Maryland State and Local Government Cybersecurity

2021
Analysis and Recommendations

Prepared by

The Ad Hoc Committee on State and Local Cybersecurity of the Maryland Cybersecurity Council

December 22, 2021

TABLE OF CONTENTS

LETTER OF TRANSMITTAL

With cybersecurity threats increasing and expanding, the need has never been greater to protect our state agencies as well as our county and municipal governments, school systems, health departments, and other local government units. While details on the attack on the Maryland Health Department are still scarce, this incident follows a long line of incidents including the attack against the Baltimore City government, costing the City an estimated $18 million. Similar ransomware attacks on MedStar and Baltimore County Public Schools have also wreaked havoc in Maryland: thousands were unable to access necessary healthcare services and 115,000 students were shut out of classes.

In this context, we respectfully deliver this report to the Attorney General and the Joint Committee on Cybersecurity, Information Technology and Biotechnology. It was conducted by an ad hoc committee convened by the Maryland Cybersecurity Council at the request of the co-chairs of the Joint Committee on Cybersecurity, Information Technology, and Biotechnology. Our goal was to "Identify key policy / governance/ resources changes for legislative action in 2022 to increase the cybersecurity of the state of Maryland."

We believe that this report provides a robust view of where the state needs to invest and grow to become even more secure. The report includes over 35 recommendations, each an important component of cybersecurity governance, prioritization, modernization and adopting a 'whole of state' approach.

First, following the national trend towards consolidation, we believe cybersecurity across the executive branch agencies should be centralized. All cybersecurity budgets should become part of one cybersecurity budget and agency cybersecurity staff should report to the State Chief Information Security Officer (SCISO) instead of their respective secretaries.

Second, the state must continue to measure and manage cybersecurity across the executive branch with increased prioritization and vigilance. It must ensure that all state IT systems are as secure as possible, which requires continued management and monitoring of sensitive information, vulnerability and risk assessments, remediation objectives and appropriate training. The state must also prioritize funding for upgrades and the modernization of legacy systems, including creating a new investment oversight process.

Third, we must adopt a 'whole of state' approach. The state must do more to protect our units of local government ranging from assessments and response plans to training and model policies. It should establish a Local Cybersecurity Support Fund, providing financial assistance to local units of government as a state match to the Federal State, Local, Tribal, and Territorial (SLTT) Grant Program in the Federal Infrastructure Bill. The state can do more to support local units of government through procurement of managed cybersecurity services under state vehicles, use available funds for local government cybersecurity insurance, and support a local level security operations/fusion center.

We would like to thank all members of the ad hoc committee for their dedication and investment of time and effort spent conducting and analyzing this research as well as the numerous individuals who volunteered their expertise and time. We hope that the data and analysis provided in this report will prove timely and critical to the policy discussions during the 2022 General Assembly Legislative session. We stand ready to assist in any way.

Very Respectfully,

Katie Fr Hester

Senator Katie Fry Hester
District 9, Carroll & Howard Counties
Ad Hoc Committee Co-Chair MCCC

Ben Yelin
UMD Center for Health & Homeland Security
Ad Hoc Committee Co-Chair MCCC

EXECUTIVE SUMMARY

This executive summary provides a high-level overview of the key questions, findings and recommendations of the ad hoc committee of Maryland Cybersecurity Council on Maryland State and Local Cybersecurity. It covers the three tasks explored by the committee: Governance, State Executive Branch, and Local Government Cybersecurity. The report will be presented in January 2022 at the quarterly meeting of the Maryland Cybersecurity Council.

Task 1: Cybersecurity Governance

Cybersecurity governance is embodied in the framework of laws, policies, structures, and processes that determine how cybersecurity risk is managed within the enterprise. It addresses the decisions that need to be made about threats, who should make those decisions, how those decisions should be informed, who is responsible for translating decisions into investments and programs, and how it is determined whether cybersecurity programs are effective. The governance questions addressed in Task 1 are highlighted below.

Governance Questions

- What are the roles of key state departments and local jurisdictions addressing cybersecurity risk?
- How can the state better collaborate with other actors to leverage resources, share best practices, and better understand emerging cybersecurity threats?
- How can the state improve its cybersecurity governance to consider county and municipal needs, respond to deficiencies revealed by audits, and increase compliance/awareness of state strategy and standards?
- What are the implications of the state's current fee–for–service and decentralized model?
- How does Maryland's IT strategy and security manual compare with other states?

Most states are trending toward the consolidation and centralization of their IT functions. What consolidation looks like in each state will vary, but driving this trend are the compelling management and security benefits that come with centralization. In this context, most of the answers to the questions above support Maryland's movement toward centralization and a 'whole of state' approach.

The governance section begins by describing our current state. It outlines the role of the SCISO including how the risk management role is exercised, and how it is hindered by limited resources, visibility into systems of state agencies and the distributed budget. It describes how the Maryland Cybersecurity Coordinating Council (MCCC) is maturing as a stakeholder body, has begun to stream the process for vetting authority for new systems – but has not yet begun to perform its enterprise-wide cybersecurity risk prioritization. It discusses the key role that the Maryland Department of Emergency Management (MDEM) already plays through its cybersecurity unit, as a convener, planner and coordinator of emergency management efforts in each county.

This section also discusses how Maryland could partner with the Multi-State Information Sharing and Analysis Center (MS ISAC) and Cybersecurity and Infrastructure Security Agency (CISA) and Department of Homeland Security (DHS). While there is limited data available on the state's cybersecurity spend, there is some guidance from other states and the federal government. Finally, the state is commended for an excellent Security Manual, but notes that the cybersecurity strategy is only a chapter in the Master IT plan and could be improved.

Recommendations emerging from Task I include:

- Codify the key elements of the previous Executive Orders: Maryland Cyber Defense Initiative, Maryland Data Privacy, and State Chief Data Officer.
- Centralize IT functions of all agencies in the Executive Branch within The Department of Information Technology (DoIT). All IT budgets would become part of DoIT's budget and agency staff would report to the CIO.
- Leverage and expand MDEM's role with local government on cyber-related preparedness and response planning.
- Coordinate the procurement of managed cybersecurity services under state vehicles and allow local units of government to participate.
- Connect all risk assessments required by the State Security Manual with the budgeting process and articulate the cybersecurity budget similar to the federal process.
- Shift to appropriating the cybersecurity budget, replacing the current charge-back model.
- Fully develop a separate cybersecurity strategic plan to undergird the cybersecurity budget.
- Mandate basic contractor security requirements (e.g. DFARS 52.204-21.)
- Set goals, timelines, metrics and resources for the IT Master Plan and Cybersecurity Strategic plan.
- Require the General Assembly, the State Judicial Branch and the University System of Maryland to certify compliance with DoIT minimum security standards annually.
- Expand the Maryland Cybersecurity Coordinating Council to include the General Assembly, University System and State Judiciary and exempt it from the Open Meeting Act.

Task 2 : State Executive Branch Cybersecurity

Cybersecurity at the scale and complexity of a statewide enterprise is encumbered by many challenges. Between 2016 and 2019 the Office of Legislative Audits (OLA) issued 457 reports, of which 77 reports, covering 69 units of state and local government, had 84 findings concerning the lack of Personally Identifiable Information (PII) controls.[1] Across these 77 reports, 37.9 million recorders were identified as

[1] Hook, Gregory, and Stephen Jersey. *Personally Identifiable Information (PII) Audit Issues*, Office of Legislative Audits, 17 Dec. 2019.

containing PII data elements where lack of controls left the records susceptible to increased risk of improper disclosure.[2]

Fortunately, Maryland demonstrates a growing commitment to securing the state. The nature of the findings is shifting and there is reduction of repeat findings related to PII, an increased focus on advanced security features, monitoring of contractors and third-party providers.

In order to answer the three broad executive branch questions highlighted below, The Office of Security Management completed its first cybersecurity survey. Data was gathered through a comprehensive survey that endeavored to understand the Executive Branch's ability to identify, protect, detect and respond to cybersecurity incidents.

State Executive Branch Questions

- Has each state agency completed a recent vulnerability assessment, planned to remediate any current vulnerabilities, and prepared to prevent evolving/future cybersecurity risks?
- How do the state's overall IT strategy and expenditures on cybersecurity compare to other states and the federal government, and where is there room for improvement or innovation?
- Are each state agency's personnel and partners provided sufficient cybersecurity awareness education and training to relay necessary security-related information?

The surveys were sent by the State Chief Information Security Officer to eighty-nine discrete units of state government within the purview of the Governor's authority. Of those eighty-nine, seventy responded by the time of this writing, including all twenty-one principal departments. Of the seventy, eight indicated that their results were included as part of another response as a function of shared IT and cybersecurity services.

Because this information would be valuable to a cybercriminal, specific data about systems and agencies are not included in this report. However, in the interest of a transparent government, high-level information about the survey results is included in the report and highlighted below.

- **Identify:** Survey results indicate that 80% of respondents have a complete or partial inventory of internal IT systems. More than 50% have not identified recovery time objectives for their systems.
- **Protect:** Survey Results indicate that 40% of units have at least one legacy system. More than 60% of the respondents have not conducted a cybersecurity risk assessment. Most units lacked explicit standards describing sensitive information and information-sharing agreements. Nearly 75% perform backups on a regular basis. Over 60% of respondents require multi-factor authentication for email. Only three respondents do not conduct cybersecurity training.

[2] Ibid.

- **Detect:** The Maryland IT Security manual describes the standards for scanning IT assets for vulnerabilities. Of the agencies that responded, more than half noted vulnerability scanning within standards. However, of those that responded "unknown," half received the service from DoIT but were unaware.
- **Respond:** Despite being described in the Maryland IT Security Manual, most agencies were unable to describe the remediation objective-time for vulnerabilities of various severities.

The recommendations emerging from Task 2 include:

- Conduct an annual IT & Cybersecurity survey of all state agencies including a first baseline report of specified state data.
- Develop standards to describe sensitive information and to establish information sharing and data use agreements.
- Ensure that an annual vulnerability and risk assessment is completed for each unit.
- Prioritize funding for upgrades and modernization efforts and create a new oversight process for the investment.
- Ensure that all Executive Branch Agencies?:
    - Completes a thorough inventory of their IT system(s)
    - Develop specific remediation objective-time for vulnerabilities of various severities
    - Conduct regular backup operations and more frequent restoration testing
    - Complete regular vulnerability scans
    - Operate with multi-factor authentication practices for remote access and email
    - Conduct cyber security training for all regular and contractual employees

Task 3 : Local Government Cybersecurity

The proliferation of cybersecurity incidents in recent years has shown that no local jurisdiction, no matter its size, is immune. In 2019, a ransomware attack hit the Baltimore City Government, costing the city an estimated $18 million.[3] In early 2021, a ransomware attack befell the Baltimore County School System, costing the County an estimated $7.7 million.[4] Beyond the financial cost, the attack significantly burdened students and families that were already engaged in full-time distance learning. Most recently, units of local governments have been forced to contend with the downstream effects of the cyber attack on the Maryland Department of Health (MDH).

The research team was interested in evaluating the preparedness and response capabilities of units of local government, including counties, municipalities, school districts and local emergency management departments. In addition, we sought input from these stakeholders on how the state could be most helpful as a resource for these units of local government.

[3] https://www.baltimoresun.com/politics/bs-md-ci-ransomware-expenses-20190828-njgznd7dsfaxbbaglnvnbkgjhe-story.html

[4] https://www.baltimoresun.com/education/bs-md-ransomware-cost-schools-20210609-20210611-6fipdck3h5b5peli6vgbgfsqyy-story.html

Surveys were distributed to County IT departments, municipalities, local school systems, and local emergency managers across the state. The surveys specifically focused on governance, risk assessment, risk management strategy, and awareness and training. After the data was synthesized and aggregated, stakeholders convened to discuss the results in a series of meetings.

Local Government Questions
● Has each local government unit completed a recent vulnerability assessment, planned to remediate any current vulnerabilities, and prepared to prevent evolving/future cybersecurity risks? ● How can the state best support local governments, including school systems, health departments, and municipalities, to meet minimum standards for cybersecurity and to leverage federal resources for assessment and improvement? ● Are local governments allocating sufficient resources to cybersecurity in their information technology budgets, cybersecurity awareness education and training for employees?

Overall, respondents across all sectors of local government expressed eagerness to improve their cyber security posture and in many cases have made great progress. However, survey respondents also indicated that they were limited by lack of funding for full-time staff, along with inadequate access to appropriate preparedness resources. The results of the surveys are summarized in full in the report, but among the most notable findings:

- Approximately 78% of local emergency management respondents, and 63% of municipal government respondents, have completed vulnerability assessments.
- However, almost 90% of municipality respondents reported that their municipal government had not conducted a vulnerability assessment of jurisdiction IT infrastructure and network. Likewise, 87% of respondents reported their jurisdiction had not requested or completed a cyber assessment through either Maryland National Guard’s Innovative Readiness Training (IRT) Program or the Department of Homeland Security (DHS)—Cybersecurity and Infrastructure Security Agency (CISA).
- Among local emergency management offices, 53.8% of the surveyed jurisdictions have neither a consequence management plan which covers prevention, response, and recovery nor a cyber disruption event in the form of an Emergency Operations Plan annex, nor a contingency plan.
- Only 31% of local school system respondents indicated that their organization allocates sufficient resources to cybersecurity in their budgets, including for monitoring, response, cybersecurity awareness education and training for employees.
- In focus groups with representatives from the Maryland Association of Counties (MaCO), respondents indicated that many counties are not allocating sufficient resources to cybersecurity. If there were clear standards to evaluate the effectiveness of control systems, or an intendant auditing function, it would be easier to assess whether local governments are allocating sufficient resources to cybersecurity in their information technology budgets.
- For counties to meet the minimum standards for cybersecurity, the state needs to provide additional funding and assist the counties in obtaining resources (tools, software, hardware, and personnel). It would also be helpful for the state to maintain a list of recommendations and

resources in one easy location. Additionally, the state should look into a voluntary certification program for entities that meet a defined set of standards.

The recommendations emerging from Task 3 include:

- Adopt the plan for a coordinated cybersecurity operations effort, split between the Department of Information Technology (DoIT), and the Maryland Department of Emergency Management (MDEM). This plan emerged amid negotiations over SB 69, during the 2021 Legislative Session, and was agreed to by Secretary Leahy (DoIT) and Acting Secretary Strickland (MDEM)
- Support the duties of the Maryland Department of Emergency Management (as described above), the state should fully fund and provide adequate resources to the Cyber Preparedness Unit, within the Preparedness Branch of the Consequence Management Directorate of MDEM.
- Establish a Local Cybersecurity Support Fund, to provide financial assistance to local units of government to improve their cybersecurity posture. The fund could either be a revolving fund (like the Revolving Resiliency Loan Fund, created during the 2021 legislative session) or a grant fund. The fund could be administered by both DoIT and MDEM.

