SENATE BILL 69

E4 1lr0794
SB 1036/20 – EHE (PRE–FILED) CF HB 879

By: **Senators Hester and Simonaire**
Requested: September 30, 2020
Introduced and read first time: January 13, 2021
Assigned to: Education, Health, and Environmental Affairs

Committee Report: Favorable with amendments
Senate action: Adopted
Read second time: February 27, 2021

CHAPTER _____

AN ACT concerning

~~Maryland Emergency Management Agency –~~ Cybersecurity Coordination and Operations ~~Office~~ – Establishment and Reporting

FOR the purpose of establishing the ~~Cybersecurity Coordination and Operations Office within the Maryland Emergency Management Agency (MEMA); providing for the purpose of the Office; requiring the Director of MEMA to appoint an Executive Director as head of the Office; requiring the Office to be provided with sufficient staff to perform the Office's functions; requiring the Office to establish regional assistance groups to deliver or coordinate support services to political subdivisions, agencies, or regions in accordance with certain requirements; authorizing the Office to hire or procure regional coordinators; requiring a certain report annually~~ Office of Security Management within the Department of Information Technology, certain Office positions, and the Maryland Cybersecurity Coordinating Council; establishing certain responsibilities and authority of the Office; requiring each unit of the Legislative or Judicial Branch of State government that uses a certain network to certify certain compliance to the Department on or before a certain date each year; requiring each unit of the Executive Branch of State government and certain local entities to submit a certain report to the Office on or before a certain date each year; requiring each unit of the Executive Branch of State government and certain local entities to report certain cybersecurity incidents in a certain manner and under certain circumstances; requiring the Office to submit a certain report to the Governor and certain committees of the General Assembly on or before a certain date each year; defining certain terms; ~~and generally relating to the establishment of the~~

EXPLANATION: **CAPITALS INDICATE MATTER ADDED TO EXISTING LAW.**
[Brackets**]** indicate matter deleted from existing law.
Underlining indicates amendments to bill.
~~Strike out~~ indicates matter stricken from the bill by amendment or deleted from the law by amendment.

~~Cybersecurity Coordination and Operations Office within MEMA~~ making conforming changes; and generally relating to information technology.

~~BY adding to~~
~~Article – Public Safety~~
~~Section 14–104.1~~
~~Annotated Code of Maryland~~
~~(2018 Replacement Volume and 2020 Supplement)~~

BY renumbering
Article – State Finance and Procurement
Section 3A–101 through 3A–702, respectively, and the title "Title 3A. Department of Information Technology"
to be Section 3.5–101 through 3.5–702, respectively, and the title "Title 3.5. Department of Information Technology"
Annotated Code of Maryland
(2015 Replacement Volume and 2020 Supplement)

BY repealing and reenacting, with amendments,
Article – Criminal Procedure
Section 10–221(b)
Annotated Code of Maryland
(2018 Replacement Volume and 2020 Supplement)

BY repealing and reenacting, with amendments,
Article – Health – General
Section 21–2C–03(h)(2)(i)
Annotated Code of Maryland
(2019 Replacement Volume and 2020 Supplement)

BY repealing and reenacting, with amendments,
Article – Human Services
Section 7–806(a), (b)(1), (c)(1), (d)(1) and (2)(i), and (g)(1)
Annotated Code of Maryland
(2019 Replacement Volume and 2020 Supplement)

BY repealing and reenacting, with amendments,
Article – Insurance
Section 31–103(a)(2)(i) and (b)(2)
Annotated Code of Maryland
(2017 Replacement Volume and 2020 Supplement)

BY repealing and reenacting, with amendments,
Article – Natural Resources
Section 1–403(c)
Annotated Code of Maryland
(2018 Replacement Volume and 2020 Supplement)

BY repealing and reenacting, without amendments,
Article – State Finance and Procurement
Section 3.5–101(a) and (e) and 3.5–301(a)
Annotated Code of Maryland
(2015 Replacement Volume and 2020 Supplement)
(As enacted by Section 1 of this Act)

BY adding to
Article – State Finance and Procurement
Section 3.5–2A–01 through 3.5–2A–05 to be under the new subtitle "Subtitle 2A. Office of Security Management"; and 3.5–405
Annotated Code of Maryland
(2015 Replacement Volume and 2020 Supplement)

BY repealing and reenacting, with amendments,
Article – State Finance and Procurement
Section 3.5–301(h), 3.5–302(c), 3.5–303(b)(2)(ii)2., 3.5–307(a)(2), 3.5–309(c)(2), (i)(3), and (l), 3.5–311(a)(2)(i), and 3.5–404
Annotated Code of Maryland
(2015 Replacement Volume and 2020 Supplement)
(As enacted by Section 1 of this Act)

BY repealing and reenacting, with amendments,
Article – State Finance and Procurement
Section 12–107(b)(2)(i)10. and 11.
Annotated Code of Maryland
(2015 Replacement Volume and 2020 Supplement)

SECTION 1. BE IT ENACTED BY THE GENERAL ASSEMBLY OF MARYLAND, That Section(s) 3A–101 through 3A–702, respectively, and the title "Title 3A. Department of Information Technology" of Article – State Finance and Procurement of the Annotated Code of Maryland be renumbered to be Section(s) 3.5–101 through 3.5–702, respectively, and the title "Title 3.5. Department of Information Technology".

