitted to the Maryland General Assembly
Annapolis, Maryland

July 1, 2024

William Donald Schaefer Tower
6 St. Paul Street
Baltimore, Maryland 21202-6806
www.psc.state.md.

Table of Contents

I. Introduction

During the 2023 Session, the Maryland General Assembly enacted House Bill 969[1] (HB 969) entitled "Public Service Commission – Cybersecurity Staffing and Assessments, alternatively known as the Critical Infrastructure Cybersecurity Act of 2023 (or "Act"). As introduced, the Act was focused on adding cybersecurity staff to the Commission and requiring the Commission to establish minimum cybersecurity standards for public utilities. Specifically, as introduced, the Act: (1) required the Commission to include one or more cybersecurity experts on its Staff to advise the Commission and perform certain duties; (2) required the Commission to establish minimum cybersecurity standards and best practices for regulated entities and share cybersecurity-related information/best practices with municipal electric utilities; (3) required the Commission to conduct and submit an evaluation of the public service companies' assessments to Maryland Department of Information Technology (DoIT) Office of Security Management; and (4) required public service companies to adopt and implement cybersecurity standards and conduct assessments, and report cyber security incidents. HB 969 was codified in Public Utilities Article (PUA), §2-108 and §5-306, Annotated Code of Maryland, which was enacted July 1, 2023.

The 2023 Maryland General Assembly Joint Chairmen's Report section on Cybersecurity Protections[2] also requires a report from the Public Service Commission by July 1, 2024 on cybersecurity protections for utilities. In describing the purpose of the report, the MGA states:

> "The committees believe that a robust and tested cybersecurity program to safeguard the State's public utilities is critical to protect public health and safety, prevent service disruptions, and safeguard customer and employee personal and

[1] Delegate Qi sponsored HB 969. Senator Hester introduced the identical cross-file to HB 969 as Senate Bill 800.
[2] 2023 MGA Joint Chairman's Report https://dls.maryland.gov/pubs/prod/OperBgt/Joint-Chairmens-Report-2023-Session.pdf .

> financial information. The committees request that the Public Service Commission (PSC) provide a report on efforts to plan for cybersecurity protections for public utilities in the State, including national best practices for implementing an ongoing and iterative cybersecurity regulatory structure for electric, gas, and water utilities."

II. Cybersecurity Initiative Status

The Commission has established an Office of Cybersecurity to provide oversight of public service company cybersecurity, implement the Act's requirements, and advise the Commission on cybersecurity matters, among other things. The initial staffing for the Office of Cybersecurity is three positions, a cybersecurity director and two cybersecurity specialists. All three positions require periodic training and certifications. To date, the two cybersecurity specialist positions are filled, and these specialists have completed Cybersecurity Performance Goals (CPG) training and Multi-State Information Sharing and Analysis Center (MS-ISAC) registration. They will also undertake the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF) 2.0 Lead Implementer (LI) training and certification in the second half of 2024.

The Commission's Cybersecurity Reporting Work Group (CSRWG) is the forum to collaboratively engage public service companies and other interested parties in implementing the Act's requirements. To that end, the Office of Cybersecurity has worked through the CSRWG and with the Maryland Cybersecurity Council's Critical Infrastructure Subcommittee to develop a cybersecurity regulatory structure that is not only aligned with national best practices derived from NIST, Cybersecurity Infrastructure and Security Agency (CISA), and the National Association of Regulatory Utility Commissioners (NARUC), but also includes an ongoing and iterative compliance framework. The CSRWG proposed regulations in 2024 that were approved

by the Commission in the RM76 docket on June 11, 2024, for publishing in the *Maryland Register*.

The RM76 proposed regulations establish standard cybersecurity definitions and set requirements for good cybersecurity practice by public service companies. This requires that public service company cybersecurity plans address cybersecurity-related governance, risk management, procurement practices, personnel hiring, training policies, situational awareness, response, recovery, zero trust implementation, and transparent reporting of cybersecurity incidents to state and federal entities. Cybersecurity best practices also require that public service companies align their cybersecurity practices with the CISA Cross-Sector Cybersecurity Performance Goals (CPG) or a more stringent standard based on the NIST security frameworks.

Furthermore, the RM76 proposed regulations expand the Commission's existing confidential triennial cybersecurity briefings to all public service companies with 15,000 or more combined gas, electric, and water customers in Maryland. This expansion aims to provide the Commission and the Commission's Office of Cybersecurity more insight into the cybersecurity challenges and applicable cybersecurity standards and best practices of water companies and municipal utilities. In contrast, this requirement previously only applied to the State's large gas and electric investor-owned utilities and large electric cooperative utilities.