INTRODUCTION

This study addresses three sets of questions focused on state cybersecurity: governance, state Executive Branch cybersecurity, and local government cybersecurity. The study was conducted by an ad hoc committee convened by the Maryland Cybersecurity Council at the request of the co-chairs of the Joint Committee on Cybersecurity, Information Technology, and Biotechnology.[5] In parallel, the Joint Committee staged a series of hearings on cybersecurity during the summer and fall of 2021.[6] The immediate impetus for this effort was the near passage of SB 69[7] in the 2021 session and an amendment to the bill[8], proposed in the final moments of the session, that called for a formal study of the state's cybersecurity to inform future legislation.

The ad hoc committee was co-chaired by Ben Yelin at the Center for Health and Homeland Security (CHHS) at the University of Maryland, Baltimore and Senator Katie Fry Hester (District 9, Carroll and Howard Counties). The other members of the ad hoc committee included Senator Susan Lee (District 16, Montgomery County), Delegate Ned Carey (District 31A, Anne Arundel County), Acting Secretary Russell Strickland (Maryland Department of Emergency Management), Charles "Chip" Stewart (State Chief Information Security Officer), Kevin Kinnally (Legislative Director, Maryland Association of Counties), and Dr. Gregory von Lehmen (Special Assistant for Cybersecurity, University of Maryland Global Campus, and staff to the Maryland Cybersecurity Council).

The study addressed three sets of questions focus on state and local cybersecurity:

- Task 1: Cybersecurity Governance, was led by Dr. Gregory von Lehmen (Special Assistant for Cybersecurity, University of Maryland Global Campus, and staff to the Maryland Cybersecurity Council).
- Task 2: Executive Branch Agencies, was led by Charles "Chip" Stewart (State Chief Information Security Officer),

[5] See Appendix A.

[6] These hearings were held on June 23, September 29, and November 9. The hearings can be viewed at https://mgaleg.maryland.gov/mgawebsite/Committees/Media/false?cmte=mjm&clip=MJM_6_23_2021_meeting_1&ys=2021rs, https://mgaleg.maryland.gov/mgawebsite/Committees/Media/false?cmte=mjm&clip=MJM_9_29_2021_meeting_1&ys=2021rs, and https://mgaleg.maryland.gov/mgawebsite/Committees/Media/false?cmte=mjm&clip=MJM_11_9_2021_meeting_1&ys=2021s1, respectively. The November 9 hearing included a presentation of preliminary findings and recommendations by the ad hoc committee.

[7] SB 69 (Cybersecurity and Coordination Office – Establishment and Reporting) at https://mgaleg.maryland.gov/2021RS/bills/sb/sb0069T.pdf

[8] The amendment was requested by the House Health and Government Operations Committee "requiring the Maryland Cybersecurity Council to conduct a certain study on cybersecurity coordination and operations in the State; requiring the Council to submit a certain report to certain committees of the General Assembly on or before a certain date; and generally relating to a report on cybersecurity coordination and operations". See https://mgaleg.maryland.gov/2021RS/amds/bil_0009/sb0069_82658501.pdf

- Task 3: Local Units of Government, was led by Acting Secretary Russell Strickland Maryland Department of Emergency Management and Kevin Kinnally (Legislative Director, Maryland Association of Counties

The study's understanding of the 'current state of play' of cybersecurity at the Maryland State and local levels was shaped by a variety of sources. These include discussions with Mr. Stewart and Acting Secretary Strickland, formal surveys of state agencies and county governments, meetings with groups of school district and county cybersecurity officials, and testimony provided to the Joint Committee over the summer and fall by the Maryland Association of Counties, the Maryland Municipal League, and the Maryland Association of County Health Officials, among others.

Altogether, the study makes 35 recommendations.[9] These stand as the consensus recommendations of the ad hoc committee. Executive branch employees on the ad hoc committee did not participate in the decision-making related to recommendations. The recommendations were shaped by best practices as captured primarily in various publications of the National Institute for Standards and Technology (NIST) and interviews with cybersecurity officials in other states and the private sector and staff at the Center for Internet Security (CIS). Discussion with staff at the National Association of State CIOs (NASCIO) and the National Governors Association (NGA) also provided important information. A draft of the study was provided to the Subcommittee on Critical Infrastructure of the Maryland Cybersecurity Council for review and a number of suggestions by subcommittee members were included in the final document.

The committee is grateful for the support of the Governor's Office, Secretary Michael Leahy (Department of Information Technology), Acting Secretary Russell Strickland, and Senate President Bill Ferguson and House Speaker Adrienne Jones who made the Department of Legislative Services staff available to the ad hoc committee. The committee would also like to recognize the leadership roles of Senator Pinsky (Chair, Senate Education, Health and Environmental Affairs Committee) and Delegate Shane Pendergrass (Chair House and Government Operations Committee) in coordinating their committee processes so critical to the shape of cybersecurity legislation.

Finally, the committee would like to express our appreciation to CHHS interns who participated in its work: Serena Chenery, Robert Layne, Gavin Rader, Alek Stathakis, Stephanie Vangellow, Mike Rovetto, and Makenzie Donaldson as well as the Christopher Lidard and Connor Armstrong from the office of Senator Katie Fry Hester. In addition, the committee is thankful to the members of the Maryland Infragard for their thoughtful review of the study.

This study is divided into three sections, corresponding to the three sets of questions mentioned above.

[9] See Appendix B for the summary of recommendations.

GOVERNANCE[10]

Question 1: What are the roles of the State Chief Information Security Officer (SCISO), the Maryland Cybersecurity Coordinating Council (MCCC), the Department of Information Technology (DoIT), the Maryland Emergency Management Agency (MEMA), and local jurisdictions *in addressing cybersecurity risk*, and how can the state foster more collaboration and definition of roles between these bodies?

Discussion

Cybersecurity governance is embodied in the framework of laws, policies, structures, and processes that determine how cybersecurity risk is managed within the enterprise.[11] It addresses the decisions that need to be made about threats, who should make those decisions, how those decisions should be informed, who is responsible for translating decisions into investments and programs, and how it is determined whether cybersecurity programs are effective.[12] As such, cybersecurity governance pertains to all activities necessary to manage risk: strategic planning, budget and procurement, risk identification and mitigation, incident response, information sharing, and workforce development.[13] Mature governance results in deliberate risk trade-offs with the entire enterprise in view and helps ensure coherent and consistent cybersecurity practices that manage risk within limits acceptable to the enterprise.

As the Center for Internet Security has observed, governance at the state level takes various forms:

> Some have the "centralized structure" recommended by many experts, essentially placing decision-making authority on cybersecurity in one or more central organizations and, in many cases, embedding cybersecurity governance within the state's centralized information technology services organization. Others have a more decentralized approach to establishing the desired control and influence, while still others have implemented hybrid models with a mix of centralized and decentralized authorities, roles, and responsibilities.[14]

[10] Dr. Greg von Lehmen developed this section with research support of three CHHS interns: Serena Chenery, Robert Lane, and Gavin Rader. The section benefitted from discussions with Acting Secretary Russell Strickland (MDEM), Charles Stewart (Maryland State CISO), Daniel Dister (CISO, State of New Hampshire), Michael Geraghty (CISO, State of New Jersey), Shawn Riley (CIO, State of North Dakota), Kevin Ford (former CISO, State of North Dakota), Mathew Pincus (Director of Government Affairs, National Association of State CIOs), John Guerriero (Senior Policy Analyst, National Governors Association), Tony Sager, Brian DeVallance, and Curtis Dukes (Center for Internet Security), Jamie Ward (Multi-State Information Sharing and Analysis Center), and Kirk Herath (former Associate General Counsel for Technology, Nationwide Insurance). The views expressed in this section are solely those of the ad hoc committee.

[11] CISA, State Cybersecurity Governance Case Studies (2017), p 5., at https://www.cisa.gov/sites/default/files/publications/Cross_Site_Report_and_Case_Studies_508.pdf

[12] CIS, Managing Cyber Threats Through Effective Governance (2020), p 1., at https://www.cisecurity.org/white-papers/managing-cyber-threats-through-effective-governance/

[13] CISA, opus cit., p. 1

[14] Ibid, p. 4

As a trend, the American states are moving toward consolidation and centralization of their IT function in general.[15] What consolidation looks like in a given state will vary; as it is often said, 'When you've seen one state, you've seen one state.' But driving the trend are the compelling management and security benefits that come with centralization. These include economies of scale in the consolidation of vendors, platforms, tools, uniform policies and procedures, and ideally a greater awareness of risk across the enterprise.

Two states that represent a high level of consolidation of vendors, platforms, and tools are Vermont and North Dakota. In Vermont, responsibility for all Executive Branch IT and security policy and operations resides with the "Agency of Digital Services" (ADS). This centralization, which absorbed all agency IT and security functions into ADS, was accomplished via a 2017 Executive Order. Under the order, there is one Executive Branch CIO and one CISO. While IT and security staff remain embedded in agencies, they all report to both the State CIO and CISO. There is one IT/security budget.

With this centralization of authority and responsibility, complete visibility into agency IT and security was realized. It eliminated shadow IT systems, enabled better prioritization of modernization needs, produced savings in the consolidation of vendors and contracts (reportedly $15 million savings to date), and has given the Executive Branch the flexibility to respond to shifting needs. For example, during the COVID -19 pandemic, ADS has been able to assign IT and security staff to the state health department from other agencies.[16]

In North Dakota, the Executive Branch "Information Technology Department" is centrally responsible for the IT and security strategy, policies, standards, guidelines, staffing, and services across the Executive Branch. While the judicial and legislative branches set their own strategies and possess their own data centers, the department, by law, runs the network operations and cybersecurity for those branches.[17] Likewise, the Department centrally defends cities, counties, K12, and higher education across the state.

The State Chief Information Security Officer (SCISO)

Consistent with this consolidation trend, Executive Order 01.012019.07 (Maryland Cyber Defense) establishes the SCISO's office within DoIT with authorities vis-à-vis the Executive Branch.[18] Under the order, the SCISO is appointed by the Governor and reports to the DoIT Secretary. The SCISO office is responsible for direction, coordination, and implementation of Executive Branch cybersecurity "including but not limited to" "standards to categorize all information and information systems collected or maintained by or on behalf of each unit of" the Executive Branch; related guidelines, "security requirements" for each category; assessing categorization and implementation, deciding which systems can be connected to the Maryland Network, managing security awareness training, "assisting in the

[15] See The Deloitte-NASCIO 2020 Cybersecurity Study, p 13, at https://www2.deloitte.com/content/dam/insights/us/articles/6899_nascio/DI_NASCIO_interactive.pdf

[16] Testimony of John Quinn, CIO, Agency of Digital Services, State of Vermont, before the Joint Committee on Cybersecurity, Information Technology, and Biotechnology, on June 23, 2021, at https://mgaleg.maryland.gov/mgawebsite/Committees/Media/false?cmte=mjm&clip=MJM_9_29_2021_meeting_1&ys=2021rs

[17] In a September 30, 2021, email, SCIO Shawn Riley noted that the "Judicial and Leg branches both control their own data centers (but rent space from ours for many systems) and have the ability to set their own strategies. They have their own IT teams for things like desktop support, data analysis, programming, etc. We do work closely together for many things, but only Network operations and Cyber Security are solely owned by NDIT."

[18] See https://governor.maryland.gov/wp-content/uploads/2019/06/Maryland-Cyber-Defense-Initiative-EO-01.01.2019.07.pdf

development of data management, data governance, and data specification standards to promote standardization and reduce risk", and "assisting in the development of a digital identity standard and specification". To "provide advice and recommendations to the SCISO", the EO also establishes the Maryland Cybersecurity Coordinating Council (MCCC).

There has been an ongoing discussion about whether the CISOs of organizations should report to the CEO or the CIO. One view is that the CISO should report to the CIO, and there are several reasons for this. There is a balance between technology and cybersecurity budgets, and there needs to be an epicenter within the organization knowledgeable enough to strike that equilibrium. Moreover, there is a lot that happens within the IT ecosystem when new tools are introduced, and these considerations likewise need to be arbitrated at the same table. The argument is that the CIO is in the best position to be this balancer or arbitrator. This is the model that most states follow.

The other view is that in organizations providing services and products there is a natural tendency to prioritize investment in enhanced services or faster availability of products at the expense of cybersecurity. Consequently, it is argued that it is necessary to separate cybersecurity as a function, establish the CISO on parity with the CIO, and implement separate reporting lines to the CEO. This arrangement raises the profile of cybersecurity within the C-suite and permits the CISO to advocate directly for the cybersecurity needs of the enterprise. It also places responsibility for that cybersecurity at the CEO level. Among US states, Arizona is the only one to implement this model.

Within the authorities outlined by the Governor's EO, the SCISO's risk management role overlays the current geography of the Maryland Executive Branch where some agencies have their IT security directly managed by DoIT while most retain their own CIOs, security teams, and security budgets. Those agencies for which DoIT directly administers their IT and cybersecurity are sometimes referred to as "within the enterprise".

Given this geography, the SCISO's risk management role within the Executive Branch is exercised in a number of ways:

- Through the State Security Manual and security goals and objectives included in the Statewide IT Master Plan (ITMP). The State Security Manual articulates security policies, procedures, standards, roles, and responsibilities that Executive Branch agencies are obligated to implement, and the ITMP incorporates cybersecurity goals and objectives to advance the state's cybersecurity management.
- By setting rules for the use of the Maryland Network. This affects all agencies since all agencies are required to use the Maryland Network. The SCISO can decide what devices can be connected to it or what applications run on it.
- By running DoIT's 24/7 Security Operations Center (SOC). The SOC monitors the Maryland Network, managed devices (mobile devices like state laptops), managed Software-as-a-Service platforms, and email to capture, analyze and respond to events that are suspicious. To reap the full benefits of the SOC, DoIT has mentioned the goal of deploying security orchestration automation and response (SOAR) to permit reaction to suspicious events at machine speed.
- By acquiring and sharing threat intelligence gleaned from the SCISO's threat intelligence staff and from third parties like the Multi-State Information and Analysis Center (MS-ISAC).
- By doing vulnerability scanning of state agency systems. This has recently included internal scanning of agency applications, 'light touch' scanning of websites and ports, and scanning of the boundaries of vendors touching state systems.
- By conducting security assessments.
- By ensuring security reviews of "major" procurements.

- By requiring participation in cybersecurity training (which the SCISO's office does through the Infosec Institute).

