Department of Legislative Services

Maryland General Assembly
2023 Session

FISCAL AND POLICY NOTE
Third Reader - Revised

Senate Bill 800 (Senator Hester)
Education, Energy, and the Environment

Public Service Commission - Cybersecurity Staffing and Assessments (Critical Infrastructure Cybersecurity Act of 2023)

This bill requires the Public Service Commission (PSC) to include one or more employees that are experts in cybersecurity on its staff for specified purposes. In supervising and regulating public service companies, PSC must also consider the protection of a public service company's infrastructure against cyberattack threats. Each public service company, except common carriers and telephone companies, must take specified actions related to cybersecurity, including engaging a third party by July 1, 2024, and every two years thereafter, for a cybersecurity assessment and submitting related certifications of compliance to PSC. By January 1, 2025, and every two years thereafter, PSC must submit a report with related information and recommendations to the State Chief Information Security Officer (SCISO), or the SCISO's designee. The bill also specifies authorized uses of Dedicated Purpose Account (DPA) funds by the Department of Information of Technology (DoIT) for fiscal 2024 for certain purposes. **The bill takes effect July 1, 2023.**

Fiscal Summary

State Effect: Special fund expenditures for PSC increase by $364,400 in FY 2024, under the assumptions discussed below. Future years reflect annualization and the elimination of one-time costs. The FY 2024 budget as passed by the General Assembly includes $364,000 in special funds and three new positions for PSC, contingent on the enactment of this bill or its cross file. DoIT can handle the bill's requirements with existing available resources. Authorizing language related to DPA does not affect State finances.

(in dollars)	FY 2024	FY 2025	FY 2026	FY 2027	FY 2028
SF Revenue	$364,400	$446,200	$465,700	$485,600	$510,500
SF Expenditure	$364,400	$446,200	$465,700	$485,600	$510,500
Net Effect	$0	$0	$0	$0	$0

Note:() = decrease; GF = general funds; FF = federal funds; SF = special funds; - = indeterminate increase; (-) = indeterminate decrease

Local Effect: Expenditures for municipal electric utilities increase beginning in FY 2024 by an unknown but potentially significant amount to comply with the bill's requirements, including third-party cybersecurity assessments every two years. Revenues are not directly affected. **This bill may impose a mandate on a unit of local government.**

Small Business Effect: Meaningful.

Analysis

Bill Summary:

Dedicated Cybersecurity Staff

The commission must include on its staff one or more employees that are experts in cybersecurity to:

- advise the PSC chair and the other commissioners on measures to improve oversight of the cybersecurity practices of public service companies;
- consult with the Office of Security Management (OSM) in DoIT on cybersecurity issues related to utility regulation;
- assist PSC in monitoring the minimum security standards developed under the bill;
- participate in briefings to discuss cybersecurity practices based on applicable National Association of Regulatory Utility Commissioners guidance and improvements to cybersecurity practices recommended in the cybersecurity assessments required under the bill; and
- support public service companies that do not meet minimum security standards with remediating vulnerabilities or addressing cybersecurity assessment findings.

PSC Actions Related to Cybersecurity

In supervising and regulating public service companies, PSC must also consider the protection of a public service company's infrastructure against cyberattack threats.

PSC must collaborate with OSM to establish cybersecurity standards and best practices for regulated entities, taking into account utility needs and capabilities based on size. PSC must periodically share information on cybersecurity initiatives and best practices with municipal electric utilities.

By January 1, 2025, and every two years thereafter, PSC must collect certifications of a public service company's compliance with standards used in the assessments conducted by

public service companies under the bill and must submit a report with related information and recommendations to the SCISO or the SCISO's designee. In addition to other information, the report must include, grouped by utility type: (1) a general overview of cybersecurity technology and policies used by public service companies in the State; and (2) general recommendations for improving cybersecurity technology and policies used by public service companies in the State.

Public Utility Cybersecurity Requirements

Each public service company, except common carriers and telephone companies, must adopt and implement cybersecurity standards that are equal to or exceed the standards adopted by PSC, adopt a zero-trust cybersecurity approach for on-premises services and cloud-based services, and establish minimum security standards for each operational technology and information technology (IT) device.

Additionally, by July 1, 2024, and every two years thereafter, each affected public service company must engage a third party to conduct an assessment of the operational technology and IT devices, as specified. Each company must submit certification of the company's compliance with the standards used in the assessment to PSC.

Each public service company must report a cybersecurity incident, including an attack on a system being used by the public service company, to the State Security Operations Center in DoIT, as specified. The center must immediately notify appropriate State and local agencies of the reported incidents. The SCISO, in consultation with PSC, must establish a process for such reports and related criteria, processes, and requirements.

Use of Dedicated Purpose Account Funds

The bill also authorizes the use of DPA funds by DoIT for fiscal 2024 for the purpose of adding additional staffing and operational capacity for DoIT to improve State and local cybersecurity.

Legislative Intent

It is the intent of the General Assembly that PSC work with the federal Cybersecurity and Infrastructure Security Agency and OSM to improve PSC's capacity to implement the bill.