SECTION ~~1.~~ 2. AND BE IT FURTHER ENACTED ~~BY THE GENERAL ASSEMBLY OF MARYLAND~~, That the Laws of Maryland read as follows:

~~**Article – Public Safety**~~

~~**14–104.1.**~~

~~**(A) (1) IN THIS SECTION THE FOLLOWING WORDS HAVE THE MEANINGS INDICATED.**~~

~~**(2) "OFFICE" MEANS THE CYBERSECURITY COORDINATION AND OPERATIONS OFFICE ESTABLISHED WITHIN MEMA.**~~

~~(3) "REGION" MEANS A COLLECTION OF POLITICAL SUBDIVISIONS.~~

~~(B) THERE IS A CYBERSECURITY COORDINATION AND OPERATIONS OFFICE WITHIN MEMA.~~

~~(C) THE PURPOSE OF THE OFFICE IS TO:~~

~~(1) IMPROVE LOCAL, REGIONAL, AND STATEWIDE CYBERSECURITY READINESS AND RESPONSE;~~

~~(2) ASSIST POLITICAL SUBDIVISIONS, SCHOOL BOARDS, AND AGENCIES IN THE DEVELOPMENT OF CYBERSECURITY DISRUPTION PLANS;~~

~~(3) IN CONSULTATION WITH THE DEPARTMENT OF INFORMATION TECHNOLOGY, COORDINATE WITH POLITICAL SUBDIVISIONS, LOCAL AGENCIES, AND STATE AGENCIES ON THE IMPLEMENTATION OF CYBERSECURITY BEST PRACTICES;~~

~~(4) COORDINATE WITH POLITICAL SUBDIVISIONS AND AGENCIES ON THE IMPLEMENTATION OF THE DEPARTMENT OF INFORMATION TECHNOLOGY'S STATEWIDE MASTER PLAN DEVELOPED IN ACCORDANCE WITH TITLE 3A, SUBTITLE 3 OF THE STATE FINANCE AND PROCUREMENT ARTICLE; AND~~

~~(5) CONSULT WITH THE STATE CHIEF INFORMATION SECURITY OFFICER AND THE SECRETARY OF INFORMATION TECHNOLOGY TO CONNECT POLITICAL SUBDIVISIONS AND AGENCIES TO THE APPROPRIATE RESOURCES FOR ANY OTHER PURPOSE RELATED TO CYBERSECURITY READINESS AND RESPONSE.~~

~~(D) (1) THE HEAD OF THE OFFICE IS THE EXECUTIVE DIRECTOR, WHO SHALL BE APPOINTED BY THE DIRECTOR.~~

~~(2) THE OFFICE SHALL BE PROVIDED WITH SUFFICIENT STAFF TO PERFORM THE FUNCTIONS OF THE OFFICE.~~

~~(E) (1) THE OFFICE SHALL ESTABLISH REGIONAL ASSISTANCE GROUPS TO DELIVER OR COORDINATE SUPPORT SERVICES TO POLITICAL SUBDIVISIONS, AGENCIES, OR REGIONS.~~

~~(2) THE OFFICE MAY HIRE OR PROCURE REGIONAL COORDINATORS TO DELIVER OR COORDINATE THE SERVICES UNDER PARAGRAPH (1) OF THIS SUBSECTION.~~

~~(3) THE OFFICE SHALL PROVIDE OR COORDINATE SUPPORT SERVICES UNDER PARAGRAPH (1) OF THIS SUBSECTION THAT INCLUDE:~~

~~(I) CONNECTING MULTIPLE POLITICAL SUBDIVISIONS AND AGENCIES WITH EACH OTHER TO SHARE BEST PRACTICES OR OTHER INFORMATION TO INCREASE READINESS OR RESPONSE EFFECTIVENESS;~~

~~(II) PROVIDING TECHNICAL SERVICES FOR THE IMPLEMENTATION OF CYBERSECURITY BEST PRACTICES IN ACCORDANCE WITH SUBSECTION (C)(3) OF THIS SECTION;~~

~~(III) COMPLETING CYBERSECURITY RISK ASSESSMENTS;~~

~~(IV) DEVELOPING CYBERSCORECARDS AND REPORTS ON REGIONAL READINESS;~~

~~(V) CREATING AND UPDATING CYBERSECURITY DISRUPTION PLANS IN ACCORDANCE WITH SUBSECTION (C)(2) OF THIS SECTION; AND~~

~~(VI) CONDUCTING REGIONAL EXERCISES IN COORDINATION WITH THE NATIONAL GUARD, MEMA, THE DEPARTMENT OF INFORMATION TECHNOLOGY, LOCAL EMERGENCY MANAGERS, AND OTHER STATE AND LOCAL ENTITIES.~~

~~(F) ON OR BEFORE DECEMBER 1 EACH YEAR, THE OFFICE SHALL REPORT TO THE GOVERNOR AND, IN ACCORDANCE WITH § 2–1257 OF THE STATE GOVERNMENT ARTICLE, THE GENERAL ASSEMBLY ON THE ACTIVITIES OF THE OFFICE.~~

Article – Criminal Procedure

10–221.