The SCISO's exercise of these risk management activities appears to operate under a number of constraints, including budget and lack of authority.[19]

- *Security assessments have been hampered by limited staff/human resources*. While the Governor's Office has provided $5M to support assessments, as of the fall of 2021, DoIT has indicated that five or six of these assessments were underway. To get these off the ground, they are being conducted at a basic level. DoIT points out that there are 114 units of state government and that many of these have subunits, so it is unlikely that the assessments across the state Executive Branch will be possible with the funding provided. Vendor support would speed the progress of the current assessment initiative but securing such support has been slowed by the COVID-related state procurement backlog.[20]
- *DoIT has extremely limited visibility into systems and applications run by agencies*. It was noted in testimony that systems and applications not reported are found when incidents occur. DoIT states that it is aware of larger systems used by agencies but underscores that those unidentified smaller systems and applications pose similar risks.[21]
- *DoIT does not have visibility into the cybersecurity budgets, dedicated staffing, and security priorities of Executive Branch agencies 'outside of the enterprise'*.
- *DoIT has limited visibility into agency compliance with security policy for those agencies whose IT and security it does not directly manage*. However, DoIT states that it is in the process of implementing a governance risk and compliance (GRC) module as part of "ServiceNow[22]" that will enable DoIT to track agency compliance with security policy and will aggregate the information that will create the possibility of more strategic risk management across the Executive Branch. The target for the initial rollout of the GRC module is this FY.
- *There are exposures in the procurement process.* Agency purchases of devices and systems within their delegated authority do not receive DoIT security reviews.[23] Further, services contracts allowing vendors to access state databases (e.g., medical billing) do not go through DoIT security review and are not covered by state security requirements.

Centralization of the IT and security functions is an answer to many of these problems. With centralization comes visibility and with visibility there is clarity about what needs to be defended.

[19] See for example DoIT testimony to the Joint Committee on Cybersecurity, Information Technology, and Biotechnology, that the difficulty of DoIT knowing all legacy systems within the agencies is as much a "data management and governance issue" as it is a hardware issue. Hearing on June 23, 2021, at https://mgaleg.maryland.gov/mgawebsite/Committees/Media/false?cmte=mjm&clip=MJM_6_23_2021_meeting_1&ys=2021rs

[20] Ibid.

[21] Ibid.

[22] ServiceNow is a platform-as-a-service offering that provides Information Technology Service Management, IT Operations Management, "Governance, Risk, and Compliance," and other business workflows.

[23] "USGs [Units of State Government] hold independent authority ("Delegated Authority") to conduct procurements to expend amounts less than $50,000 without going through DGS OSP and DoIT (known as "Small Procurements")." Memorandum of October 1, 2019, from Secretary Leahy and Secretary Churchill to agency heads regarding "Information technology requests, State of Maryland procurement reorganization effective October 1, 2019". As an example, the purchase of 30 laptops manufactured in an adversary nation pose a security risk.

Moreover, centralization supports discussions about how security IT resources and security budgets could be pooled to achieve greater economies of scale and risk reduction.

Recommendations

- *Governance Recommendation 1.* That the General Assembly codify the key elements of the EO (Maryland Cyber Defense Initiative), viz. the SCISO's position, the SCISO's Office of Security Management and the Maryland Cybersecurity Coordinating Council as well as the authorities outlined in the recent Executive Orders (State Chief Data Officer) and (Maryland Data Privacy.)[24]
- *Governance Recommendation 2*. That the SCISO continues to be appointed by the Governor.
- *Governance Recommendation 3.* That the IT functions of all agencies in the Executive Branch be centralized in DoIT and brought into the "enterprise". All IT budgets would become part of DoIT's budget and agency IT security staff would report to the CIO.
- *Governance Recommendation 4.* That the cybersecurity functions of the Executive Branch be centralized and made part of the "enterprise". All cybersecurity budgets would become part of one cybersecurity budget and agency cybersecurity staff would report to the SCISO.
- *Governance Recommendation 5*. That DoIT makes the implementation of its GRC module a priority.
- *Governance Recommendation 6*.That the State mandates basic security requirements as part of the procurement process for state contractors who will have access to state databases or systems consistent with a widely recognized standard such as NIST SP 800-171, ISO27001, CMMC, or other.
- *Governance Recommendation 7.* That DoIT implements a security regime for all agency procurements below $50,000 of systems or devices that connect to networks, whether through whitelists or other review procedures. Anything connected to or running on the network should have some verified level of trust.
- *Governance Recommendation 8.* That the General Assembly, the State Judicial Branch, and the University System of Maryland be required to annually certify compliance with DoIT minimum security standards.

The Maryland Cybersecurity Coordinating Council (MCCC)

Effective cybersecurity governance requires engagement with stakeholders for at least three reasons:

- How security controls ensure confidentiality, integrity, and availability of data and systems are implemented requires tradeoffs in support of agency business functions. Data access controls that are too restrictive, for example, could make it too difficult to effectively provide certain citizen services. Agencies are best positioned to inform the SCISO about how to implement controls aimed at confidentiality, integrity, and availability in the context of agency business needs.
- Engagement creates buy-in and makes implementation easier.
- An enterprise-wide stakeholder group, if properly informed, is best positioned to perform the "Tier 1" risk framing, risk monitoring, and the risk assessment function. Among other things, Tier I risk

[24] Executive Order 01.01.2021.09 (State Chief Data Officer) and Executive Order 01.01.2021.10 (Maryland Data Privacy) at https://governor.maryland.gov/wp-content/uploads/2021/07/State-Chief-Data-Officer.pdf and https://governor.maryland.gov/wp-content/uploads/2021/07/Maryand-Data-Privacy-EO.pdf, respectively.

assessment results in recommendations concerning the prioritization of cybersecurity risk across the enterprise and of the investments that can mitigate the most risk.[25]

The Maryland Cybersecurity Coordinating Council is in a position to perform these essential governance roles within the Executive Branch. As the EO stipulates, the MCCC must:

- Be chaired by the SCISO
- Include the heads of Executive Branch agencies to help shape policy and procedures and perform the Tier 1 risk assessment function. In this connection, the EO states that the "The MCCC shall provide advice and recommendations to the SCISO "about i) strategy and implementation of cybersecurity initiatives and recommendations; and ii) building and sustaining the state's capability to identify, mitigate, detect cybersecurity risk, and respond and recover from cybersecurity-related incidents".[26]

The MCCC is gradually maturing as a stakeholder body informing State Executive Branch cybersecurity under the EO. To date, the MCCC has met eight times.[27] Much of the MCCC's work has focused on building shared definitions and education. Earlier this year, it established a working group to formalize the Authorization to Operate processes and documents. As the working group completes its mission, it will present the documents to the Maryland Cybersecurity Coordinating Council. In addition, the council has contributed to several policy and guidance documents that were requested by members and other units. The Maryland Cybersecurity Coordinating Council has evolved to voting on the approval of these documents as a mechanism to ensure consensus in the contents, with the expectation that this will result in increased compliance with these policies, guidelines, and processes.

As yet, the MCCC has not begun performing its enterprise-wide cybersecurity risk prioritization to guide investments that reduce risk across Executive Branch State agencies. As a best practice—one required of federal agencies—each unit within an agency should identify what its business functions are, what systems it uses, and what the consequences to the unit's mission would be if the system were compromised. These "risk registers" should be aggregated upwards to the agency executive level with business functions and systems prioritized by importance. These agency registers in turn should be integrated into a State Executive Branch wide document that would prioritize business function and system across the enterprise and enable the prioritization of risk and of cybersecurity investments to best reduce risk.

Recommendations

- *Governance Recommendation 9*. That the risk assessments required by the State Security Manual be performed, aggregated, and prioritized by agencies and used by the MCCC to prioritize risk across the Executive Branch and to connect that with the budgeting process, i.e., make corresponding recommendations for security investments that will have the greatest impact in buying down risk.[28]

[25] NIST SP 800-30 (r1) (Guide to Performing Risk Assessments), 2012, at https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf and NIST 800-39 (Managing Information Security Risk), 2011, at https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-39.pdf

[26] See Section D (2).

[27] See MCCC meeting minutes at https://doit.maryland.gov/Pages/cyber-security.aspx

[28] A methodology for performing this activity is discussed in NISTIR 8276 (Integrating Cybersecurity and Enterprise Risk Management), October 2020, at https://nvlpubs.nist.gov/nistpubs/ir/2020/NIST.IR.8286.pdf

- *Governance Recommendation 10*. That the meetings of the MCCC be exempt from the Open Meetings Act so that it can be an ongoing forum for the sharing of information, discussing sensitive cybersecurity issues, and shaping recommendations to the SCISO. This is consistent with the fact that the MCCC does not make or recommend public policy and that there are other ways of ensuring accountability for the cybersecurity effort of the state—both as to process and outcomes—that are discussed below.
- *Governance Recommendation 11*. That the MCCC be expanded to include representatives of the General Assembly, the University System of Maryland, and the state judiciary as non-voting members and that the chair have the prerogative to appoint or invite other participants.

The Maryland Department of Emergency Management Agency (MDEM)

Under Title 14 of the Public Safety Article, MDEM "may act to reduce the disaster risk and vulnerability of persons and property located in the State; (2) develop and coordinate emergency planning and preparedness; and (3) coordinate emergency management activities and operations".[29] This remit includes "disaster risk" to state and local governments as pivotal parts of the nation's critical infrastructure. With mounting examples of cyber attacks on state and local jurisdictions across the nation, MDEM has identified disruptions due to cyber attacks as an important hazard to address in its consequence management planning.[30] Such planning has now become an integral part of "emergency management" as defined in the statute:

> "Emergency management" means the planning, implementing, and conducting of risk reduction and consequence management activities across the mission areas of prevention, protection, mitigation, response, and recovery to enhance preparedness, save lives, preserve public health and safety, protect public and private property, and minimize or repair injury and damage that results or may result from emergencies.[31]

Under a pilot grant program funded in the National Capital Region by the U.S. Department of Homeland Security, MDEM has established a Cyber Preparedness Unit (CPU) within the Consequence Management Directorate. The new unit is staffed by three FTEs whose backgrounds are a hybrid of planning and cybersecurity. The CPU is focused on county government, public safety departments, and school districts. Its mission is to work with local jurisdictions to develop relationships between emergency management and the cyber / IT professionals within their jurisdiction (government, public schools, public safety), assist them in developing [cyber] response/ disruption plans, training on those plans, and exercising those plans. These plans include updates to existing emergency management plans to take into account the dependencies on IT systems of essential county services, including the 911 centers. As suggested in the section on local government cybersecurity, there is a need for these updates.

In practice, this means working with the 26 locally appointed emergency directors and the IT staff for the 24 counties, Annapolis, and Ocean City. The CPU does not have the capacity to work directly with all cities across the State because of the number of staff members that would be involved.[32] While MDEM

[29] Title 14 of the Public Safety Article Subtitle 1 §14-103(d)(1-3)

[30] Remarks by Acting Secretary Strickland at a joint meeting of county emergency managers and county IT and cybersecurity staff as part of the study on September 28, 2021.

[31] Title 14 of the Public Safety Article Subtitle 1 §14-101(d)(1)

[32] There are 157 municipalities in the state. See https://planning.maryland.gov/MSDC/Pages/pop_estimate/popest_muni.aspx

depends on the counties to work with the cities, it is willing to support counties that assist cities in developing their own plans to manage the consequences of cyber attacks.

While the focus of consequence management planning is for the aftermath of a cyber event, the process that informs the plan is likely to have positive consequences in the preparedness phase. Specifically, MDEM's consequence planning brings local emergency management staff together with the county IT staff, 911 center directors, and others to identify cybersecurity threats, vulnerabilities, and risk mitigations. All of these items are necessary to focus emergency management plans—a likely outcome is an improvement in the cybersecurity posture of the jurisdictions doing the planning. MDEM's Cybersecurity Planning Unit intends to test drive this planning process by first creating a cyber consequence management plan for the agency itself. This model is not new, the practice of having a subject matter expert on staff as part of the planning effort has precedent. To assist with nuclear disaster planning, it has had a nuclear energy subject matter expert on staff.

MDEM's role is as a convener, planner, and coordinator of emergency management efforts for all hazards faced by the state in coordination with the emergency managers in each local jurisdiction. MDEM and the CPU coordinate the integration of cyber incidents into the implementation of the State's Consequence Management Operations Plan (CMOP). In cases where there is an emergency precipitated by a cyber attack, MDEM's protocol is to receive the request for assistance, review and validate it, source it to the state agencies able to provide assistance, monitor the effort, and eventually close out the action.[33] Cyber attacks can precipitate down-stream effects on state and local services which necessitate significant response and recovery coordination, a key MDEM role outlined by statute. Generally, local jurisdictions should request assistance through the county emergency management office which conveys the request to MDEM. Because MDEM's role has traditionally been defined in practice by natural disasters, jurisdictions needing cybersecurity assistance have sometimes reached out directly to DoIT. As MDEM engages locally on cybersecurity consequence management, it will review the procedure for cyber-related emergencies in the same way as for any other emergencies.

The question was asked whether a special cybersecurity planning unit in MDEM blurs lines between MDEM and the SCISO's Office of Security Management. There is no one rule across the states. As part of its 'all hazards approach', New Jersey houses its SCISO within the Office of Homeland Security and Preparedness. The SCISO's office works directly with local jurisdictions with some help from the emergency staff on preparedness. In North Dakota, the emergency management and homeland security functions report to the Adjutant General and have their own cyber teams. But in the event of a compromise where they may be called to respond, their line of reporting changes to the SCISO as incident commander.

Recommendations

- *Governance Recommendation 12.* The Maryland Joint Operations Center (MJOC) is the state's 24/7 emergency operations center capable of quickly and effectively managing initial emergency response coordination in support of state and local governments. The MJOC has the responsibility to receive, analyze, and disseminate information to appropriate MDEM and interagency personnel with areas of responsibility for hazards in Maryland. Local governments should report cyber attacks or network disruptions to the MJOC, including those attacks on state

[33] Consequence Management Operations Plan (2019), pp 34-35, at https://mdem.maryland.gov/Documents/Maryland_Consequence_Management_Operations_Plan%202.0_January%202019_FINAL%201.pdf

systems being used by local governments (e.g. METERS). MJOC will notify the appropriate agencies including DoIT through the MDSOC.