Current Law:

Public Service Commission Generally

PSC must supervise and regulate public service companies subject its jurisdiction to (1) ensure their operation in the interest of the public and (2) promote adequate, economical, and efficient delivery of utility services in the State without unjust discrimination. In doing so, PSC must consider the public safety, the economy of the State, the maintenance of fair and stable labor standards and for affected workers, the conservation of natural resources, the preservation of environmental quality, and the achievement of the State's climate commitments for reducing greenhouse gas emissions. PSC must also enforce compliance with legal requirements by public service companies, including requirements with respect to financial condition, capitalization, franchises, equipment, manner of operation, rates, and service.

"Public service company" means a common carrier company, electric company, gas company, sewage disposal company, telegraph company, telephone company, water company, or any combination of public service companies.

Cybersecurity Regulations

PSC adopted cybersecurity regulations in 2022 for all electric, gas, and water companies ("utilities") regulated by the commission. The utilities are required to follow good cybersecurity practice, generally. At a minimum, cybersecurity plans must address cybersecurity related governance, risk management, procurement practices, personnel hiring, training policies, situational awareness, response, recovery, and transparent reporting of cybersecurity incidents to State and federal entities.

Each utility with 30,000 or more customers in the State must provide periodic confidential cybersecurity reports describing the utility's adherence to good cybersecurity practice, including the utility's cybersecurity maturity level trends, cybersecurity performance metric trends, or any other cybersecurity related topics of current interest to PSC and such additional representatives as PSC designates. Reports are required at least every three years, or as otherwise directed by PSC.

Each utility (regardless of size) must report confirmed cybersecurity breaches of a smart grid system, IT system, or operations technology system to a PSC-designated representative without divulging energy/electric infrastructure information, no later than one business day after confirmation, unless prohibited or recommended by law enforcement to avoid compromising an investigation.

Office of Security Management

The SCISO is the head of OSM, and the officer's responsibilities include, among other things, (1) developing and maintaining IT security policies, standards, and guidance documents consistent with best practices developed by the National Institute of Standards and Technology and (2) providing technical assistance to localities in mitigating and recovering from cybersecurity incidents.

Chapters 241, 242, and 243 of 2022 expanded and enhanced the State's regulatory framework for State and local government cybersecurity. Among other things the Acts codified the Maryland Cyber Defense Initiative (which codified OSM within DoIT) and the Maryland Cybersecurity Coordinating Council and expanded the responsibilities of OSM and the council.

The Acts also required the Governor to include in the annual budget bill for fiscal 2024 an appropriation of at least 20% of the aggregated amount appropriated for information technology and cybersecurity resources in the annual budget bill for fiscal 2023. The fiscal 2024 budget as passed by the General Assembly includes $152.0 million for DPA to meet the mandated appropriations required for Chapters 241, 242, and 243. DoIT processed a fiscal 2023 budget amendment to transfer $94.0 million from DPA for remediation of State and local governments' cybersecurity. Although DoIT typically provides services on a reimbursable basis, these funds will enable DoIT to provide the remediation services at no cost to State and local government agencies, consistent with the requirements of Chapters 241, 242, and 243.

State Fiscal Effect: The fiscal 2024 budget as passed by the General Assembly includes $364,000 in special funds and three new positions for PSC, contingent on the enactment of this bill or its cross file. In the absence of additional information from PSC, this estimate assumes that amount of funding is sufficient for PSC to implement the bill.

Accordingly, special fund expenditures for PSC increase by $364,424 in fiscal 2024, which accounts for a 90-day start-up delay. This estimate reflects the cost of hiring one IT director and two IT technicians and reflects current salaries paid by PSC for those job classifications. It includes salaries, fringe benefits, one-time start-up costs, and ongoing operating expenses.

Positions	3.0
Salaries and Fringe Benefits	$335,447
Operating Expenses	28,977
Total FY 2024 State Expenditures	**$364,424**

Future year expenditures reflect full salaries with annual increases and employee turnover as well as annual increases in ongoing operating expenses. Special fund revenues increase correspondingly from assessments imposed on public service companies.

DoIT advises that it can handle the bill's requirements with existing budgeted resources and that the bill's authorizing language related to DPA does not affect State finances. The Department of Legislative Services notes that the DPA funding is already available in the fiscal 2024 budget, ostensibly for the purposes authorized by the bill pursuant to the requirements of Chapters 241, 242, and 243 of 2022. The bill adds clarity to the use of those funds.

Small Business Effect: PSC regulates the rates of 22 water/sewer companies, which combined serve approximately 11,000 residents. These companies – several of which are likely small businesses – are public service companies by definition in the Public Utilities Article and must comply with the bill's requirements for public service companies.

Additional Information

Prior Introductions: Similar legislation has not been introduced within the last three years.

Designated Cross File: HB 969 (Delegate Qi) - Economic Matters and Health and Government Operations.

Information Source(s): Public Service Commission; Department of Information Technology; Department of Legislative Services

Fiscal Note History: First Reader - March 3, 2023
rh/lgc Revised - Budget Information - April 6, 2023
Third Reader - April 10, 2023
Revised - Amendment(s) - April 10, 2023
Revised - Clarification - April 10, 2023

Analysis by: Stephen M. Ross

Direct Inquiries to:
(410) 946-5510
(301) 970-5510