Cyber Governance Act of 2022

The major provisions of SB812 codify roughly 20 recommendations of the Maryland Cybersecurity Council's 2021 Study.

- Codifies the Office of Security Management (OSM) and Chief Information Security Officer (CISO).
- Establishes the positions of Director of State Cybersecurity and the Director of Local Cybersecurity.
- Codifies the Maryland Cybersecurity Coordinating Council (MCCC).
- Requires that DoIT and OSM establish a transition plan toward a centralized cybersecurity enterprise structure no later than June 30, 2023.
- Clarifies that costs associated with implementing this legislation are considered an allowable expense from the Dedicated Purpose Account.
- Requires biennial cybersecurity assessments.

What has been done

- DoIT has completed cybersecurity maturity assessments for 75 units among 61 agencies within the executive branch using the NIST Cybersecurity Framework.
- DoIT has hired both the Director of State Cybersecurity and the Director of Local Cybersecurity.
- DoIT established the Maryland-Information Sharing and Analysis Center (MD-ISAC).
- DoIT completed several legislative mandates including incident reporting requirements for local governments and policy creating authority for the state CISO to issue binding operational and emergency directives.
- DBM processed two amendments to the Dedicated Purpose Account that totaled $50 million at the end of fiscal 2022. ($9.6 million) supported state agency cyber assessments. ($40.4 million) to support remediation costs for the MDH cyber incident.

What remains

- DoIT anticipates that the Treasurer's Office and MDH will be assessed in calendar year 2023.
- Ernst & Young has been hired to develop the assessment framework that will address: whether additional staff are necessary for implementation; the timeline for developing a cybersecurity strategy to serve as the basis for centralization and budgetary allocations; the appropriation necessary to implement the cybersecurity master plan without relying on a charge-back model; assess DoIT's performance and capacity to meet legislative requirements; the security and financial implications of partnering with other states to procure IT or cybersecurity products or services. An interim report of findings is not due until December 1, 2023 and we recommend a mid-term update.
- DGS advises there is not a defined timeline for updating state contracts to include cybersecurity standards for contractors that have access to state systems.

Modernize Maryland Act of 2022

46% of state agencies have at least one identified "legacy system," meaning a system that is too old to be updated, is often expensive to operate or maintain, and presents significant risk to the continuity of government operations. There are four major provisions to HB1205:

- Establishes an independent Modernize Maryland Oversight Commission to advise the Secretary and CISO on necessary IT/cyber upgrades to critical systems.
- Establishes a Local Cybersecurity Support Fund to extend state resources and technical expertise to units of local government.
- Requires cybersecurity assessments and upgrades for wastewater treatment plants.
- Increases the Department of General Services' (DGS) delegated authority for cybersecurity procurements.
- Clarifies that costs associated with implementing this legislation are considered an allowable expense from the Dedicated Purpose Account.

What has been done

- DoIT has contracted with Ernst & Young to (1) develop the mandated assessment framework and (2) assist in satisfying statutory requirements. Terms of reference
- Modernize Maryland kickoff meeting held in October 2022; interim report due on December 1, 2023.
- Governor Moore's FY24 budget includes $7M for the Local Cybersecurity Support Fund.
- MDE has shared its guidance document to assist public and private water and wastewater systems. Additionally, MDE developed and published a survey to poll different water and wastewater systems. MDE has found the following resources for counties and/or the Department to apply to:
    - cisa.gov/cybergrants
    - epa.gov/system/files/documents/2021-07/technicalassistanceflyerupdate-hwg.pdf

What remains

- Ernst & Young's interim report of findings is due on December 1, 2023.
- MDE will conduct outreach to follow up on the guidance document and ensure that all wastewater treatment centers are aware of funding application cycles. The results of MDE's survey regarding wastewater treatment operational technology assessments are pending.
- DBM anticipates significant additional expenditures in FY23 for amendments to the Dedicated Purpose Account and state agency cyber assessments. Additional spending will also occur to begin addressing the recommendations of cyber assessments.
- The Cybersecurity Planning Committee will be responsible for establishing a cybersecurity investment plan for the next two years.

Local Support Act of 2022

SB754 is a critical bill setting State policy to support local government cybersecurity preparedness and extending state-level resources to protect our local units of government. Specifically, the legislation:

- Codifies an existing Cyber Preparedness Unit within MDEM.
- Provides for five full-time staff, in a regional support approach, modeled after the Opioid Command Operation.
- Establishes an Information Sharing and Analysis Center (ISAC) within DoIT.
- Empowers DGS to leverage state purchasing power and economies of scale by negotiating master IT/cybersecurity contracts and cheaper rates for units of local government.
- Clarifies that costs associated with implementation of this legislation are an allowable expense of the Dedicated Purpose Account.

What has been done

- Local government certification compliance and guidance documents have been made available by DoIT for review:
  - Cybersecurity Incident Reporting Requirements for Local Governments
  - Cybersecurity Incident Reporting Requirements for State Government Agencies
  - Guidelines for the Public Disclosure of Cybersecurity Incidents

  Through the Maryland Cybersecurity Coordinating Council, OSM has published the following policies and standards:
  - Emergency and Binding Operational Directives
  - Minimum Security Standard for Units of Government on networkMaryland
- DoIT officially established the MD-ISAC, a hub for sharing bidirectional strategic and tactical Cyber Threat Intelligence for Maryland governments.
- MDEM has communicated new requirements to local emergency managers and local information technology directors.
- The MDEM Cyber Preparedness Unit (CPU) meets with DoIT twice a month; MDEM has hired a Supervisor for the CPU.
- MDEM and DoIT have developed an online reporting form for local jurisdictions and State entities to use.

What remains

- The consultant hired to develop the assessment framework will address: the anticipated timeline and cost to connect local governments with the ISAC and the status of the feasibility study on expanding the SOC for units of local government.
- The ISAC and OSM will support cybersecurity coordination through existing local government stakeholder organizations.
- DGS is reliant on DoIT's guidance on what existing contracts or products should be made available to the local governments. DoIT is responsible for establishing the timeline for local governments, schools, and health departments to certify compliance with minimum standards.