A cybersecurity incident was defined in the RM76 proposed regulations as a malicious act or suspicious event that compromises, or was an attempt to compromise, a public service company's cybersecurity device.[3] The Commission also approved cybersecurity incident

[3] "Cybersecurity device" means any combination of hardware, software, and related services, including informational technology systems, operational technology systems and smart grid systems used for delivery of electricity, gas, or water, or systems that store customer information.

reporting requirements in the RM76 proposed regulations that are aligned with NERC CIP-008[4] incident reporting requirements at the federal level and require that all public service companies shall report cybersecurity incidents no later than 24 hours to the State Security Operations Center according to the method specified by DoIT. Public service company, cybersecurity incident reporting is an evolving practice within the industry, and the Commission's Office of Cybersecurity will continue to work with DoIT, public service companies, and the Maryland Cybersecurity Council's Critical Infrastructure Subcommittee in the future to improve these practices.

One of the most impactful improvements to cybersecurity protections in the State involves establishing zero trust requirements for public utilities in RM76. Zero trust is a cybersecurity approach focused on cybersecurity resource protection based on the premise that trust is never implicitly granted, requiring continuous evaluation. Where technically feasible, public service companies must plan to implement zero trust approaches that are aligned with the tenets of the latest revised version of the NIST Special Publication 800-207 and provide timelines or industry roadmaps for implementing zero trust approaches, among other things.

The Act also requires that on or before July 1, 2024, and on or before July 1 every other year thereafter, public service companies shall engage a third party to conduct an assessment of cybersecurity devices and supply chain risk based on either of the CISA CPG or a more stringent standard that is based on NIST security frameworks. The Commission issued a Notice of Statutory Requirement on April 10, 2024, in Case No. 9492—*In the Matter of Cyber-Security*

[4] The North American Electric Reliability Corporation Critical Infrastructure Protection (NERC CIP) plan is a set of standards aimed at regulating, enforcing, monitoring and managing the security of the bulk electric system in North America.

Reporting of Maryland Utilities[5]—to conduct these assessments and submit certifications to the Commission and further directed utilities on the requirements for these assessments and the manner of reporting. These requirements also will be codified in the proposed RM76 regulations approved by the Commission.

In RM76, the Commission also plans to codify requirements for public service companies to notify the Office of Cybersecurity of its cybersecurity contacts. In addition, in RM76, the Commission has set requirements for public service company responses to the Office of Cybersecurity for specific information requests related to cybersecurity incidents, standards, practices, procedures, or other information reasonably related to cybersecurity unless such processes are superseded by applicable federal cybersecurity standards and regulations that prohibit such disclosures.

Additionally, the Commission has approved a compliance framework in RM76 for the Office of Cybersecurity to enforce the cybersecurity regulations, including certain administrative procedures for issuing a Notice of Probable Violation (NOPV) upon finding reasonable cause to believe a violation of cybersecurity requirements. This compliance framework includes provisions for compliance orders, public service company response options, consent orders, stays of enforcement, and civil penalties. The Commission's Office of Cybersecurity has also developed internal protocols to protect confidential cybersecurity information it receives from public service companies in its oversight of public service company cybersecurity.

[5] Maillog No. 308885.

III. Other Cybersecurity Initiatives

The Commission's Office of Cybersecurity will continue to engage the State's public service companies through the CSRWG and with direct contact. In addition, the Office of Cybersecurity will meet in person at the Commission's offices or at another mutually agreeable location with public service companies to review their third-party cybersecurity assessments of cybersecurity devices and supply chain risk after July 1, 2024, when their biennial certifications are due to be submitted. An anonymized summary of findings from these assessments and certifications will be consolidated in a confidential report to the State Chief Information Security Officer by January 1, 2025, as required by PUA §2-108(d)(8)(i)(3).

In addition, as required by PUA §2-108(d)(8)(i)(1), the Office of Cybersecurity will collaborate with the Office of Security Management and the CSRWG to further develop cybersecurity standards and best practices for public service companies, taking into account utility needs and capabilities based on size. To that end, the Office of Cybersecurity surveyed public service companies in the first half of 2024 to determine cybersecurity standards and best practices already in use. Public service companies representing approximately 2.5 million of Maryland's 2.6 million electric customers and 1.1 million of Maryland's 1.2 million gas customers responded to the survey. These respondents included electric and gas investor-owned companies, municipal utilities, electric cooperatives, and water companies.