(b) Subject to Title **[**3A**]** **3.5**, Subtitle 3 of the State Finance and Procurement Article, the regulations adopted by the Secretary under subsection (a)(1) of this section and the rules adopted by the Court of Appeals under subsection (a)(2) of this section shall:

(1) regulate the collection, reporting, and dissemination of criminal history record information by a court and criminal justice units;

(2) ensure the security of the criminal justice information system and criminal history record information reported to and collected from it;

(3) regulate the dissemination of criminal history record information in accordance with Subtitle 1 of this title and this subtitle;

(4) regulate the procedures for inspecting and challenging criminal history record information;

(5) regulate the auditing of criminal justice units to ensure that criminal history record information is:

(i) accurate and complete; and

(ii) collected, reported, and disseminated in accordance with Subtitle 1 of this title and this subtitle;

(6) regulate the development and content of agreements between the Central Repository and criminal justice units and noncriminal justice units; and

(7) regulate the development of a fee schedule and provide for the collection of the fees for obtaining criminal history record information for other than criminal justice purposes.

Article – Health – General

21–2C–03.

(h) (2) The Board is subject to the following provisions of the State Finance and Procurement Article:

(i) Title **[**3A**] 3.5**, Subtitle 3 (Information Processing), to the extent that the Secretary of Information Technology determines that an information technology project of the Board is a major information technology development project;

Article – Human Services

7–806.

(a) (1) Subject to paragraph (2) of this subsection, the programs under § 7–804(a) of this subtitle, § 7–902(a) of this title, and **[**§ 3A–702**] § 3.5–702** of the State Finance and Procurement Article shall be funded as provided in the State budget.

(2) For fiscal year 2019 and each fiscal year thereafter, the program under **[**§ 3A–702**] § 3.5–702** of the State Finance and Procurement Article shall be funded at an amount that:

(i) is equal to the cost that the Department of Aging is expected to incur for the upcoming fiscal year to provide the service and administer the program; and

(ii) does not exceed 5 cents per month for each account out of the surcharge amount authorized under subsection (c) of this section.

(b) (1) There is a Universal Service Trust Fund created for the purpose of paying the costs of maintaining and operating the programs under:

(i) § 7–804(a) of this subtitle, subject to the limitations and controls provided in this subtitle;

(ii) § 7–902(a) of this title, subject to the limitations and controls provided in Subtitle 9 of this title; and

(iii) **[**§ 3A–702**] § 3.5–702** of the State Finance and Procurement Article, subject to the limitations and controls provided in Title **[**3A**] 3.5**, Subtitle 7 of the State Finance and Procurement Article.

(c) (1) The costs of the programs under § 7–804(a) of this subtitle, § 7–902(a) of this title, and **[**§ 3A–702**] § 3.5–702** of the State Finance and Procurement Article shall be funded by revenues generated by:

(i) a surcharge to be paid by the subscribers to a communications service; and

(ii) other funds as provided in the State budget.

(d) (1) The Secretary shall annually certify to the Public Service Commission the costs of the programs under § 7–804(a) of this subtitle, § 7–902(a) of this title, and **[**§ 3A–702**] § 3.5–702** of the State Finance and Procurement Article to be paid by the Universal Service Trust Fund for the following fiscal year.

(2) (i) The Public Service Commission shall determine the surcharge for the following fiscal year necessary to fund the programs under § 7–804(a) of this subtitle, § 7–902(a) of this title, and **[**§ 3A–702**] § 3.5–702** of the State Finance and Procurement Article.

(g) (1) The Legislative Auditor may conduct postaudits of a fiscal and compliance nature of the Universal Service Trust Fund and the expenditures made for purposes of § 7–804(a) of this subtitle, § 7–902(a) of this title, and **[**§ 3A–702**] § 3.5–702** of the State Finance and Procurement Article.

Article – Insurance

31–103.

(a) The Exchange is subject to:

(2) the following provisions of the State Finance and Procurement Article:

(i) Title **[**3A**] 3.5**, Subtitle 3 (Information Processing), to the extent that the Secretary of Information Technology determines that an information technology project of the Exchange is a major information technology development project;

(b) The Exchange is not subject to:

(2) Title **[**3A**] 3.5**, Subtitle 3 (Information Processing) of the State Finance and Procurement Article, except to the extent determined by the Secretary of Information Technology under subsection (a)(2)(i) of this section;

Article – Natural Resources

1–403.

(c) The Department shall develop the electronic system consistent with the statewide information technology master plan developed under Title **[**3A**] 3.5**, Subtitle 3 of the State Finance and Procurement Article.

Article – State Finance and Procurement

3.5–101.

(a) In this title the following words have the meanings indicated.

(e) "Unit of State government" means an agency or unit of the Executive Branch of State government.

SUBTITLE 2A. OFFICE OF SECURITY MANAGEMENT.

3.5–2A–01.

(A) IN THIS SUBTITLE THE FOLLOWING WORDS HAVE THE MEANINGS INDICATED.

(B) "COUNCIL" MEANS THE MARYLAND CYBERSECURITY COORDINATING COUNCIL.

(C) "OFFICE" MEANS THE OFFICE OF SECURITY MANAGEMENT.

