STATE OF MARYLAND

PUBLIC SERVICE COMMISSION

March 3, 2022

Chair C.T. Wilson
Economic Matters Committee
House Office Building, Room 231
Annapolis, Maryland 21401

RE: UNFAVORABLE – HB 1339 – Cybersecurity – Critical Infrastructures and Public Service Companies (Critical Infrastructure Act of 2022)

Dear Chair Wilson and Committee Members:

House Bill1339 sets forth several provisions affecting cybersecurity as it relates to public service companies in Maryland. Specifically, the bill: (1) authorizes the Department of Emergency Management to establish the Critical Infrastructure Cybersecurity Grant Program in the Department; (2) requires public service companies to establish and adopt minimum cybersecurity standards and to report on their cybersecurity programs; (3) directs promulgation of certain cybersecurity-related regulation; and (4) assigns the Maryland Public Service Commission certain cybersecurity-related requirements.

While well intentioned, HB 1339 could compromise cybersecurity and critical infrastructure within the State, providing conflicting direction to public utility companies and impeding the evolution of mature cybersecurity programs.

HB 1339 Compromises Cybersecurity and Critical Infrastructure in the State

In authorizing the establishment of the Department's Grant Program, the Bill would require public service companies to reveal cybersecurity risks for the purpose of determining types of cybersecurity improvements and recipients that would be eligible for grants under the program and require the Department to publish a report on those risks. These provisions would serve to compromise the public service companies' cybersecurity programs and critical infrastructure by requiring them to reveal areas of potential vulnerability. Public utility companies' cybersecurity programs have always been treated confidentially in the interest of preserving the integrity of those programs and of the critical infrastructure serving the State. The sharing of any such confidential material is also protected from public disclosure under Section 104(d)(4)(B) of the federal Cybersecurity Act of 2015.

HB 1339 Provides Conflicting Direction to Public Utility Companies Regarding Their Cybersecurity Initiatives

HB 1339 duplicates existing cybersecurity processes established under Commission directives established pursuant to § 2–113 of the Public Utilities Article. Since 2017, the public utility companies serving the vast majority of the State, under the jurisdiction of the Commission, have been involved in the development of cybersecurity definitions and protocols in the interest of their critical infrastructure and the customers they serve. These efforts have culminated in the issuance of Order No. 89015 in 2019, and a pending Commission Staff petition for rulemaking. To date, every major public utility has had confidential meetings with the Commission to discuss their cybersecurity programs and the maturity of those programs.

The Bill proposes cybersecurity-related definitions and implementation propositions that suggest cybersecurity can contain or rely upon specific, categorical metrics. However, cybersecurity employs a holistic, defense-in-depth approach to ensuring safeguards. The Commission's directives recognize this important distinction reflecting the key factors of cybersecurity program implementation inherent in National Association of Regulatory Utility Commissioners (NARUC) cybersecurity guidelines and federal/national cybersecurity frameworks. However, the Bill would require public service companies to create and establish security standards that could not only undermine many years of cybersecurity work but would signal a lower bar for cybersecurity in the State. Requiring compliance to and regulatory oversight of unmeasurable criteria would be impossible.

The Bill also imposes requirements upon grant recipients to establish cybersecurity plans that serve to duplicate or confuse utility companies' cybersecurity efforts. As indicated, utility companies adhere to cybersecurity protocols established through Commission directive. A separate or parallel requirement under the auspices of the Grant Program introduces the prospect of applying certain but undefined criteria upon utility operations in a manner that may detract from their ongoing cybersecurity efforts. This is in addition to confidentiality concerns related to the requirement that grant recipients submit reports on these criteria.

HB 1339 Does Not Recognize the Evolving Nature of Cybersecurity

As indicated, HB 1339 would establish and apply specific cybersecurity standards and potentially inconsistent program requirements under different state agencies. None of the requirements align with the recognition that cybersecurity threats are ever evolving and that public utility companies serving the State would strive to evolve their programs accordingly. Attention to defense-in-depth and maturity within a utility company's cybersecurity program, as opposed to adherence to prescriptive standards or plans, should remain a guiding principle.

Conclusion

HB 1339 would serve to duplicate, confuse and/or replicate years of cybersecurity development that has been applied to public utility companies under Commission directives. Importantly, if enacted, this law could also provide a road map to compromising critical infrastructure by revealing confidential details associated with the utility companies' cybersecurity programs. For these reasons, the Commission requests an unfavorable report on HB 1339.

Please contact Lisa Smith, Director of Legislative Affairs, at (410) 336-6288 if you have any questions.

Sincerely,

Jason M. Stanek
Chairman