The data collected has been anonymized and provides a robust list of cybersecurity regulations and standard requirements already in place for public service companies, notwithstanding the Maryland Critical Infrastructure Cybersecurity Act of 2023 and COMAR 20.06 requirements. They include the Federal Energy Regulatory Commission (FERC) Order 706 - NERC CIP Standards, the federal Cyber Incident Reporting for Critical Infrastructure Act

of 2022 (CIRCIA), the Maryland Personal Information Protection Act (Commercial Law, §§14-3501- 14-3508), the Department of Homeland Security Transportation Security Administration (TSA) Gas Pipeline Security Directives, Defense Federal Acquisition Regulation Supplement (DFARS) Clause 252.204-7012 (NIST 800-171), Security and Exchange Commission Cyber Reporting, Sarbanes-Oxley, the Department of Homeland Security Chemical Facility Anti-Terrorism Security Act, the Health Insurance Portability and Accountability Act (HIPAA), the U.S. Federal Acquisition Regulation, the U.S. Department of Transportation (USDOT) Hazardous Materials Safety Regulations and USDOT Pipeline Safety Regulations.

The list of cybersecurity frameworks, guidelines, and tools that Maryland public service companies are currently using or have used in the past includes the NIST CSF, the NIST Special Publications 800-53 and 800-37, the Department of Energy Cybersecurity Capability and Maturity Model (DOE C2M2), American Water Works Association (AWWA) Cybersecurity Guidance and Assessment Tool, the National Rural Electric Cooperative Association (NRECA) Essence Cybersecurity Tool, the American Public Power Association (APPA) Cybersecurity Scorecard, NERC CIP, the Edison Electric Institute (EEI) Culture of Security Tool, the CISA Cross-Sector Cybersecurity Performance Goals (CPG), Center for Internet Security (CIS) Critical 18 Controls, and International Organization for Standardization (ISO) 27001.

In alignment with national directives and best practices outlined in the White House National Security Memorandum on Critical Infrastructure Security and Resilience[6] issued by President Biden on April 30, 2024, the Commission's Office of Cybersecurity will continue its efforts to improve the cybersecurity resilience of its critical infrastructure in the electric, gas, and

[6] National Security Memorandum on Critical Infrastructure Security and Resilience https://www.whitehouse.gov/briefing-room/presidential-actions/2024/04/30/national-security-memorandum-on-critical-infrastructure-security-and-resilience/.

water utilities sectors. A key point from this memorandum that intersects with our current regulatory framework prescribes a risk-based approach where regulatory requirements should be tailored to each public service company's specific risk profile, considering factors like size, system complexity, and the potential impact of cyberattacks. Furthermore, regulations should be adaptive and iterative, and the regulatory structure should be designed to evolve alongside cyber threats and best practices, incorporating ongoing assessments and feedback mechanisms, and focusing on measuring outcomes and managing risks rather than prescribing specific technologies or procedures. Collaboration and partnership is also encouraged to foster open communication and cooperation between regulators, utilities, industry stakeholders, and federal agencies.

The Commission's Office of Cybersecurity also continues to benefit from biannual NARUC cybersecurity training support and resources such as the NARUC Cybersecurity Manual and other NARUC Critical Infrastructure Subcommittee cybersecurity initiatives. In the first half of 2024, NARUC published its "Cybersecurity Baselines for Electric Distribution Systems and Distributed Energy Resources" report. This initiative was developed by NARUC in partnership with the U.S. Department of Energy's Office of Cybersecurity, Energy Security, and Emergency Response (DOE CESER). These baselines focus on cybersecurity for electric distribution systems and distributed energy resources (DERs) that connect to them. These baselines are a common starting point for cyber risk reduction activities, and they provide tailored guidelines specifically for electric distribution systems and DERs to be applied by state public utility commissions, utilities, and DER operators/aggregators. The goal is to enhance grid security by mitigating cybersecurity risks. The Office of Cybersecurity will evaluate these baselines for potential adoption in collaboration with the public service companies, the State

Chief Information Security Officer, and the Maryland Cybersecurity Council's Critical Infrastructure Subcommittee, among other stakeholders.

Finally, the Commission's Office of Cybersecurity has a statutory responsibility in PUA §2-108(d)(8)(i)(2) to undertake cybersecurity initiatives and share best practices with a particular focus on municipal electric utilities. This effort is expected to begin in the second half of 2024.

IV. Conclusion

This Commission's Office of Cybersecurity has made progress in implementing the Act's requirements in the past year. This regulatory framework and other cybersecurity initiatives will provide a foundation for an ongoing and iterative approach to safeguarding Maryland's critical infrastructure from cyber threats. We will continue to work with the public service companies, the State Chief Information Security Officer, the Maryland Cybersecurity Council's Critical Infrastructure Subcommittee, and other stakeholders to improve the resilience of critical infrastructure and enhance the safety and reliability of essential services for all Maryland citizens by effectively implementing the Act and its related COMAR 20.06 requirements, adopting national standards and best practices, fostering stakeholder collaboration and embracing continuous improvement.