Local Units of Government and Cyber Risk

A key argument for a whole-of-state approach to cybersecurity is that state and local exposures are intertwined, and interruptions of key locally managed services can quickly become statewide emergencies. As one Maryland county CISO states:

> …many counties rely on systems provided by the state, [so] vulnerabilities that are introduced at the state flow down to the counties. It would be best to have the state Agencies remediate their legacy applications so that risk is reduced for the local jurisdictions. For example, METERS[34] which is a major risk [to] all local jurisdictions and [is] owned by DPSCS. [There are also] [m]ultiple legacy health applications owned by the Department of Health and numerous other dated application[s] that do not have an overarching support framework across many state Agencies. Having the state Agencies remediate and work with the local jurisdictions would go a long way with reducing the risk to local jurisdictions.[35]

But the exposure runs in the other direction too. As one county IT official noted, local jurisdictions create many endpoints to numerous state systems that can be compromised as well.[36]

Beyond these network-level risks that state and local governments share with each other, there are simply the spill-over effects on state government when local jurisdictions are independently impacted by cyber disruptions. As two recent examples from Baltimore City and Baltimore County Schools highlight how the cyber disruptions required the commitment of DoIT staff away from their normal roles to support the local security teams. Due to the emergency response,their effectiveness in day-to-day responsibilities is thus diminished.

If these mutual dependencies call for a 'whole of state' approach to cybersecurity, the question is what a corresponding governance structure would look like. This is discussed below.

Question 2: How can the state better collaborate with the federal government, other states, and the private sector to leverage resources, share best practices, and better understand emerging cybersecurity threats?

Discussion

There are a number of practical resources from the private sector and the federal government that state and local governments in Maryland are leveraging. Nonetheless, there is opportunity for the state to take a leadership role in promoting these resources and in offering aid more directly itself.

There are approximately 100 public entities in Maryland—including the State government and political subdivisions—that are members of the Multi-State Information Sharing and Analysis Center (MS ISAC). The MS ISAC is part of the nonprofit Center for Internet Security funded in part by the U.S. Department of Homeland Security. Membership is open to any public entity at no cost. The ISAC has over 15,000

[34] METERS is a state-run portal used by public safety agencies.
[35] Comment on survey of county CIOs.
[36] Comment on survey of county CIOs.

members, including county and city governments, school districts, school boards, boards of election, state agencies, and public higher education, among others.

The ISAC operates a 24/7 Security Operations Center (SOC) that monitors and analyzes threats targeting SLTT entities. Examples of no-cost services include the daily threat reports, indicators of compromise, lists of compromised IP addresses, malicious domain blocking (MDBR), a web-based platform where members can submit suspicious code, files and other artifacts for malware analysis, and the assistance of a remote computer emergency response team (CERT) for members who are severely disrupted and need assistance. Membership also includes access to SecureSuite products and services: the CIS Benchmarks (product configuration recommendations), CIS Critical Security Controls, and tooling (CIS-CAT Pro, CSAT Pro) to assess enterprise configurations. Likewise, the ISAC offers various white papers, webinars, and networking opportunities for free.

There are also low-cost fee-based services. These include the ISAC's network security monitoring and analysis service (Albert), managed security services (MSS), and vulnerability assessment services. Most recently, the ISAC has added a fee-based endpoint monitoring and protection service in partnership with a prominent cybersecurity vendor. As a nonprofit, the ISAC works to keep fees within reach of public entities. For example, the price range for an Albert subscription for jurisdictions whose departments ride on the same internet connection is $10,800 to $25,200 per year with a one-time cost of $6,000 or $8,000 for the sensor on the internet connection. Moreover, the ISAC will discount pricing where states seek to negotiate bulk participation of their jurisdictions. Service is within industry standards. With Albert, detection, analysis, and notification of the affected member occurs within an average of six minutes.[37]

Approximately 250 governments or government agencies in Maryland participate in the .gov domain initiative of the Cybersecurity and Infrastructure Security Agency (CISA) at DHS. CISA offers a variety of no-cost services through its Cyber Resources Hub,[38] such as risk and vulnerability assessment, phishing campaign assessment, and remote penetration testing. As a practical matter, however, the most accessible of its services is assistance in transitioning to the .gov domain. The .gov domain is administered exclusively by CISA. There is an application process but no charge by the agency for its assistance. Spoofing (imitating) the .gov domain is much more difficult, providing more security for jurisdictions and citizens alike.

Services can also be procured from other states. The North Dakota Department of IT provides internet backbone services, network operations, and cybersecurity for all public entities in the state. Its license agreements with vendors are at the 250,000-user level and bring with it the buying power and discounts equivalent to a Fortune 11 company. Under North Dakota law, any government agency outside the state can also access these contract vehicles. Membership is multi-tiered, starting with information sharing and working up to network operations management and cybersecurity with an automated response playbook. The Minneapolis School District, the largest in that state, participates in the North Dakota program. Similarly, North Dakota, South Dakota, and Montana have combined to form a Joint Cybersecurity Operations Center with three more states likely to join.

With respect to the federal government, Maryland and its local governments participate in various DHS grant programs. These include the State Homeland Security Grant (SHSG) and the Emergency Management Planning Grant (EMPG). Together, these grants bring more than $12 million to the state

[37] Reported in discussions with an MS-ISAC representative.

[38] See https://www.cisa.gov/cyber-resource-hub)

each year, but most of these funds are spent on sustaining Emergency Management (EM) offices and their activities at the local level, with very little funding available for cybersecurity.

Some states manage the SHSG in a manner that permits investments to align with security priorities. Iowa and Virginia are two examples. By design, 80% of SHSG funds must be allocated to local governments and at a minimum 25% of that amount must be targeted on national preparedness goals. In Maryland, the funds are allocated to jurisdictions according to a formula. The jurisdictions make decisions about how they wish to spend their allocation and propose these to MDEM for approval. In Iowa, the 80% has been used by the state government to fund cybersecurity licenses, hardware/appliances, and tools that local governments as well as the state can use[39]. This has enabled all of Iowa's counties to take advantage of these services**.** Virginia places the 80% in one bucket and awards are made on a competitive basis with a focus on impact.

In Maryland, it is not practical to try to re-program SHSG or EMPG funds in this manner since local jurisdictions rely on the funds for sustainment of the EM function. But the same approach could be achieved by establishing a revolving grant or loan fund for cybersecurity investments that would be managed by either DoIT or the MDEM and 100% sourced through appropriations. But the same approach could be achieved by establishing a revolving grant or loan fund for cybersecurity investments. The argument for such a fund is that it would represent the principle of paying forward to reduce cyber compromises in lieu of the costs of managing and remediating compromises after they occur.

Finally, cybersecurity workforce development is an area of governance that is urgent for both the public and private sectors. There are a number of efforts across the state to address this need. As one example, the state has moved recently to produce a coordinated effort to help build the talent pipeline for state agencies through the Maryland Institute for Innovating Computing (MIIC). Established through a Memorandum of Understanding (MOU) between the state and UMBC this summer, MIIC is intended to serve as a hub for bringing student talent from across the University System of Maryland to "address high-impact, high-value technological and data projects in state agencies", to house a strategic IT investment funding for faculty and student teams to develop "scalable solutions to IT problems currently considered intractable", and to "activate a multilevel workforce development strategy building on the Maryland Technical Internship Program and current workforce upskilling through UMBC. The execution plan to launch the program will be funded at $500,000.

Recommendations

- *Governance Recommendation 13.* That the state consider partnering with other states such as North Dakota to leverage even greater buying power for IT and cyber security services both for the state government itself but also for its political subdivisions.
- *Governance Recommendation 14.* That MDEM incorporate information sessions about the MS ISAC and CISA's .gov initiative in its periodic training summits with local jurisdictions to ensure awareness of the services available and that the Cyber Preparedness Unit serve as a bridge to assist local entities where needed to access these services.

[39] NASCIO, Stronger Together: State and Local Cybersecurity Collaboration (2020), at https://www.nascio.org/wp-content/uploads/2020/01/NASCIO_NGA_StateLocalCollaboration.pdf

Question 3: How can the state improve its cybersecurity governance to consider county and municipal needs, respond to deficiencies revealed by audits, and increase compliance/awareness of state strategy and standards?

Discussion

This question squarely concerns how Maryland might implement a 'whole of state' approach to cybersecurity and what the role of DoIT is in this connection. This is not a new question for the General Assembly as evidenced last session by SB 49/HB 38[40] (which passed) and SB 69/HB 879[41] (which did not).

By passing SB 49/HB 38, the General assembly took a clear step in the direction of a 'whole of state' approach to cybersecurity. This law expands the duties of the DoIT Secretary to "advise and consult with the legislative and judicial branches regarding a cybersecurity strategy" and in "consultation with the Attorney General" a) to advise and oversee a consistent cybersecurity strategy for units of state government, including "institutions under the control of the governing boards of public higher education" and b) develop "guidance on a consistent cybersecurity strategy" for all political subdivisions of the state.

SB 69/HB 879 would have codified the key elements of Executive Order 01.012019.07 (Maryland Cyber Defense) while pursuing changes that would have further implemented the whole of government approach by expanding the membership of the Maryland Cybersecurity Coordinating Council (MCCC), providing assistance to local governments, and providing greater visibility into IT and cybersecurity across the Executive Branch and of local units of government (counties, school districts, and local health departments).

Specifically, the bill provided for a SCISO appointed by the Governor and an Office of Security Management with the responsibilities vis-à-vis the Executive Branch as defined in the EO: establishing strategy, policy, standards, requirements, and guidelines. Additionally, assisting with the categorization of information and information systems, making decisions about what can be connected to the Maryland Network, assisting with the development of data management, governance, and standards; managing security awareness training, and assisting with the development of a digital identity standard. The bill preserved the MCCC, but consistent with its 'whole of government' premise, it added representation from the Office of Legislative Services, the Administrative Office of the Courts, the University System of Maryland, and authorized the SCISO as chair to appoint other stakeholders.

Moreover, the bill went further by building out the Office of Security Management to distinguish two roles appointed by the SCISO, a Director of State Cybersecurity to "direct, coordinate, and implement" the aforementioned cybersecurity responsibilities across the Executive Branch and a Director of Local Cybersecurity "to provide technical assistance, coordinate resources, and improve cybersecurity preparedness for units of local government". As part of this redefinition and enlargement the Office of Security Management would also be responsible for identifying federal and other non-state funding to support the work of the Office, to review and certify local cybersecurity preparedness plans, to provide technical assistance in mitigating and recovering from cyber incidents, and to provide technical services to local governments.

[40] SB49/HB38, State Government - Department of Information Technology - Cybersecurity (2021) aleg.maryland.gov/mgawebsite/Legislation/Details/sb0049?ys=2021RShttps://mg

[41] SB69/H879, Cybersecurity Coordination and Operations - Establishment and Reporting (2021), https://mgaleg.maryland.gov/mgawebsite/legislation/details/sb0069?ys=2021rs

With respect to these local responsibilities, the bill recognized the core role that MDEM has with respect to preparedness and response planning in the state and would have required OSM to coordinate with MDEM in helping local units develop preparedness and response plans, implement best practices and guidance from DoIT, connect local units with other resources, and develop appropriate reports on local cybersecurity preparedness. The bill also suggested that OSM ``may" coordinate with MDEM in conducting regional cyber related exercises with the National Guard and the local emergency managers while also establishing 'regional assistance groups' to deliver or coordinate cybersecurity services.

The bill established various mechanisms to create greater visibility into IT and cybersecurity across the levels of government. These include the requirement of Executive Branch agencies to complete a cybersecurity preparedness assessment each year for submission to the Governor and the Office of Security Management. These assessments should provide a variety of far-reaching reports to the Office of Security Management related to their IT and cybersecurity budgets, staffing, projects, vendors, and cybersecurity incidents, among other items.

Similarly, the bill required counties, school districts, and local health departments to annually update their cybersecurity preparedness and response plans for approval by the Office of Security Management and to conduct a cybersecurity preparedness assessment. They are required to report those results as well as other information about their IT and cybersecurity staffing, budgets, cybersecurity awareness training, and employee access to systems and databases. It also required these entities to report cybersecurity incidents to their local emergency manager.

Finally, the bill required units of the legislative and judicial branches, local units of government, and local agencies using the Maryland Network to "certify" to DoIT that it is in compliance with published DoIT minimum security standards.

Both SB 49/HB 38 and SB 69/HB 879 recognize the need of political subdivisions for guidance and assistance. There is a growing number of state governments—North Dakota, Texas, Pennsylvania, and North Carolina as examples—opting to provide or coordinate cybersecurity-related services to local jurisdictions. North Dakota and North Carolina are examples of states that likewise require local jurisdictions to report cyber incidents to the state government, with the state serving to coordinate reporting and responses at the national and law enforcement level. It is noteworthy that services provided to local jurisdictions are not always provided directly but through managed services arrangements coordinated and subsidized by the state in order to boost the coverage of the many jurisdictions involved.

With the concern by state governments about the cybersecurity of local jurisdictions have come governance structures that include local jurisdictional representation. As one example, New Hampshire's Information Technology Council is charged, among other things, to advise on the "statewide information technology plan" and on "statewide information technology policies and standards" and includes representatives of municipal and county governments.[42]

Recommendations

[42] TITLE I, THE STATE AND ITS GOVERNMENT, CHAPTER 21-R, DEPARTMENT OF INFORMATION TECHNOLOGY Section 21-R:6 at https://www.lawserver.com/law/state/new-hampshire/nh-statutes/new_hampshire_revised_statutes_21-r_6

- *Governance Recommendation 15.* That the state directly provide or coordinate the procurement of managed cybersecurity services under state vehicles and subsidized by the state to address the preparedness and response capabilities of local jurisdictions.
- *Governance Recommendation 16.* That there be some consultative process of the SCISO with representatives of political subdivisions on their cybersecurity needs that leverages organic associations and forums that already exist, such as the Maryland Association of Counties, the Maryland Municipal League, the Maryland Association of County Health Officials, and the Public School Superintendents Association of Maryland.

Question 4: What are the implications of the state's current fee–for–service and decentralized model for cybersecurity risk? Are there additional models to be considered?

Discussion

NASCIO's biennial surveys of state CIOs have consistently identified insufficient budget as one of the top three challenges that they face in providing for the cybersecurity of their systems.[43] NASCIO staff estimate that 80% of the states use the charge-back or fee-for-service model. These two facts are not unrelated.

The perspective of several professionals interviewed for this study is that the charge-back model puts agencies in a bind between their own tight budgets, priorities on the one hand and their cybersecurity needs, on the other, forcing them to do their own balancing. This results in a reluctance to take on other costs and obligations. The result is a headwind to the implementation of more robust security by the SCISO and an underfunding of the cybersecurity function. Not surprisingly, the NASCIO 2020 survey reports that the fourth top challenge reported by state CIO's is the lack of a dedicated cybersecurity budget. It is far easier and more effective to fund cybersecurity across agencies from a dedicated central budget.[44]

It is difficult to know how much states spend on cybersecurity as a percentage of their total technology spend. NASCIO staff estimate this to be between 1-3%. As shown below, this is far lower than published federal civilian spending on cybersecurity. The following comes from the OMB's annual analysis of the proposed budget for FY 2021.[45]

	Actual FY 2019	**Estimated FY 2020**	**Proposed FY 2021**
	Billions of Dollars		
Federal Government Cyber	16.937	18.792	18.779
Less DoD Cyber	-8.527	-10.075	-9.846

[43] 2020 Deloitte-NASCIO Cybersecurity Study, p.7, at https://www2.deloitte.com/content/dam/insights/us/articles/6899_nascio/DI_NASCIO_interactive.pdf

[44] Ibid.