3.5–2A–02.

THERE IS AN OFFICE OF SECURITY MANAGEMENT WITHIN THE DEPARTMENT.

3.5–2A–03.

(A) THE HEAD OF THE OFFICE IS THE STATE CHIEF INFORMATION SECURITY OFFICER.

(B) THE STATE CHIEF INFORMATION SECURITY OFFICER SHALL:

(1) BE APPOINTED BY THE GOVERNOR WITH THE ADVICE AND CONSENT OF THE SENATE;

(2) SERVE AT THE PLEASURE OF THE GOVERNOR;

(3) BE SUPERVISED BY THE SECRETARY; AND

(4) SERVE AS THE CHIEF INFORMATION SECURITY OFFICER OF THE DEPARTMENT.

(C) THE STATE CHIEF INFORMATION SECURITY OFFICER SHALL PROVIDE CYBERSECURITY ADVICE AND RECOMMENDATIONS TO THE GOVERNOR ON REQUEST.

(D) (1) (I) THERE IS A DIRECTOR OF LOCAL CYBERSECURITY, WHO SHALL BE APPOINTED BY THE STATE CHIEF INFORMATION SECURITY OFFICER.

(II) THE DIRECTOR OF LOCAL CYBERSECURITY SHALL WORK IN COORDINATION WITH THE MARYLAND EMERGENCY MANAGEMENT AGENCY TO PROVIDE TECHNICAL ASSISTANCE, COORDINATE RESOURCES, AND IMPROVE CYBERSECURITY PREPAREDNESS FOR UNITS OF LOCAL GOVERNMENT.

(2) (I) THERE IS A DIRECTOR OF STATE CYBERSECURITY, WHO SHALL BE APPOINTED BY THE STATE CHIEF INFORMATION SECURITY OFFICER.

(II) THE DIRECTOR OF STATE CYBERSECURITY IS RESPONSIBLE FOR IMPLEMENTATION OF THIS SECTION WITH RESPECT TO UNITS OF STATE GOVERNMENT.

(E) THE DEPARTMENT SHALL PROVIDE THE OFFICE WITH SUFFICIENT STAFF TO PERFORM THE FUNCTIONS OF THIS SUBTITLE.

(F) THE OFFICE MAY PROCURE RESOURCES, INCLUDING REGIONAL COORDINATORS, NECESSARY TO FULFILL THE REQUIREMENTS OF THIS SUBTITLE.

3.5–2A–04.

(A) THE OFFICE IS RESPONSIBLE FOR:

(1) THE DIRECTION, COORDINATION, AND IMPLEMENTATION OF THE OVERALL CYBERSECURITY STRATEGY AND POLICY FOR UNITS OF STATE GOVERNMENT; AND

(2) THE COORDINATION OF RESOURCES AND EFFORTS TO IMPLEMENT CYBERSECURITY BEST PRACTICES AND IMPROVE OVERALL CYBERSECURITY PREPAREDNESS AND RESPONSE FOR UNITS OF LOCAL GOVERNMENT, LOCAL SCHOOL BOARDS, LOCAL SCHOOL SYSTEMS, AND LOCAL HEALTH DEPARTMENTS.

(B) THE OFFICE SHALL:

(1) ESTABLISH STANDARDS TO CATEGORIZE ALL INFORMATION COLLECTED OR MAINTAINED BY OR ON BEHALF OF EACH UNIT OF STATE GOVERNMENT;

(2) ESTABLISH STANDARDS TO CATEGORIZE ALL INFORMATION SYSTEMS MAINTAINED BY OR ON BEHALF OF EACH UNIT OF STATE GOVERNMENT;

(3) DEVELOP GUIDELINES GOVERNING THE TYPES OF INFORMATION AND INFORMATION SYSTEMS TO BE INCLUDED IN EACH CATEGORY;

(4) ESTABLISH SECURITY REQUIREMENTS FOR INFORMATION AND INFORMATION SYSTEMS IN EACH CATEGORY;

(5) ASSESS THE CATEGORIZATION OF INFORMATION AND INFORMATION SYSTEMS AND THE ASSOCIATED IMPLEMENTATION OF THE SECURITY REQUIREMENTS ESTABLISHED UNDER ITEM (4) OF THIS SUBSECTION;

(6) IF THE STATE CHIEF INFORMATION SECURITY OFFICER DETERMINES THAT THERE ARE SECURITY VULNERABILITIES OR DEFICIENCIES IN THE IMPLEMENTATION OF THE SECURITY REQUIREMENTS ESTABLISHED UNDER ITEM (4) OF THIS SUBSECTION, DETERMINE WHETHER AN INFORMATION SYSTEM SHOULD BE ALLOWED TO CONTINUE TO OPERATE OR BE CONNECTED TO THE NETWORK ESTABLISHED IN ACCORDANCE WITH § 3.5–404 OF THIS TITLE;

(7) MANAGE SECURITY AWARENESS TRAINING FOR ALL APPROPRIATE EMPLOYEES OF UNITS OF STATE GOVERNMENT;

(8) ASSIST IN THE DEVELOPMENT OF DATA MANAGEMENT, DATA GOVERNANCE, AND DATA SPECIFICATION STANDARDS TO PROMOTE STANDARDIZATION AND REDUCE RISK;