[45] Office of Management and Budget. FY 2021: A Budget for America's Future. Analytical Perspectives, pp 221 and 268-269at https://www.novoco.com/sites/default/files/atoms/files/fy_2021_analytical_perspectives_budget_021020_0.pdf

Total Cyber Civilian	8.410	8.717	8.933
Total Civilian IT Budget	51.880	52.930	53.360
% Civilian Cyber /Civilian IT	16.2%	16.5%	16.7%

With federal agencies implementing the NIST Cybersecurity Framework (CsF) the government not only reports spending and budgets broadly for IT and cybersecurity but has begun reporting civilian expenditures for agencies for the specific cybersecurity functions: identify, protect, detect, respond, recover.[46] The annual publication of this data by OMB budget provides a measure of effort and a level of accountability of the federal government's commitment to securing data and vital services against cyber intrusions or disruption.

The size of central IT and cybersecurity budgets for the Maryland Executive Branch are beyond the scope of this study. However, were the IT and cybersecurity budgets across the Executive Branch pooled into central budgets consistent with Recommendations 3 and 4 above, it would provide a baseline for analysis. It is likely that centralization would allow economies of scale and other cost avoidance measures such that additional appropriations might not be required. As noted, this has been the experience of Vermont.[47]

Recommendations

- *Governance Recommendation 17*. That the cybersecurity budget for the state enterprise should be appropriated and not based on the charge-back model.
- *Governance Recommendation 18*. That there be a fully developed, separate cybersecurity strategic plan to undergird the cybersecurity budget requests and that this plan be informed by the 'whole of state' governance group called for in Recommendation 15.
- *Governance Recommendation 19*. That the Governor's annual budget overview should include statistics on the IT budget and the cybersecurity budget across the state enterprise and include a comparison of the cybersecurity budget to the IT budget and an annual OMB overview of the President's budget submission to Congress.

Question 5: How does Maryland's IT strategy and security manual compare with other states? What are the opportunities for improvement?

Discussion

NIST Special Publication 800-53 Revision 5 was used as the evaluation standard of the security manuals of 39 states across the US.[48] If a security manual discussed or provided guidance for a specific security or privacy control family, it was given a passing grade in that specific category and deemed to have satisfied

[46] Ibid, p. 267

[47] Testimony of John Quinn, CIO of Vermont, before the Joint Committee on Information Technology, Cybersecurity, and Biotechnology on June 23, 2021, at https://mgaleg.maryland.gov/mgawebsite/Committees/Media/false?cmte=mjm&clip=MJM_6_23_2021_meeting_1&ys=2021rs

[48] Security and Privacy Controls for Information Systems and Organizations (September 2020), at https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf

the NIST 800-53 Revision 5 requirement. If a security manual did not discuss a security or privacy control family, then that state's manual did not receive a passing grade in that category. An overall maximum score of 20 points was achievable under this method; 1 point for each of the NIST 800-53 security and privacy control family categories.

Maryland tied for second within the top five highest-scoring states under this review method.

State	Score
New Jersey	20/20
Illinois	19/20
Maryland	19/20
Michigan	18/20
California	18/20

The missing elements in the Maryland's security manual concerned supply chain risk management.[49] Revision 5 of NIST 800-53 was published earlier than anticipated, and DoIT has confirmed that supply chain risk management is to be included in its next update to the security manual.

The research team also canvassed the IT master plans and cybersecurity plans (if separate) of 43 states. One key question was how many states had separate cybersecurity strategic plans for their Executive Branches. Another question concerned plans in general, whether IT master plans or cybersecurity strategic plans are used, and whether there are practices that might enhance Maryland's IT master plan.

The publication of a separate cybersecurity plan is in sync with the visibility of cybersecurity as a high-priority issue and as a more extensive guide and justification for greater investment in cybersecurity. Six states—Illinois, Indiana, Iowa, Minnesota, Missouri, and New Jersey—were found to have cybersecurity plans separate from their IT master plans that address the cybersecurity of their Executive Branches. To date, Maryland has included its strategic cybersecurity goals in the State IT Master Plan and has not published a separate strategic plan for cybersecurity.

A key part of governance is the capability to monitor the achievement of strategic objectives, and as a best practice this entails attaching appropriate measures of effectiveness to objectives.[50] In canvassing the strategic plans of states for their Executive Branches, there are plans that have timelines and include metrics (e.g. percentage of staff receiving security awareness training) and identify particular offices or departments responsible for achieving stated goals.[51] State IT strategic plans that best exemplify this

[49] Program management is a security control family. While a discussion of program management is not included in the Maryland Security Manual, it is published separately, and the State is accordingly given credit for it in the evaluation. It may be found at https://doit.maryland.gov/SDLC/Pages/templates-phases.aspx

[50] See ISO/IEC Standard 27014: 7.3.4.

[51] Examples of state plans that exhibit one of more of these elements include those of Georgia, Hawaii, Indiana, and Iowa.

practice are the North Carolina Department of Information Technology Plan for 2019 – 2021[52] and the North Dakota Information Technology Strategy Review.[53]

Recommendation

Governance Recommendation 20. That both the Maryland IT Master Plan and any cybersecurity strategic plan attach timelines and appropriate metrics to the plan's goals and objectives and that the cybersecurity strategic plan provides information about the maturity level of the state's cybersecurity and how goals and objectives will advance that maturity.[54]

[52] See https://it.nc.gov/resources/statewide-it-strategic-plan

[53] See https://www.nd.gov/itd/sites/itd/files/NDIT_StrategicReview_and_Plan_March2020.pdf

[54] An overview of maturity models can be found in *HC3 Intelligence Brief: Cybersecurity Maturity Models* (8/6/2020) at https://www.hhs.gov/sites/default/files/cybersecurity-maturity-model.pdf. For more detailed information, see US Department of Energy, Cybersecurity Maturity Model (July 2021) at https://www.energy.gov/sites/default/files/2021-07/C2M2%20Version%202.0%20July%202021_508.pdf and NIST, Framework for Improving Critical Infrastructure Cybersecurity (April 2018) at https://nvlpubs.nist.gov/nistpubs/cswp/nist.cswp.04162018.pdf

STATE EXECUTIVE BRANCH CYBERSECURITY[55]

Question 1: Has each state agency completed a recent vulnerability assessment, planned to remediate any current vulnerabilities, and prepared to prevent evolving/future cybersecurity risks?

Question 2: Are each state agency's personnel and partners provided sufficient cybersecurity awareness education and training to perform necessary information security-related duties?

Question 3: Are each state agency's personnel and partners provided sufficient cybersecurity awareness education and training to relay necessary security-related information?

Discussion

Cybersecurity at the scale and complexity of a statewide enterprise is encumbered by challenges unlike almost any other organization. Fortunately, Maryland demonstrates a growing commitment to securing the state.

The Annapolis Cybersecurity Summit that took place this July invoked thought leadership, ingenuity, and collaboration between the private sector and the government to address these unique challenges. The summit concluded with the issuance of several executive orders intending to further bolster this commitment, including the creation of the state's first "State Chief Privacy Officer" and "State Chief Data Officer." These roles will complement the State Chief Information Security Officer in meeting the obligation to protect the security and privacy of the data the state holds on citizens.

Overview of Audit Findings

The most notable trend in the audit findings, when viewed over time, is the shifting nature of the findings. In previous years, findings frequently described a lack of foundational cybersecurity controls. Between 2016 and 2019 the Office of Legislative Audits issued 457 reports, of which 77 reports, covering 69 units of state and local government had 84 findings concerning the lack of PII controls.[56] Across these 77 reports, 37.9 million records were identified as containing PII data elements where lack of controls left the records susceptible to increased risk of improper disclosure.[57]

The Department of Information Technology, including the State Chief Information Security Officer, appreciates the work performed by the dedicated team at the Office of Legislative Audits and values the partnership with them in reducing risk by improving the cybersecurity posture of the state. The following four trends show how the audit findings are changing:

[55] Charles Stewart, State CISO, was responsible for the factual discussion of this component of the study. He did not participate in the ad hoc committee's decision-making with respect to the recommendations.

[56] Hook, Gregory, and Stephen Jersey. *Personally Identifiable Information (PII) Audit Issues*, Office of Legislative Audits, 17 Dec. 2019.

[57] Ibid.

Trend 1: Reduction in Repeat Findings Related to Personally Identifiable Information

A positive trend is reflected in the reduction of repeat findings related to Personally Identifiable Information to a single occurrence in calendar year 2020. This is overshadowed by that single instance representing one of the eight total findings related to inadequate protection of Personally Identifiable Information. With 38% of the findings describing issues related to Personally Identifiable Information, units should apply additional energy to implementing technology that provides appropriate protection where possible and modernizing systems that cannot support controls that provide adequate security. As noted above, the addition of data-oriented expertise in the positions of Chief Privacy and Chief Data Officers for the state demonstrates the Governor's commitment to addressing the protection and proper management of sensitive and Personally Identifiable Information.

Trend 2: Increased focus on advanced security features

An increasing trend in the Office of Legislative Audit’s reports, representing four of the twenty-one (19%) findings, is the failure to enable or fully utilize advanced firewall features such as intrusion detection and prevention systems. Because of substantial investments initiated by the Office of Security Management in fiscal year 2020, the State has already addressed one of these findings and has an active project to address two of the remaining three findings.

Trend 3: Increased focus on monitoring

A longer-standing positive trend in the Office of Legislative Audit’s reports is a focus on the monitoring of systems for unusual events and reviewing system logs to detect anomalous behavior. Findings related to monitoring and logging comprise four of the twenty-one (19%) findings in calendar year 2020. This trend is important to monitor because it is predicated on having an environment that is mature enough to support such collection of monitoring data. As such, this finding should be viewed as an indicator of increasing maturity.

Trend 4: Increased focus on contractors and third-party providers

Another trend indicating an improvement is evidenced in the reports from calendar year 2020, with an increased focus on third-party providers and contractors. Again, representing four of the twenty-one (19%) findings, this finding is demonstrative of units maturing from the previous audit cycle and having implemented foundational controls, such as properly configured boundary devices, anti-malware software, and consistent software patching.

Reducing Future Audit Findings

In general, organizations should approach the goal of reducing audit findings with care because overemphasizing compliance in favor of security can result in a spotless report and a breach. The Office of Security Management, at the direction of the State Chief Information Security Officer, has three major initiatives that support the goals of compliance and security.

1. **Continuous Network Risk Assessment Program** – The State Chief Information Security Officer considers identifying and managing unknown and unaddressed network risk to be the most impactful tool in preventing cybersecurity breaches. Through this initiative, the State Security

Operations Center will continue to identify exposed systems that provide adversaries with opportunities and assist with the mitigation of discovered issues.

2. **Cybersecurity Assessment Program** – The Office of Security Management is performing security assessments based on the National Institute of Standards and Technology's Cybersecurity Framework. Through this initiative, we endeavor to improve security for agencies.
3. **Managed Governance, Risk, and Compliance** – The Office of Security Management is implementing tools to support ongoing compliance and risk management. These tools will help the teams responsible for managing systems to ensure compliance with the applicable standards, ultimately leading to fewer negative audit findings.

The outcomes of these initiatives are already demonstrably productive, with the most notable being the elimination of the "Remote Desktop Protocol" (RDP) service from state systems on the Maryland network from January 2020 through present, from what was several dozen systems. With many research organizations finding RDP as the most common intrusion method for ransomware attacks, the first listed initiative has driven a meaningful reduction of risk for the state and reinforced the compliance requirement. While still in their beginning stages, we similarly expect simultaneous downward trends in the severity of audit findings and cybersecurity incidents through the second and third initiatives.

Shifts in cybersecurity risk from increased remote work

Starting in March of 2020, Maryland saw an unprecedented shift to remote work due to the COVID-19 pandemic. For many agencies, including those supported by the Department of Information Technology, the supporting infrastructure was already established and easily reconfigured to meet the increased demand for secure remote access because the underlying architecture integrated cloud design principles such as elasticity. In many cases, because of this architectural foresight, supporting the additional demand required little more than an expedited procurement for additional licenses and a handful of keystrokes to increase system capacity. For several units of state government that relied on less scalable solutions, the shift to remote work became the catalyst for transitioning these units onto remote access solutions offered by the Department of Information Technology. Maryland was also fortunate to have purchased and implemented software in December 2019, that provided additional protection and insight into assets not connected to the enterprise network. These factors, in combination with implementing enhanced protection for email and transitioning security operations in-house, provided protections that supported better defense for the state from cyber-attacks.

While much of the state government was prepared for this shift, vendors and other organizations in the supply chain were less prepared. Maryland was fortunate in that it experienced limited impacts resulting from supply-chain related incidents and is continuing to bolster security controls to better protect itself from threats introduced through vendors and software providers. In considering the risks from third parties and the supply chain, the Office of Security Management began efforts in late 2020 to consolidate and automate risk management in this area. Related efforts are underway with an expected project completion date of December 2021, after which units may use these tools to track and manage identified risks.

One notable area of increasing risk was a significant uptick in fraud activities, both against employees and the state. The shift to remote work created a commonly reported opportunity for criminals to perpetrate gift card scams that rely on impersonating a trusted individual to convince victims to purchase gift cards. While the frequency of this attack increased substantially overall, Maryland state government experienced few successful attacks.

In addition to these attacks on state employees, significant attempts were made to defraud both the Department of Labor's unemployment insurance program and the programs supporting small businesses within the Department of Commerce. Because transactions that previously occurred in-person moved online, much of the friction that prevented this class of attack was removed. These attacks were, and still are, frequently carried out by sophisticated criminal organizations that use stolen identity information to impersonate individuals seeking benefits.

Maryland was able to prevent and stop many of these attempts through partnerships between the Maryland Security Operations Center, the affected Agency, and local and federal law enforcement cooperative actions. As the success of these attacks decreased, cybercriminals have shifted targets from the government agency to the citizen through phishing attacks impersonating the agency. The Maryland Security Operations Center responded to this new threat against citizens by developing a new capability to identify websites used to perform these crimes and apply legal processes to take them down.

The evolution of cybersecurity risk

Much like previous years, many cyber-adversaries rely on several common tactics to carry out attacks. While nation-state attacks against state governments are uncommon, attacks from cybercriminal gangs and hacktivists continue to occur. These attacks rely on risk introduced by:

1. Older, unpatched vulnerabilities
2. Compromised credentials
3. Zero-day attacks
4. Email delivery of malware or malware links

In addition, with the transition to online learning for the educational systems supported by the Department of Information technology and networkMaryland, Distributed Denial of Service (DDoS) attacks against state infrastructure, including networkMaryland, reduced dramatically in frequency in calendar year 2020. This reduction was short-lived, and both the frequency and amplitude of these attacks has increased in 2021.

To combat these risks, the Office of Security Management (OSM) conducts routine vulnerability scans of state systems and subscribes to several services to identify state systems that are not connected to the state's network. Additionally, the Maryland Security Operations Center (MSOC) aggressively responds to attacks against the state email system, which complements the additional security functionality within the state email system. As part of the proactive work by the threat intelligence team in the Office of Security Management, controls have been implemented to minimize the risk from these attacks, including identifying compromised credentials. This work, however, remains ongoing because the adversaries continue to increase the sophistication of their attacks and to demonstrate agility in their approach.

Cybersecurity Survey Results and Evaluation

Data was gathered through a comprehensive survey that endeavored to understand, at an agency level, the status of several important cybersecurity controls. While this information will be gathered and evaluated as part of the ongoing cybersecurity assessment program, the information obtained will also be used to prioritize outreach for improving the cybersecurity posture of organizations as directed by the State Chief Information Security Officer.

The process of conducting the cybersecurity survey in itself was an informative exercise that underscores the need for continued measurement and tracking. The conversations that occurred during the survey process are important to continue.

Recommendation

- *State Executive Branch Cybersecurity (SEBC) Recommendation 1.* That an Annual Cybersecurity survey of all units of state government is conducted every-other year. The high level findings are compiled into an Annual Cybersecurity report by the Office of Security Management and submitted to the General Assembly.

Survey Data

Surveys were sent by the State Chief Information Security Officer to eighty-nine discrete units of state Government within the purview of the Governor's authority. Of those eighty-nine, seventy responded by the time of this writing, including all twenty-one principal departments. Of the seventy, eight indicated that their results were included as part of another response as a function of shared IT and cybersecurity services. While incomplete, the State Chief Information Security Officer believes that the sample is representative of the data that will eventually be collected from all units and is therefore useful to make assertions regarding the overall status of cybersecurity in the state. While most of the units that did not respond indicated that they outsourced IT to a Managed IT service provider and did not have the information available, it is noteworthy that the State Board of Elections refused to provide results. The Department of Information Technology intends to continue follow-ups and support until all agencies provide responses.

The development of the survey was a collaborative effort between members of the Department of Information Technology, the Maryland Cybersecurity Council, and members of the legislature. The survey included twenty questions that were grouped where appropriate. Responses were generally limited to a subset of specific answers to facilitate easier data processing and higher data utility. Respondents were asked to provide inventory lists if available and provide the date of that inventory.

Because this information would be valuable to a cybercriminal, specific data about systems and agencies are not included in this report. However, in the interest of transparency of government, high-level information about the survey results is included below.

Identify

The first portion of the survey focused on Identification, including asset management, business environment, risk assessment, governance and awareness training. The questions asked are highlighted in the table below.

Survey Questions - Identify

- Does your organization have a complete inventory of its IT Systems?
- Does your organization have a complete inventory of its external IT Systems? (External IT systems include SaaS, PaaS, IaaS, and niche "as-a-Service" offerings)
- Has your organization identified the Recovery Time Objectives and Recovery Point Objectives for its IT Systems?
- Has your unit conducted a cybersecurity risk assessment in the past two years?
- At what frequency are IT assets scanned or tested for vulnerabilities?
- Does your unit have a standard definition of sensitive information?
- Has your unit set standards for how it shares sensitive information with third parties?

An aggregation of the the respondents received indicate that:

- **More than 66% reported having a complete inventory of internal IT systems.**
- **More than 80% reported having a complete or partial inventory of internal IT systems.**

  Having an accurate inventory of IT systems is a requirement for successfully managing cybersecurity risk. At the conclusion of the cybersecurity assessment initiative, all units should have a complete inventory of their IT systems.
- **More than half had not identified Recovery Time Objectives/Recovery Point Objectives for their systems.**

  Understanding the business need for system recovery is crucial for continuing to provide services in the event of a cybersecurity incident or other disaster. Remediation activities that follow the cybersecurity assessments will ensure that units can describe the recovery time objectives and recovery point objectives for key systems.
- **The Maryland IT Security manual describes the standards for scanning IT assets for vulnerabilities. Of the agencies that responded, more than half noted vulnerability scanning within standards. Of those that responded "unknown," half received the service from DoIT but were unaware.**

  The Office of Security Management, through the Department of Information Technology Portfolio Office, plans to conduct outreach to ensure that IT assets receive regular vulnerability scans and that units can use this information to prioritize remediation activities.

Recommendations

- *SEBC Recommendation 2*. That the state hire an independent third party to work with the Chief Data Officer and all state agencies to produce the first baseline report of their IT systems and specified state data.
- *SEBC Recommendation 3.* That each state unit develops specific Recovery Time Objectives/Recovery Point Objectives to ensure system recovery and continuity of services in the event of a cybersecurity incident or other disaster. These objectives should be updated every other year and shared with the Office of Security Management for inclusion in the Annual Cybersecurity report.
- *SEBC Recommendation 4.* That all units of state government complete regular vulnerability scans. The Office of Security Management should conduct outreach to ensure that IT assets receive regular vulnerability scans. The state units should use the information from these scans to prioritize remediation activities. This should be reported in the Annual Cybersecurity Survey.

Protect

The next portion of the survey focused on access control and protection of information, processes and procedures. The questions asked are highlighted in the table below.

Survey Questions - Protect
● Does your unit require multi-factor authentication (two distinct factors) for: administrative access, regular user access, email, remote access, SaaS? ● Does your organization require all vendors with access to state systems or state data to complete periodic security training? ● Has your organization identified the Recovery Time Objectives and Recovery Point Objectives for its IT Systems? ● Does your unit have any legacy systems, defined as software or hardware which no longer (1) receives updates, (2) receives security patches, or (3) has replacement parts and technical support available from the manufacturer? ● Does your organization conduct regular backups? ● Are backups stored either in an immutable format or disconnected from the network ● How often are test restorations of systems performed to validate processes are working properly? ● At what frequency does your unit provide cybersecurity awareness and training to the following groups? Employees? Contractual Employees?

An aggregation of the survey data from respondents indicate that:

- **40% of units have at least one legacy system.**
  As part of the cybersecurity assessment initiative and other proactive outreach, further work will occur to determine if upgrades or modernization efforts are more appropriate for addressing these issues. Efforts related to prioritizing upgrades and modernization is outside the scope of the cybersecurity surveys.
- **More than 60% of the respondents had not conducted a cybersecurity risk assessment.**
  As part of the proactive risk identification and reduction work performed by the Office of Security Management, external vulnerability and risk assessments are performed for all systems connected to networkMaryland (including county governments using the network). The Security Operations Center reports vulnerabilities and high-risk configurations to the agencies for awareness and remediation.
- **Most units lacked explicit standards describing sensitive information and information-sharing agreements.**
  One of the key initiatives for the State Chief Data Officer and State Chief Privacy Officer is to foster the development of standards to describe data, to protect data in all its forms (at rest, in motion, in use), and to ensure that agencies establish information sharing and data use agreements.

- **Nearly 75% reported that they performed backups on a regular basis, with slightly fewer reporting immutable or offline backups. A similar number of testing restoration capabilities of a subset of systems at least annually.**
  This is a strong indicator of a maturing program, but results indicate that more frequent test restorations should occur as part of ongoing improvement initiatives.
- **Multi-factor authentication utilization:**
  - o **63% of respondents report requiring multi-factor authentication for email**
  - o **47% of respondents report requiring multi-factor authentication for Remote Access**

  Multi-factor authentication for remote access and email access is a requirement described in the Maryland Information Technology Security Manual. In addition, it is impactful in protecting systems from unauthorized access. The Department of Information Technology portfolio office plans to contact non-compliant agencies to ensure that their systems are either configured to meet the standards described in policy or that access is transitioned into Department of Information Technology services.
- **Regarding cybersecurity training for employees and contractual employees, only three respondents reported not conducting cybersecurity training as required in the Security Manual**
  The Office of Security Management is conducting proactive outreach to ensure that all units conduct cybersecurity training. The Maryland Cybersecurity Coordinating Council will review this issue and may make recommendations to mandate cybersecurity training as a contractual requirement for vendors with access to state systems or data.

Recommendations

- *SEBC Recommendation 5.* Given the number of legacy systems in state units, the state should prioritize funding for upgrades and modernization efforts. The General Assembly should consider bonding for a major investment in updating the state's technical deficit in a manner like that undertaken by the State of Massachusetts. A new oversight board (like the Board of Public Works process, but specific for IT systems) should be charged with oversight of the investment. Issues of the safety of procurement and economies of scale should be considered.
- *SEBC Recommendation 6.* That the Office of Security Management should ensure that an external vulnerability and risk assessment is completed for each state unit annually. Each unit of government should report vulnerabilities and high-risk configurations to the Office of Security Management and work with the Office on remediation. Each unit should report back to the Office of Security Management on remediation efforts based on the assessments.
- *SEBC Recommendation 7.* That the Chief Data Officer and the Chief Privacy Officer should work with units of state government to develop standards to describe sensitive information and to establish information sharing and data use agreements. Units of government should report on their implementation of these standards in the Annual Cybersecurity Survey.
- *SEBC Recommendation 8*. That as stated in The Security Manual, all state units should conduct regular backup operations and more frequent restoration testing. This activity should be reported to the Office of Security Management in the Annual Cybersecurity Survey.
- *SEBC Recommendation 9.* That state agencies should operate with multi-factor authentication practices for remote access and email access. The Office of Security Management should ensure that state agency systems are either configured to meet the standards described in Maryland

Information Technology Security Manual or access of the system to the Department of Information Technology services.

- *SEBC Recommendation 10*. That all units of state government conduct cybersecurity training that reflects best practices and is available for all regular and contractual employees. The Office of Security Management should work with each state agency to identify appropriate training for all unit employees and contractors. The % of employees completing the training should be reported in the Annual Cybersecurity Survey.

Respond

The next portion of the survey focused on remediation objectives. The question asked is highlighted in the table below.

Survey Questions - Respond
● Does the organization have prioritized remediation objective-times for vulnerabilities

- **Despite being described in the Maryland IT Security Manual, most agencies were unable to describe the remediation objective-time for vulnerabilities of various severities.**
  The Office of Security Management, through the Department of Information Technology Portfolio Office, plans to conduct outreach to ensure that units that manage IT systems understand their obligations and the expectations for managing cybersecurity risk.

Recommendation

- *SEBC Recommendation 11*. That all units of state government are able to describe the remediation objective-time for vulnerabilities of various severities. This description should be updated and reported in the Annual Cybersecurity Survey. The Office of Security Management should conduct outreach to ensure that state units that manage IT systems understand their obligations and the expectations for managing cybersecurity risk.

LOCAL GOVERNMENT CYBERSECURITY[58]

Question 1: Has each local government completed a recent vulnerability assessment, planned to remediate any current vulnerabilities, and prepared to prevent evolving/future cybersecurity risks?

Question 2: How can the state best support local governments, including school systems, health departments, and municipalities, to meet minimum standards for cybersecurity and to leverage federal resources for assessment and improvement?

Question 3: Are local governments allocating sufficient resources to cybersecurity in their information technology budgets, including for cybersecurity awareness education and training for employees?

The proliferation of cybersecurity incidents in recent years has shown that no local jurisdiction, no matter its size, is immune. In 2019, a ransomware attack hit the Baltimore City Government, costing the city an estimated $18 million.[59] In early 2021, a ransomware attack befell the Baltimore County School System, costing the County an estimated $7.7m.[60] Beyond the financial cost, the attack significantly burdened students and families that were already engaged in full-time distance learning.

Even small jurisdictions are not immune to the effects of cyber incidents. The cities of Leonardtown, and North Beach, MD lost access to their networks when a ransomware attack crippled the system of one of their shared IT contractors, Kaseya. These small localities were delayed in sending out water bills and other important correspondences and had to use significant staff and financial resources in rebuilding their networks.[61] This attack exemplifies that securing internal networks does not ensure that state or local jurisdictions will not be impacted by a cyber incident. In actuality, it drives home why planning and response, along with ensuring suppliers practice good cyber hygiene, is critical to the overall operational security of state and local networks.

This study sought information from local subdivisions on two fundamental areas of interest: cyber readiness, and how the state can be most helpful in improving the cybersecurity posture of local jurisdictions.

Readiness

While each survey varied in its exact questions, all were designed to solicit responses to some fundamental questions about local cybersecurity readiness:

- **Risk Assessment**

[58] The following discussion was drafted by Ben Yelin with the support of four CHHS interns: Serena Chenery, Makenzie Donaldson, Michael Rovetto, Alek Stathakis, and Stephanie Vangellow.

[59] https://www.baltimoresun.com/politics/bs-md-ci-ransomware-expenses-20190828-njgznd7dsfaxbbaglnvnbkgjhe-story.html

[60] https://www.baltimoresun.com/education/bs-md-ransomware-cost-schools-20210609-20210611-6fipdck3h5b5peli6vgbgfsqyy-story.html

[61] https://www.washingtonpost.com/technology/2021/07/08/kaseya-ransomware-attack-leonardtown-maryland/

    - Does each unit of local government understand the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals?
    - Has each unit of local government conducted a recent vulnerability assessment?
    - How best does the state determine if the local government, school system, and health departments are prepared to prevent and respond to evolving cybersecurity risks?

- **Risk Management**
    - Does each unit of local government have plans to remediate any vulnerabilities exposed by the assessments?
    - Is each unit of local government prepared to prevent and respond to evolving cybersecurity risks?
    - What is the ratio of the unit of local government expenditures on cybersecurity to total information technology spending for the immediately preceding three (3) calendar years?

- **Awareness and Training**
    - Is each unit of local government personnel and partners provided cybersecurity awareness education and are each adequately trained to perform their information security-related duties and responsibilities consistent with related policies, procedures, and agreements?

State Support

This study sought input from local subdivisions as to how the state can best support local governments, so they are able to maintain and implement effective cybersecurity plans. The study also assessed the need for state cybersecurity support for local entities, including county and municipal governments, local health departments, local school systems, and local offices of emergency management. While each survey varied in its exact questions on this topic, general areas of inquiry were as follows:

    - How great is the need for state cybersecurity support for local entities, including county governments, local health departments, local school systems, and municipalities?
    - How can local government agencies best leverage available federal resources for cybersecurity assessments and improvement grants?
    - How can the state best encourage/support local government units to implement and maintain minimum cybersecurity standards, including using budget structures and grants to ensure compliance?