(9) ASSIST IN THE DEVELOPMENT OF A DIGITAL IDENTITY STANDARD AND SPECIFICATION APPLICABLE TO ALL PARTIES COMMUNICATING, INTERACTING, OR CONDUCTING BUSINESS WITH OR ON BEHALF OF A UNIT OF STATE GOVERNMENT;

(10) DEVELOP AND MAINTAIN INFORMATION TECHNOLOGY SECURITY POLICY, STANDARDS, AND GUIDANCE DOCUMENTS, CONSISTENT WITH BEST PRACTICES DEVELOPED BY THE NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY;

(11) TO THE EXTENT PRACTICABLE, SEEK, IDENTIFY, AND INFORM RELEVANT STAKEHOLDERS OF ANY AVAILABLE FINANCIAL ASSISTANCE PROVIDED BY THE FEDERAL GOVERNMENT OR NON–STATE ENTITIES TO SUPPORT THE WORK OF THE OFFICE;

(12) REVIEW AND CERTIFY LOCAL CYBERSECURITY PREPAREDNESS AND RESPONSE PLANS;

(13) PROVIDE TECHNICAL ASSISTANCE TO LOCALITIES IN MITIGATING AND RECOVERING FROM CYBERSECURITY INCIDENTS; AND

(14) PROVIDE TECHNICAL SERVICES, ADVICE, AND GUIDANCE TO UNITS OF LOCAL GOVERNMENT TO IMPROVE CYBERSECURITY PREPAREDNESS, PREVENTION, RESPONSE, AND RECOVERY PRACTICES.

(C) THE OFFICE, IN COORDINATION WITH THE MARYLAND EMERGENCY MANAGEMENT AGENCY, SHALL:

(1) ASSIST LOCAL POLITICAL SUBDIVISIONS, INCLUDING COUNTIES, SCHOOL SYSTEMS, SCHOOL BOARDS, AND LOCAL HEALTH DEPARTMENTS, IN:

(I) THE DEVELOPMENT OF CYBERSECURITY PREPAREDNESS AND RESPONSE PLANS; AND

(II) IMPLEMENTING BEST PRACTICES AND GUIDANCE DEVELOPED BY THE DEPARTMENT;

(2) CONNECT LOCAL ENTITIES TO APPROPRIATE RESOURCES FOR ANY OTHER PURPOSE RELATED TO CYBERSECURITY PREPAREDNESS AND RESPONSE; AND

(3) DEVELOP APPROPRIATE REPORTS ON LOCAL CYBERSECURITY PREPAREDNESS.

(D) THE OFFICE, IN COORDINATION WITH THE MARYLAND EMERGENCY MANAGEMENT AGENCY, MAY:

(1) CONDUCT REGIONAL EXERCISES, AS NECESSARY, IN COORDINATION WITH THE NATIONAL GUARD, LOCAL EMERGENCY MANAGERS, AND OTHER STATE AND LOCAL ENTITIES; AND

(2) ESTABLISH REGIONAL ASSISTANCE GROUPS TO DELIVER OR COORDINATE SUPPORT SERVICES TO LOCAL POLITICAL SUBDIVISIONS, AGENCIES, OR REGIONS.

(E) ON OR BEFORE DECEMBER 31 EACH YEAR, THE OFFICE SHALL REPORT TO THE GOVERNOR AND, IN ACCORDANCE WITH § 2–1257 OF THE STATE GOVERNMENT ARTICLE, THE SENATE BUDGET AND TAXATION COMMITTEE, THE HOUSE APPROPRIATIONS COMMITTEE, AND THE JOINT COMMITTEE ON CYBERSECURITY, INFORMATION TECHNOLOGY, AND BIOTECHNOLOGY ON THE ACTIVITIES OF THE OFFICE AND THE STATE OF CYBERSECURITY PREPAREDNESS IN MARYLAND, INCLUDING:

(1) THE ACTIVITIES AND ACCOMPLISHMENTS OF THE OFFICE DURING THE PREVIOUS 12 MONTHS AT THE STATE AND LOCAL LEVELS; AND

(2) A COMPILATION AND ANALYSIS OF THE DATA FROM THE INFORMATION CONTAINED IN THE REPORTS RECEIVED BY THE OFFICE UNDER § 3.5–405 OF THIS TITLE, INCLUDING:

(I) A SUMMARY OF THE ISSUES IDENTIFIED BY THE CYBERSECURITY PREPAREDNESS ASSESSMENTS CONDUCTED THAT YEAR;

(II) THE STATUS OF VULNERABILITY ASSESSMENTS OF ALL UNITS OF STATE GOVERNMENT AND A TIMELINE FOR COMPLETION AND COST TO REMEDIATE ANY VULNERABILITIES EXPOSED;

(III) RECENT AUDIT FINDINGS OF ALL UNITS OF STATE GOVERNMENT AND OPTIONS TO IMPROVE FINDINGS IN FUTURE AUDITS, INCLUDING RECOMMENDATIONS FOR STAFF, BUDGET, AND TIMING;