Data Collection Process

The data collection process was as follows:

- County Governments: To obtain data from County Governments, the ad hoc committee worked with Kevin Kinnally, Legislative Director, Maryland Association of Counties. Senator Hester and other members of the research team also attended a live session at the Maryland Association of Counties Conference in August 2021 to ask follow-up questions on the initial survey.
- Municipal Governments: To help obtain data from the Municipal Governments, the team worked closely with Justin Fiore, Government Relations Manager, Maryland Municipal League (MML).

The team attended the annual MML conference on October 11th to give a presentation and solicit additional responses for the survey questions.

- Local Emergency Managers: Brian Bauer, Preparedness Branch Manager, and Paul Gump, Cyber Preparedness Unit (CPU) Supervisor, at the Maryland Department of Emergency Management (MDEM) helped develop the survey tool for local emergency managers. Besides the survey, the team held a Zoom call with the County IT professionals and local Emergency Managers on September 28, 2021.
- Local School Districts: The ad hoc committee reached out to Mary Pat Fannon, the Executive Director of the Public School Superintendents Association of Maryland. The team worked in coordination with Edward Gardner from the Frederick County Public School system on soliciting input from each County school district CIO. On September 22, 2021, the team hosted a call with IT professionals from most Maryland jurisdictions.

Survey

To achieve the objectives outlined above, surveys were distributed to County IT departments, municipalities, local school systems, and local emergency managers across the state. The surveys specifically focused on governance, risk assessment, risk management strategy, and awareness and training. After the data was synthesized and aggregated, stakeholders convened to discuss the results in a series of meetings.

Summary of Key Findings

Overall, respondents across all sectors of local government expressed eagerness to improve their cyber security posture but are limited by lack of funding for full-time staff, along with inadequate access to appropriate resources. The following is a breakdown of the common themes from the data collected.

Survey Results

1. **County IT Department Survey/Focus Group: Baltimore County, Wicomico County, Somerset County, Garrett County, Prince George's County**

- Some counties are not allocating sufficient resources to cybersecurity. If there were clear standards to evaluate the effectiveness of control systems, or an intendant auditing function, it would be easier to assess whether local governments are allocating sufficient resources to cybersecurity in their information technology budgets.
- For counties to meet the minimum standards for cybersecurity, the state needs to provide additional funding and assist the counties in obtaining resources (tools, software, hardware, and personnel). It would also be helpful for the state to maintain a list of recommendations and resources in one easy location. Additionally, the state should look into a voluntary certification program for entities that meet a defined set of standards.
- Patch management and vulnerability management go hand in hand.
- Vulnerability management cannot be addressed by having vendors come in to perform assessments. Often these assessments indicate the entity is failing.
- Many counties rely on legacy systems provided by the state, so vulnerabilities that are introduced at the state flow down to the counties.

- Each expressed a desire for the state to serve as subject matter experts for Cyber and promulgate best practices, guidance and resources for Counties in need of minimum-security standards.
- Would be helpful to provide grants to local governments to close cybersecurity gaps but avoid unfunded statewide mandates.
- Desire for a "cyber patriots" strike team, which can be deployed to any locality that suffers a ransomware attack.
- State should serve as a partner to local CIOs and CISOs to make use of their institutional expertise, rather than have the state push down outdated information, concepts and assumptions.

2. Appointed Local Emergency Manager Cyber Survey

- 13 responses representing 12 jurisdictions.
- 78.6% of local emergency managers reported that their respective local emergency management organization or the local office of IT conducted a vulnerability assessment of jurisdiction IT infrastructure and network. For those who completed a vulnerability assessment, the most common barriers to closing identified gaps, mitigating known vulnerabilities, and reducing cybersecurity risks were time, staffing, resources, and outdated systems.
- 84.6% of surveyed jurisdictions maintain cyber insurance.
- 53.8% of the surveyed jurisdictions have neither a consequence management plan which covers prevention, response, and recovery nor a cyber disruption event in the form of an Emergency Operations Plan annex, nor a contingency plan.
- More than 90% of surveyed jurisdictions conduct regular technical cybersecurity awareness training for the protection and mitigation of IT systems, networks, and resources:
    - However, about 85% of surveyed jurisdictions do not conduct and/or host training courses on cybersecurity and preparedness that focus on emergency management and homeland security.
    - Most jurisdictions do not conduct exercises for the consequence management of a cyber disruption event.
- Respondents listed lack of time, lack of resources, and departments working in silos as some of the challenges jurisdictions experience in developing an After-Action Report (AAR) for a cyber disruption event.
- Jurisdictions listed funding, training, and resources as some of the top ways the state can support jurisdictions for non-technical cyber preparedness:
    - Survey respondents also want extra training in malware and phishing, real world ransomware prevention, best practices for inter-agency and inter-municipal cooperation and coordination during a cyber security incident that impacts critical agency systems.

3. MD Public School System Survey on Cyber Security Survey

- 19 survey responses:
    - Total students enrolled for the 2021/22 school year ranged from 3,600 to 180,000.
- Only 31% of respondents indicated that their organization allocates sufficient resources to cybersecurity in their budgets, including for monitoring, response, cybersecurity awareness education and training for employees.

- 63% of respondents had completed a recent vulnerability assessment for all internal information systems.
- Almost 90% of respondents reported that their organizational leadership supports the implementation of an industry standard cybersecurity framework and the enforcement of vulnerability remediation activities.
- However, only 31% of respondents reported that their organizations require all external information systems to have a vulnerability assessment completed within the past year.
- Most respondents (58%) reported that their LEA does not have a complete and accurate inventory of all information systems, applications, and technology hardware that has access to their organization's data.
- 21% of respondents reported their LEA has a Disaster Recovery Plan and an Incident Response Plan, which have been tested within the past 12 months.
- More than half of respondents reported that their units require multi-factor authentication for administrator privileged accounts and/or remote access accounts. Only 5 respondents said their unit requires multi-factor authentication of non-privileged user accounts and/or software as a service account.
- The state can best support LEA's work to meet the minimum standards for cyber security by providing funding, guidance, and the resources to hire qualified personnel and additional staff.
- There is a disparity between urban and rural communities. Rural districts have a difficult time recruiting and retaining talented staff.
- The state could help districts by providing the following:
  - Free virtual training.
  - Increased communication:
    - A state help desk, essentially a hotline that districts can call to get guidance on how to handle issues.
    - Incorporate other stakeholders.
    - System for information sharing and best practices.
  - Additional funding, especially for hiring full time employees:
    - Rural communities struggle to get talent.
    - Funding to sustain new "gadgets," devices, and firewalls in the future.
    - IT people.

4. Municipalities Cyber Survey

- Responses from ten municipalities.
- 80% of respondents expressed interest in participating in legislative advocacy on cybersecurity issues before the Maryland General Assembly.
- Almost 90% of respondents reported that their municipal government had not conducted a vulnerability assessment of jurisdiction IT infrastructure and network. Likewise, 87% of respondents reported their jurisdiction had not requested or completed a cyber assessment through either Maryland National Guard's Innovative Readiness Training (IRT) Program or the Department of Homeland Security (DHS)—Cybersecurity and Infrastructure Security Agency (CISA).
- About 55% of respondents indicated their jurisdictions maintain cyber insurance.
- 80% of respondents reported that their jurisdiction does not currently have a consequence management plan, covering prevention, response, and recovery for a cyber disruption event in the form of an Emergency Operations Plan (EOP), annex, or contingency plan.

- Only 44% of respondents report that their jurisdiction includes, as an annex or within the Continuity of Operations plans, an information technology recovery component that catalogs and details the recovery of information technology systems, platforms, hardware and software.
- None of the respondents reported that their jurisdictions conduct regular technical cybersecurity awareness training for the protection and mitigation of IT systems, networks, and resources. They also do not conduct and/or host training courses on cyber security preparedness focusing on emergency management and homeland security, or conduct exercises for the consequences management (prevention, response, and recovery) of a cyber disruption event.
- 85% of respondents were unsure if their jurisdiction has a multi-disciplinary stakeholder working group for coordination of cybersecurity and preparedness.
- In terms of non-technical cyber preparedness, technical cybersecurity, and/or consequence management, respondents reported that they would like the state to provide:
    - General training and best practices:
        - Resources and training specifically for small towns on tight budgets.
        - Certification.
        - Compliance ratings.
        - Conduct assessments of current systems and preparedness plans to help guide policy.
- In terms of technical cybersecurity, non-technical cyber preparedness, or cyber in emergency management, respondents would like additional training courses for:
    - Cybersecurity awareness basics:
        - Preparedness training.
        - Record management.
        - Training to spot fraud and bogus emails.
    - Resource sharing.
    - Legacy system upgrades.
    - Training to reduce human error.

Recommendations

- *Local Government Cybersecurity (LGC) Recommendation 1.* The state should adopt the plan for a coordinated cybersecurity operations effort, split between the Department of Information Technology (DoIT), and the Maryland Department of Emergency Management (MDEM). This plan emerged during negotiations over SB69, during the 2021 Legislative Session, and was agreed to by Secretary Leahy (DoIT) and Acting Secretary Strickland (MDEM). The division of duties should be as follows, as it relates to **local** units of government:

Effort	**State**	**Local**
Preparedness (Measures taken to plan for an incident - ensuring you have protocols and are ready for an incident should it happen)	MDEM - ● State interagency consequence management preparedness ● State-federal intergovernmental	MDEM - ● Response planning (includes comms). DoIT - ● Technical evaluation of response and recovery plans

	coordination of EM planning, training, and exercise DoIT - ● Response planning (includes comms) ● Recovery planning ● Technical evaluations of plans ● Subject Matter Expert	● Subject Matter Expert
Prevention (Measures taken to prevent an incident)	MDEM - (No Role) DoIT - ● Coalescer of prevention plans ● Technical evaluation of prevention plans ● Subject Matter Expert	MDEM - ● Coalescer of prevention plans DoIT - ● Technical evaluation of prevention plans ● Subject Matter Expert
Response (Actions taken during a detected cybersecurity incident to contain the impact and ameliorate any effects created by the incident.)	MDEM - ● Communications and coordination (already in state law) DoIT - ● Cybersecurity incidents are reported to MDSOC ● Analysis (making sure recovery activities happen as they're supposed to) ● Mitigation of technical incident ● Improvement phase of response (after-action review, retrospective incident response analysis) ● Technical guidance and advice	MDEM - ● Communications and coordination (already in state law) ● Cybersecurity incidents are reported to MJOC ● Improvement phase of response (after-action review, retrospective incident response analysis) DoIT - ● Analysis (making sure recovery activities happen as they're supposed to) ● Mitigation of technical incident ● Technical guidance and advice
Recovery (Activities to update plans for future preparedness, restore any capabilities or services that were impaired due to a cybersecurity incident, and	MDEM - ● Intra-agency and state-federal intergovernmental coordination of	MDEM - ● Improvement phase of response (after-action review, retrospective incident response

achieve a timely return to normal operations.)	recovery funding through emergency management pathways DoIT - ● Improvement phase of response (after-action review, retrospective incident response analysis) ● Communications ● Technical guidance and advice	analysis) ● Communications DoIT - ● Technical guidance and advice

- *LGC Recommendation 2.* In order to support the duties of the Maryland Department of Emergency Management (as described above), the state should fully fund and provide adequate resources to the **Cyber Preparedness Unit,** within the Preparedness Branch of the Consequence Management Directorate of MDEM. The responsibilities of that unit should include:
  a) Support each subdivision in developing a vulnerability assessment and a cyber assessment through either Maryland National Guard's Innovative Readiness Training (IRT) Program or the Department of Homeland Security (DHS)—Cybersecurity and Infrastructure Security Agency (CISA). Provide subdivisions with the resources and best practices to complete this assessment annually.
  b) Develop an online clearinghouse with cybersecurity training resources for personnel. This should include technical training resources, cybersecurity Continuity of Operations (COOP) templates, consequence management plans, training in malware and ransomware detection. The clearinghouse should be updated regularly.
  c) Staff a statewide helpline to provide real-time emergency assistance to a jurisdiction that has experienced a cyber incident or attack and needs resources.
  d) Work with the Department of Information Technology (DoIT) on replacing legacy systems that increase cybersecurity risks.
- *LGC Recommendation 3.* Establish a **Local Cybersecurity Support Fund**, to provide financial assistance to local units of government to improve their cybersecurity posture. The fund could either be a revolving fund (like the Revolving Resiliency Loan Fund, created during the 2021 legislative session) or a grant fund. The fund could be used for the following:
  a) Hardening current devices and networks with the most up-to-date cybersecurity protections.
  b) Supporting the purchase of new hardware, software, devices, and firewalls to improve cybersecurity posture.
  c) Recruiting and hiring additional IT staff that focus exclusively on cybersecurity.
  d) Paying outside vendors for cybersecurity staff training.
  e) Rebuilding systems or networks in the event of a cyber incident or cyber attack.
- *LGC Recommendation 4.* That the state should use available funds to ensure local units of government have access to cybersecurity insurance.

APPENDIX A: REQUEST OF CO-CHAIRS, JOINT COMMITTEE ON CYBERSECURITY, INFORMATION TECHNOLOGY AND BIOTECHNOLOGY

Katie Fry Hester
Legislative District 9
Carroll and Howard Counties

Education, Health, and
Environmental Affairs Committee

Chair, Joint Committee on
Cybersecurity, Information Technology
and Biotechnology

THE SENATE OF MARYLAND
Annapolis, Maryland 21401

Annapolis Office
James Senate Office Building
11 Bladen Street, Room 304
Annapolis, Maryland 21401
410-841-3671 · 301-858-3671
800-492-7122 *Ext.* 3671
KatieFry.Hester@senate.state.md.us

May 27th, 2021

The Honorable Brian Frosh
Chair, Maryland Cybersecurity Council
Office of the Attorney General
State of Maryland
200 St. Paul Place, 20th Floor
Baltimore, Maryland 21202

Dear Attorney General Frosh:

Thank you for your ongoing leadership on the issue of Cybersecurity in the state of Maryland. With cybersecurity threats increasing and expanding, the need has never been greater to protect our state agencies and critical infrastructure, as well as our local government, school systems, health departments, and other units of local government.

In 2019, Atlanta, Georgia; New Bedford, Massachusetts; New Orleans, Louisiana; Greenville, North Carolina; Pensacola, Florida; Wilmer, Texas; St. Lucie Florida; and our very own Baltimore City were victims of cybersecurity attacks, with costs in recovery and lost revenue stretching into the millions. In 2020 we experienced a slew of cybersecurity attacks aimed at local governments and school systems, not the least of which is our very own Baltimore County Public Schools. With bad actors becoming more sophisticated, and the prevalence of cyber threats rising at almost every level of government and industry, the risk of a cyberattack is no longer "if," it's "when."