(IV) ANALYSIS OF THE STATE'S EXPENDITURE ON CYBERSECURITY RELATIVE TO OVERALL INFORMATION TECHNOLOGY SPENDING FOR THE PRIOR 3 YEARS AND RECOMMENDATIONS FOR CHANGES TO THE BUDGET, INCLUDING AMOUNT, PURPOSE, AND TIMING TO IMPROVE STATE AND LOCAL CYBERSECURITY PREPAREDNESS;

(V) EFFORTS TO SECURE FINANCIAL SUPPORT FOR CYBER RISK MITIGATION FROM FEDERAL OR OTHER NON–STATE RESOURCES;

(VI) KEY PERFORMANCE INDICATORS ON THE CYBERSECURITY STRATEGIES IN THE DEPARTMENT'S INFORMATION TECHNOLOGY MASTER PLAN, INCLUDING TIME, BUDGET, AND STAFF REQUIRED FOR IMPLEMENTATION; AND

(VII) ANY ADDITIONAL RECOMMENDATIONS FOR IMPROVING STATE AND LOCAL CYBERSECURITY PREPAREDNESS.

3.5–2A–05.

(A) THERE IS A MARYLAND CYBERSECURITY COORDINATING COUNCIL.

(B) THE COUNCIL CONSISTS OF THE FOLLOWING MEMBERS:

(1) THE SECRETARY OF BUDGET AND MANAGEMENT, OR THE SECRETARY'S DESIGNEE;

(2) THE SECRETARY OF GENERAL SERVICES, OR THE SECRETARY'S DESIGNEE;

(3) THE SECRETARY OF HEALTH, OR THE SECRETARY'S DESIGNEE;

(4) THE SECRETARY OF HUMAN SERVICES, OR THE SECRETARY'S DESIGNEE;

(5) THE SECRETARY OF PUBLIC SAFETY AND CORRECTIONAL SERVICES, OR THE SECRETARY'S DESIGNEE;

(6) THE SECRETARY OF TRANSPORTATION, OR THE SECRETARY'S DESIGNEE;

(7) THE SECRETARY OF DISABILITIES, OR THE SECRETARY'S DESIGNEE;

(8) THE STATE CHIEF INFORMATION SECURITY OFFICER;

(9) THE ADJUTANT GENERAL OF THE MARYLAND NATIONAL GUARD, OR THE ADJUTANT GENERAL'S DESIGNEE;

(10) THE DIRECTOR OF THE MARYLAND EMERGENCY MANAGEMENT AGENCY, OR THE DIRECTOR'S DESIGNEE;

(11) THE SUPERINTENDENT OF STATE POLICE, OR THE SUPERINTENDENT'S DESIGNEE;

(12) THE DIRECTOR OF THE GOVERNOR'S OFFICE OF HOMELAND SECURITY, OR THE DIRECTOR'S DESIGNEE;

(13) THE EXECUTIVE DIRECTOR OF THE DEPARTMENT OF LEGISLATIVE SERVICES, OR THE EXECUTIVE DIRECTOR'S DESIGNEE;

(14) ONE REPRESENTATIVE OF THE ADMINISTRATIVE OFFICE OF THE COURTS;

(15) THE CHANCELLOR OF THE UNIVERSITY SYSTEM OF MARYLAND, OR THE CHANCELLOR'S DESIGNEE; AND

(16) ANY OTHER STAKEHOLDER THAT THE STATE CHIEF INFORMATION SECURITY OFFICER DEEMS APPROPRIATE.

(C) THE CHAIR OF THE COUNCIL IS THE STATE CHIEF INFORMATION SECURITY OFFICER.

(D) THE COUNCIL SHALL MEET AT LEAST QUARTERLY AT THE REQUEST OF THE CHAIR.

(E) THE COUNCIL SHALL PROVIDE ADVICE AND RECOMMENDATIONS TO THE STATE CHIEF INFORMATION SECURITY OFFICER REGARDING:

(1) THE STRATEGY AND IMPLEMENTATION OF CYBERSECURITY INITIATIVES AND RECOMMENDATIONS; AND

(2) BUILDING AND SUSTAINING THE CAPABILITY OF THE STATE TO IDENTIFY AND MITIGATE CYBERSECURITY RISK AND RESPOND TO AND RECOVER FROM CYBERSECURITY–RELATED INCIDENTS.

(F) IN CARRYING OUT THE DUTIES OF THE COUNCIL, THE COUNCIL MAY CONSULT WITH OUTSIDE EXPERTS, INCLUDING EXPERTS IN THE PRIVATE SECTOR, GOVERNMENT AGENCIES, AND INSTITUTIONS OF HIGHER EDUCATION.

3.5–301.

(a) In this subtitle the following words have the meanings indicated.

(h) "Nonvisual access" means the ability, through keyboard control, synthesized speech, Braille, or other methods not requiring sight to receive, use, and manipulate

information and operate controls necessary to access information technology in accordance with standards adopted under **[**§ 3A–303(b)**] § 3.5–303(B)** of this subtitle.

3.5–302.

(c) Notwithstanding any other provision of law, except as provided in subsection (a) of this section and **[**§§ 3A–307(a)(2), 3A–308, and 3A–309**] §§ 3.5–307(A)(2), 3.5–308, AND 3.5–309** of this subtitle, this subtitle applies to all units of the Executive Branch of State government including public institutions of higher education other than Morgan State University, the University System of Maryland, and St. Mary's College of Maryland.