Recognizing the growing problem, numerous pieces of legislation have been introduced in the past few years. Most notably, SB 69 (which included SB 348) did not pass the house in 2021. A study (see Appendix B) was proposed by the House Health and Government Operations Committee, but was not passed by the full chamber in time to become law. As cybersecurity is a complicated, new topic for many stakeholders and lawmakers, key questions must be answered to ensure concrete action in the 2022 session. In this context I am requesting that the Maryland Cybersecurity Council embark on a short, special study aimed at (1) policy actions that can be taken to increase the cybersecurity of the state of Maryland, and (2) methods of securing the required state and federal resources to achieve greater cybersecurity preparedness for the people of Maryland. Appendix A includes a proposed work plan, which sketches out:

- **Scope:** State governance, state agency, local government units and critical infrastructure
- **Resources:** MCC, UMD CHHS, DOIT, MEMA, MACO
- **Deliverables:** Final Report, Review of State Strategy and Security Manual, Promotion of opportunities for security assessments and federal grants
- **Timeline:** June 9 – December 13, 2021

As the Chair of the Maryland Cybersecurity Council, we anticipate your role would be one of leadership and communication. Specifically:

- Elevating this effort by forming a temporary subcommittee of the council to address these governance issues
- Endorsing the subcommittee's work and the outcomes of the report
- Engaging with other key leaders in the area, including but not limited to the Governor, President of the Senate, Speaker of the House, Standing Committee Chairs
- Supporting efforts by the Subcommittee to secure state and federal grants for increasing cybersecurity related state, local and critical infrastructure.

As Co-Chairs of the Legislative Joint Committee on Cyber Security, Information and Biotechnology, we stand ready to assist this effort as the next step in the critical path towards ensuring the state is as prepared as possible for the evolving digital risks and cybersecurity threats the State of Maryland continues to face.

Very respectfully,

Katie Fry Hester   Pat Young

Senator Katie Fry Hester District 9, Carroll and Howard Counties	Delegate Pat Young District 44B, Baltimore County

Cc:
Governor Larry Hogan
Senate President Bill Ferguson
House Speaker Adriane Jones
Secretary Michael Leahy
Director Russel Strickland
Senator Paul Pinsky, Chair Senate Education, Health & Environmental Affairs Committee
Delegate Shane Pendergrass, Chair House & Government Operations Committee

APPENDIX B: SUMMARY OF RECOMMENDATIONS

GOVERNANCE

- *Governance Recommendation 1.* That the General Assembly codify the key elements of the EO (Maryland Cyber Defense Initiative), viz. the SCISO's position, the SCISO's the Office of Security Management, the authorities outlined in the EO consistent with two recent Executive Orders (Maryland Data Privacy and State Chief Data Officer), and the Maryland Cybersecurity Coordinating Council.
- *Governance Recommendation 2*. That the SCISO continues to be appointed by the Governor.
- *Governance Recommendation 3.* That the IT functions of all agencies in the Executive Branch be centralized in DoIT and brought into the "enterprise". All IT budgets would become part of DoIT's budget and agency staff would report to the CIO.
- *Governance Recommendation 4*. That the cybersecurity functions of the Executive Branch be centralized and made part of the "enterprise". All cybersecurity budgets would become part of one cybersecurity budget and agency cybersecurity staff would report to the SCISO.
- *Governance Recommendation 5*. That DoIT makes the implementation of its Governance Risk and Compliance module a priority.
- *Governance Recommendation 6.* That the General Assembly mandate basic security requirements as part of the procurement process for contractors who will have access to state databases. One example of such requirements is DFARS 52.204-21 (Basic Safeguarding of Covered Contractor Information Systems).
- *Governance Recommendation 7.* That DoIT implements a security regime for all agency procurements below $50,000 of systems or devices that connect to networks, whether through whitelists or other review procedures. Anything connected to or running on the network should have some verified level of trust.
- *Governance Recommendation 8.* That the General Assembly, the State Judicial Branch, and the University System of Maryland be required to annually certify compliance with DoIT minimum security standards.
- *Governance Recommendation 9*. That the risk assessments required by the State Security Manual be performed, aggregated, and prioritized by agencies and used by the Maryland Cybersecurity Coordinating Council (MCCC) to prioritize risk across the Executive Branch and to connect that with the budgeting process, i.e., make corresponding recommendations for security investments that will have the greatest impact in buying down risk.
- *Governance Recommendation 10.* That the meetings of the MCCC be exempt from the Open Meetings Act so that it can be an ongoing forum for the sharing of information, discussing sensitive cybersecurity issues, and shaping recommendations to the SCISO. This is consistent with the fact that the MCCC does not make or recommend public policy and that there are other ways of ensuring accountability for the cybersecurity effort of the state—both as to process and outcomes—that are discussed below.
- *Governance Recommendation 11.* That the MCCC be expanded to include representatives of the General Assembly, the University System of Maryland, and the state judiciary as non-voting members and that the chair have the prerogative to appoint or invite other participants.
- *Governance Recommendation 12.* The Maryland Joint Operations Center (MJOC) is the state's 24/7 emergency operations center capable of quickly and effectively managing initial emergency response coordination in support of state and local governments. The MJOC has the responsibility to receive, analyze, and disseminate information to appropriate Maryland Department of Emergency

Management (MDEM) and interagency personnel with areas of responsibility for hazards in Maryland. Local governments should report cyber attacks or network disruptions to the MJOC, including those attacks on state systems being used by local governments (e.g. METERS[62]). MJOC will notify the appropriate agencies including DoIT through the MDSOC.

- *Governance Recommendation 13.* That the state consider partnering with other states such as North Dakota to leverage even greater buying power for IT and cyber security services both for the state government itself but also for its political subdivisions.
- *Governance Recommendation 14.* That MDEM incorporate information sessions about the MS ISAC and CISA's .gov initiative in its periodic training summits with local jurisdictions to ensure awareness of the services available and that the Cyber Preparedness Unit serve as a bridge to assist local entities where needed to access these services.
- *Governance Recommendation 15*. That the state directly provide or coordinate the procurement of managed cybersecurity services under state vehicles and subsidized by the state to address the preparedness and response capabilities of local jurisdictions
- *Governance Recommendation 16*. That there be some consultative process of the SCISO with representatives of political subdivisions on their cybersecurity needs that leverages organic associations and forums that already exist, such as the Maryland Association of Counties, the Maryland Municipal League, the Maryland Association of County Health Officials, and the Public School Superintendents Association of Maryland.
- *Governance Recommendation 17.* That the cybersecurity budget for the state enterprise should be appropriated and not based on the charge-back model.
- *Governance Recommendation 18*. That there be a fully developed, separate cybersecurity strategic plan to undergird the cybersecurity budget requests.
- *Governance Recommendation 19.* That the Governor's annual budget overview should include statistics on the IT budget and the cybersecurity budget across the state enterprise and include a comparison of cybersecurity budget to the IT budget ala annual OMB overview of the President's budget submission to Congress.
- *Governance Recommendation 20.* That both the Maryland IT Master Plan and any cybersecurity strategic plan attach timelines and appropriate metrics to the plan's goals and objectives and that the cybersecurity strategic plan provides information about the maturity level of the state's cybersecurity and how goals and objectives will advance that maturity.

[62] METERS is a state-run portal used for public safety agencies.

STATE EXECUTIVE BRANCH CYBERSECURITY

- *State Executive Branch Cybersecurity (SEBC) Recommendation 1.* That an Annual Cybersecurity survey of all units of state government is conducted every-other year. The high level findings are compiled into an Annual Cybersecurity report by the Office of Security Management and submitted to the General Assembly.
- *SEBC Recommendation 2.* That the state hire an independent third party to work with the Chief Data Officer and all state agencies to produce the first baseline report of their IT systems and specified state data.
- *SEBC Recommendation 3.* That each state unit develops specific Recovery Time Objectives/Recovery Point Objectives to ensure system recovery and continuity of services in the event of a cybersecurity incident or other disaster. These objectives should be updated every other year and shared with the Office of Security Management for inclusion in the Annual Cybersecurity report.
- *SEBC Recommendation 4.* That all units of state government complete regular vulnerability scans. The Office of Security Management should conduct outreach to ensure that IT assets receive regular vulnerability scans. The state units should use the information from these scans to prioritize remediation activities. This should be reported in the Annual Cybersecurity Survey.
- *SEBC Recommendation 5.* Given the number of legacy systems in state units, the state should prioritize funding for upgrades and modernization efforts. The General Assembly should consider bonding for a major investment in updating the state's technical deficit in a manner like that undertaken by the State of Massachusetts. A new oversight board (like the BPW process, but specific for IT systems) should be charged with oversight of the investment. Issues of the safety of procurement (such as recommendation 7) and economies of scale (recommendation 8) should be considered.
- *SEBC Recommendation 6.* That the Office of Security Management should ensure that an external vulnerability and risk assessment is completed for each state unit once every other year. Each unit of government should report vulnerabilities and high-risk configurations to the Office of Security Management and work with the Office on remediation. Each unit should report back to the Office of Security Management on remediation efforts based on the assessments.
- *SEBC Recommendation 7.* That the Chief Data Officer and the Chief Privacy Officer should work with units of state government to develop standards to describe sensitive information and to establish information sharing and data use agreements. Units of government should report on their implementation of these standards in the Annual Cybersecurity Survey.
- *SEBC Recommendation 8*. That as stated in The Security Manual, all state units should conduct regular backup operations and more frequent restoration testing. This activity should be reported to the Office of Security Management in the Annual Cybersecurity Survey.
- *SEBC Recommendation 9*. That state agencies should operate with multi-factor authentication practices for remote access and email access. The Office of Security Management should ensure that state agency systems are either configured to meet the standards described in Maryland Information Technology Security Manual or access of the system to the Department of Information Technology services.
- *SEBC Recommendation 10*. That all units of state government conduct cybersecurity training that reflects best practices and is available for all regular and contractual employees. The Office of Security Management should work with each state agency to identify appropriate training for all unit

employees and contractors. The percent of employees completing the training should be reported in the Annual Cybersecurity Survey.

- *SEBC Recommendation 11.* That all units of state government are able to describe the remediation objective-time for vulnerabilities of various severities. This description should be updated and reported in the Annual Cybersecurity Survey. The Office of Security Management should conduct outreach to ensure that State units that manage IT systems understand their obligations and the expectations for managing cybersecurity risk.

LOCAL GOVERNMENT CYBERSECURITY

Local Government Cybersecurity (LGC) Recommendation 1. The state should adopt the plan for a coordinated cybersecurity operations effort, split between the Department of Information Technology (DoIT), and the Maryland Department of Emergency Management (MDEM). This plan emerged during negotiations over SB69, during the 2021 Legislative Session, and was agreed to by Secretary Leahy (DoIT) and Acting Secretary Strickland (MDEM). The division of duties should be as follows, as it relates to **local** units of government:

Effort	**State**	**Local**
Preparedness (Measures taken to plan for an incident - ensuring you have protocols and are ready for an incident should it happen)	MDEM - ● State interagency consequence management preparedness ● State-federal intergovernmental coordination of EM planning, training, and exercise DoIT - ● Response planning (includes comms) ● Recovery planning ● Technical evaluations of plans ● Subject Matter Expert	MDEM - ● Response planning (includes comms). DoIT - ● Technical evaluation of response and recovery plans ● Subject Matter Expert
Prevention (Measures taken to prevent an incident)	MDEM - (No Role) DoIT - ● Coalescer of prevention plans ● Technical evaluation of prevention plans ● Subject Matter Expert	MDEM - ● Coalescer of prevention plans DoIT - ● Technical evaluation of prevention plans ● Subject Matter Expert
Response (Actions taken during a detected cybersecurity incident to contain the impact and ameliorate any effects created by the incident.)	MDEM - ● Communications and coordination (already in state law) DoIT - ● Cybersecurity incidents are reported to MDSOC ● Analysis (making sure recovery activities	MDEM - ● Communications and coordination (already in state law) ● Cybersecurity incidents are reported to MJOC ● Improvement phase of response (after-action review, retrospective

	happen as they’re supposed to) ● Mitigation of technical incident ● Improvement phase of response (after-action review, retrospective incident response analysis) ● Technical guidance and advice	incident response analysis) DoIT - ● Analysis (making sure recovery activities happen as they’re supposed to) ● Mitigation of technical incident ● Technical guidance and advice
Recovery (Activities to update plans for future preparedness, restore any capabilities or services that were impaired due to a cybersecurity incident, and achieve a timely return to normal operations.)	MDEM - ● Intra-agency and state-federal intergovernmental coordination of recovery funding through emergency management pathways DoIT - ● Improvement phase of response (after-action review, retrospective incident response analysis) ● Communications ● Technical guidance and advice	MDEM - ● Improvement phase of response (after-action review, retrospective incident response analysis) ● Communications DoIT - ● Technical guidance and advice

- *LGC Recommendation 2.* In order to support the duties of the Maryland Department of Emergency Management (as described above), the state should fully fund and provide adequate resources to the **Cyber Preparedness Unit,** within the Preparedness Branch of the Consequence Management Directorate of MDEM. The responsibilities of that unit should include:
    a. Support each subdivision in developing a vulnerability assessment, and a cyber assessment through either Maryland National Guard’s Innovative Readiness Training (IRT) Program or the Department of Homeland Security (DHS)—Cybersecurity and Infrastructure Security Agency (CISA). Provide subdivisions with the resources and best practices to complete this assessment annually.
    b. Develop an online clearinghouse with cybersecurity training resources for personnel. This should include technical training resources, cybersecurity Continuity of Operations (COOP) templates, consequence management plans, training in malware and ransomware detection. The clearinghouse should be updated regularly.

    c. Staff a statewide helpline to provide real-time emergency assistance to a jurisdiction that has experienced a cyber incident or attack and needs resources.
    d. Work with the Department of Information Technology (DoIT) on replacing legacy systems that increase cybersecurity risks.

- *LGC Recommendation 3.* Establish a **Local Cybersecurity Support Fund**, to provide financial assistance to local units of government to improve their cybersecurity posture. The fund could either be a revolving fund (like the Revolving Resiliency Loan Fund, created during the 2021 legislative session) or a grant fund. The fund could be used for the following:
    a. Hardening current devices and networks with the most up-to-date cybersecurity protections.
    b. Supporting the purchase of new hardware, software, devices and firewalls to improve cybersecurity posture.
    c. Recruiting and hiring additional Information Technology staff that focus exclusively on cybersecurity.
    d. Paying outside vendors for cybersecurity staff training.
    e. Rebuilding systems or networks in the event of a cyber incident or cyber attack

- *LGC Recommendation 4:* That the state should use available funds to ensure local units of government have access to cybersecurity insurance.