3.5–303.

(b) On or before January 1, 2020, the Secretary, or the Secretary's designee, shall:

(2) establish a process for the Secretary or the Secretary's designee to:

(ii) 2. for information technology procured by a State unit on or after January 1, 2020, enforce the nonvisual access clause developed under **[**§ 3A–311**] § 3.5–311** of this subtitle, including the enforcement of the civil penalty described in **[**§ 3A–311(a)(2)(iii)1**] § 3.5–311(A)(2)(III)1** of this subtitle.

3.5–307.

(a) (2) A unit of State government other than a public institution of higher education may not make expenditures for major information technology development projects except as provided in **[**§ 3A–308**] § 3.5–308** of this subtitle.

3.5–309.

(c) The Secretary:

(2) subject to the provisions of § 2–201 of this article and **[**§ 3A–307**] § 3.5–307** of this subtitle, may receive and accept contributions, grants, or gifts of money or property.

(i) The Fund may be used:

(3) notwithstanding **[**§ 3A–301(b)(2)**] § 3.5–301(B)(2)** of this subtitle, for the costs of the first 12 months of operation and maintenance of a major information technology development project.

(l) Notwithstanding subsection (b) of this section, money paid into the Fund under subsection (e)(2) of this section may be used to support the State telecommunication and computer network established under **[**§ 3A–404**] § 3.5–404** of this title, including program development for these activities.

3.5–311.

(a) (2) On or after January 1, 2020, the nonvisual access clause developed in accordance with paragraph (1) of this subsection shall include a statement that:

(i) within 18 months after the award of the procurement, the Secretary, or the Secretary's designee, will determine whether the information technology meets the nonvisual access standards adopted in accordance with **[**§ 3A–303(b)**] § 3.5–303(B)** of this subtitle;

3.5–404.

(a) The General Assembly declares that:

(1) it is the policy of the State to foster telecommunication and computer networking among State and local governments, their agencies, and educational institutions in the State;

(2) there is a need to improve access, especially in rural areas, to efficient telecommunication and computer network connections;

(3) improvement of telecommunication and computer networking for State and local governments and educational institutions promotes economic development, educational resource use and development, and efficiency in State and local administration;

(4) rates for the intrastate inter–LATA telephone communications needed for effective integration of telecommunication and computer resources are prohibitive for many smaller governments, agencies, and institutions; and

(5) the use of improved State telecommunication and computer networking under this section is intended not to compete with commercial access to advanced network technology, but rather to foster fundamental efficiencies in government and education for the public good.

(b) (1) The Department shall establish a telecommunication and computer network in the State.

(2) The network shall consist of:

(i) one or more connection facilities for telecommunication and computer connection in each local access transport area (LATA) in the State; and

(ii) facilities, auxiliary equipment, and services required to support the network in a reliable and secure manner.

(c) The network shall be accessible through direct connection and through local intra–LATA telecommunications to State and local governments and public and private educational institutions in the State.

(D) ON OR BEFORE DECEMBER 1 EACH YEAR, EACH UNIT OF THE LEGISLATIVE OR JUDICIAL BRANCH OF STATE GOVERNMENT, EACH UNIT OF LOCAL GOVERNMENT, AND ANY LOCAL AGENCIES THAT USE THE NETWORK ESTABLISHED UNDER SUBSECTION (B) OF THIS SECTION SHALL CERTIFY TO THE DEPARTMENT THAT THE UNIT IS IN COMPLIANCE WITH THE DEPARTMENT'S MINIMUM SECURITY STANDARDS.

3.5–405.

(A) ON OR BEFORE DECEMBER 1 EACH YEAR, EACH UNIT OF STATE GOVERNMENT SHALL:

(1) COMPLETE A CYBERSECURITY PREPAREDNESS ASSESSMENT AND REPORT THE RESULTS TO THE OFFICE OF SECURITY MANAGEMENT IN ACCORDANCE WITH GUIDELINES DEVELOPED BY THE OFFICE; AND

(2) SUBMIT A REPORT TO THE GOVERNOR AND THE OFFICE OF SECURITY MANAGEMENT THAT INCLUDES:

(I) AN INVENTORY OF ALL INFORMATION SYSTEMS AND APPLICATIONS USED OR MAINTAINED BY THE UNIT;

(II) A FULL DATA INVENTORY OF THE UNIT;

(III) A LIST OF ALL CLOUD OR STATISTICAL ANALYSIS SYSTEM SOLUTIONS USED BY THE UNIT;

(IV) A LIST OF ALL PERMANENT AND TRANSIENT VENDOR INTERCONNECTIONS THAT ARE IN PLACE;

(V) THE NUMBER OF UNIT EMPLOYEES WHO HAVE RECEIVED CYBERSECURITY TRAINING;

(VI) THE TOTAL NUMBER OF UNIT EMPLOYEES WHO USE THE NETWORK;

(VII) THE NUMBER OF INFORMATION TECHNOLOGY STAFF POSITIONS, INCLUDING VACANCIES;

(VIII) THE NUMBER OF NON–INFORMATION TECHNOLOGY STAFF POSITIONS, INCLUDING VACANCIES;

(IX) THE UNIT'S INFORMATION TECHNOLOGY BUDGET, ITEMIZED TO INCLUDE THE FOLLOWING CATEGORIES:

1. SERVICES;

2. EQUIPMENT;

3. APPLICATIONS;

4. PERSONNEL;

5. SOFTWARE LICENSING;

6. DEVELOPMENT;

7. NETWORK PROJECTS;

8. MAINTENANCE; AND

9. CYBERSECURITY;

(X) ANY MAJOR INFORMATION TECHNOLOGY INITIATIVES TO MODERNIZE THE UNIT'S INFORMATION TECHNOLOGY SYSTEMS OR IMPROVE CUSTOMER ACCESS TO STATE AND LOCAL SERVICES;

(XI) THE UNIT'S PLANS FOR FUTURE FISCAL YEARS TO IMPLEMENT THE UNIT'S INFORMATION TECHNOLOGY GOALS; AND

(XII) ANY OTHER KEY PERFORMANCE INDICATORS REQUIRED BY THE OFFICE OF SECURITY MANAGEMENT TO TRACK COMPLIANCE OR CONSISTENCY WITH THE DEPARTMENT'S STATEWIDE INFORMATION TECHNOLOGY MASTER PLAN.

(B) (1) EACH UNIT OF STATE GOVERNMENT SHALL REPORT A CYBERSECURITY INCIDENT IN ACCORDANCE WITH PARAGRAPH (2) OF THIS SUBSECTION TO THE STATE CHIEF INFORMATION SECURITY OFFICER.

(2) FOR THE REPORTING OF CYBERSECURITY INCIDENTS UNDER PARAGRAPH (1) OF THIS SUBSECTION, THE STATE CHIEF INFORMATION SECURITY OFFICER SHALL DETERMINE:

(I) THE CRITERIA FOR DETERMINING WHEN AN INCIDENT MUST BE REPORTED;

(II) THE MANNER IN WHICH TO REPORT; AND

(III) THE TIME PERIOD WITHIN WHICH A REPORT MUST BE MADE.

(C) (1) THIS SUBSECTION DOES NOT APPLY TO MUNICIPAL GOVERNMENTS.

(2) ON OR BEFORE DECEMBER 1 EACH YEAR, EACH COUNTY GOVERNMENT, LOCAL SCHOOL SYSTEM, AND LOCAL HEALTH DEPARTMENT SHALL:

(I) IN CONSULTATION WITH THE LOCAL EMERGENCY MANAGER, CREATE OR UPDATE A CYBERSECURITY PREPAREDNESS AND RESPONSE PLAN AND SUBMIT THE PLAN TO THE OFFICE OF SECURITY MANAGEMENT FOR APPROVAL;

(II) COMPLETE A CYBERSECURITY PREPAREDNESS ASSESSMENT AND REPORT THE RESULTS TO THE OFFICE OF SECURITY MANAGEMENT IN ACCORDANCE WITH GUIDELINES DEVELOPED BY THE OFFICE; AND

(III) REPORT TO THE OFFICE:

1. THE NUMBER OF INFORMATION TECHNOLOGY STAFF POSITIONS, INCLUDING VACANCIES;

2. THE ENTITY'S CYBERSECURITY BUDGET AND OVERALL INFORMATION TECHNOLOGY BUDGET;

3. THE NUMBER OF EMPLOYEES WHO HAVE RECEIVED CYBERSECURITY TRAINING; AND

4. THE TOTAL NUMBER OF EMPLOYEES WITH ACCESS TO THE ENTITY'S COMPUTER SYSTEMS AND DATABASES.

(3) (I) EACH COUNTY GOVERNMENT, LOCAL SCHOOL SYSTEM, AND LOCAL HEALTH DEPARTMENT SHALL REPORT A CYBERSECURITY INCIDENT IN ACCORDANCE WITH SUBPARAGRAPH (II) OF THIS PARAGRAPH TO THE APPROPRIATE LOCAL EMERGENCY MANAGER.

(II) FOR THE REPORTING OF CYBERSECURITY INCIDENTS TO LOCAL EMERGENCY MANAGERS UNDER SUBPARAGRAPH (I) OF THIS PARAGRAPH, THE STATE CHIEF INFORMATION SECURITY OFFICER SHALL DETERMINE:

1. THE CRITERIA FOR DETERMINING WHEN AN INCIDENT MUST BE REPORTED;

2. THE MANNER IN WHICH TO REPORT; AND

3. THE TIME PERIOD WITHIN WHICH A REPORT MUST BE MADE.

12–107.

(b) Subject to the authority of the Board, jurisdiction over procurement is as follows:

(2) the Department of General Services may:

(i) engage in or control procurement of:

10. information processing equipment and associated services, as provided in Title **[**3A**] 3.5**, Subtitle 3 of this article; and

11. telecommunication equipment, systems, or services, as provided in Title **[**3A**] 3.5**, Subtitle 4 of this article;

SECTION ~~2.~~ 3. AND BE IT FURTHER ENACTED, That this Act shall take effect October 1, 2021.

Approved:

_____

Governor.

_____

President of the Senate.

_____

Speaker of the House of Delegates.