SENATE BILL 780

S2, E4 2lr2090

By: **Senator Hester**
Introduced and read first time: February 7, 2022
Assigned to: Education, Health, and Environmental Affairs and Budget and Taxation

A BILL ENTITLED

AN ACT concerning

Cybersecurity Governance Act of 2022

FOR the purpose of establishing the 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; centralizing authority and control of the procurement of all information technology for the Executive Branch of State government in the Department; requiring the Secretary of Information Technology to provide or coordinate the procurement of managed cybersecurity services that are paid for by the State and used by local governments; requiring the Secretary of Information Technology, with the advice of a subcommittee of the Maryland Cybersecurity Council, to develop and maintain a statewide cybersecurity master plan; requiring the Governor to include a certain appropriation in the annual budget to cover the costs of implementing the statewide cybersecurity master plan; requiring the Governor to submit a certain annual report to certain committees of the General Assembly; requiring the Department to develop and require basic security requirements to be included in certain contracts; requiring each unit of the Legislative or Judicial Branch of State government and any division of the University System of Maryland 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 to obtain a certain periodic external vulnerability and risk assessment; 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; requiring the Department to complete implementation of a certain governance, risk, and compliance module on or before a certain date; requiring the State Chief Data Officer, on or before a certain date, to contract with an independent third party to develop a certain statewide reporting framework, run a baseline cybersecurity

EXPLANATION: **CAPITALS INDICATE MATTER ADDED TO EXISTING LAW.**
[Brackets**]** indicate matter deleted from existing law.

assessment, and report recommendations to the Governor and certain committees of the General Assembly; transferring certain appropriations, books and records, and employees to the Department; and generally relating to State cybersecurity coordination.

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
(2021 Replacement Volume)

BY repealing and reenacting, with amendments,
Article – Criminal Procedure
Section 10–221(b)
Annotated Code of Maryland
(2018 Replacement Volume and 2021 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 2021 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 2021 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 2021 Supplement)

BY repealing and reenacting, with amendments,
Article – Natural Resources
Section 1–403(c)
Annotated Code of Maryland
(2018 Replacement Volume and 2021 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
(2021 Replacement Volume)
(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"; 3.5–405, and 12–107(b)(2)(i)12.
Annotated Code of Maryland
(2021 Replacement Volume)

BY repealing and reenacting, with amendments,
Article – State Finance and Procurement
Section 3.5–301(j), 3.5–302(c), 3.5–303, 3.5–305, 3.5–307 through 3.5—314, 3.5–401, and 3.5–404
Annotated Code of Maryland
(2021 Replacement Volume)
(As enacted by Section 1 of this Act)

BY repealing
Article – State Finance and Procurement
Section 3.5–306
Annotated Code of Maryland
(2021 Replacement Volume)
(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
(2021 Replacement Volume)

BY repealing and reenacting, without amendments,
Article – State Government
Section 9–2901(b) and (g)
Annotated Code of Maryland
(2021 Replacement Volume)

BY adding to
Article – State Government
Section 9–2901(k)
Annotated Code of Maryland
(2021 Replacement Volume)

BY repealing and reenacting, with amendments,
Article – State Government
Section 9–2901(k)

Annotated Code of Maryland
(2021 Replacement Volume)

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 2. AND BE IT FURTHER ENACTED , That the Laws of Maryland read as follows:

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 DEPARTMENT OF EMERGENCY MANAGEMENT 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) FOR THE EXTERNAL ASSESSMENT REQUIRED UNDER § 3.5–405(B) OF THIS TITLE:

(I) AT LEAST ONCE EVERY 2 YEARS, ENSURE THAT THE EXTERNAL ASSESSMENT IS COMPLETED FOR EACH UNIT OF STATE GOVERNMENT;

(II) RECEIVE REPORTS ON VULNERABILITIES AND HIGH–RISK CONFIGURATIONS IDENTIFIED IN THE ASSESSMENT; AND

(III) ASSIST ANY UNIT IN NECESSARY REMEDIATION IDENTIFIED IN THE ASSESSMENT;

(10) CONDUCT AN ANNUAL CYBERSECURITY SURVEY OF ALL UNITS OF STATE GOVERNMENT;

(11) 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;

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

(13) 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;

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

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

(16) 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 DEPARTMENT OF EMERGENCY MANAGEMENT, 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 DEPARTMENT OF EMERGENCY MANAGEMENT, 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 THE STATE, INCLUDING:

(1) A SUMMARY OF THE FINDINGS OF THE SURVEY CONDUCTED UNDER SUBSECTION (B)(10) OF THIS SECTION;

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

(3) 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 VOTING 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 SECRETARY OF EMERGENCY MANAGEMENT, OR THE SECRETARY'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) IN ADDITION TO THE MEMBERS LISTED UNDER SUBSECTION (B) OF THIS SECTION, THE FOLLOWING REPRESENTATIVES SHALL SERVE AS NONVOTING MEMBERS OF THE COUNCIL:

(1) ONE MEMBER OF THE SENATE OF MARYLAND, APPOINTED BY THE PRESIDENT OF THE SENATE;

(2) ONE MEMBER OF THE HOUSE OF DELEGATES, APPOINTED BY THE SPEAKER OF THE HOUSE; AND

(3) ONE REPRESENTATIVE OF THE JUDICIARY, APPOINTED BY THE CHIEF JUDGE OF THE COURT OF APPEALS.

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

(E) (1) THE COUNCIL SHALL MEET AT LEAST QUARTERLY AT THE REQUEST OF THE CHAIR.

(2) MEETINGS OF THE COUNCIL SHALL BE CLOSED TO THE PUBLIC AND NOT SUBJECT TO TITLE 3 OF THE GENERAL PROVISIONS ARTICLE.

(F) THE COUNCIL SHALL:

(1) PROVIDE ADVICE AND RECOMMENDATIONS TO THE STATE CHIEF INFORMATION SECURITY OFFICER REGARDING:

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

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

(2) USE THE ANALYSIS COMPILED BY THE OFFICE UNDER § 3.5–2A–04(E)(3) OF THIS SUBTITLE TO PRIORITIZE CYBERSECURITY RISK ACROSS THE EXECUTIVE BRANCH AND MAKE CORRESPONDING RECOMMENDATIONS FOR SECURITY INVESTMENTS IN THE GOVERNOR'S ANNUAL BUDGET.

(G) 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.

(j) "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**] §§ 3.5–306(A)(2), 3.5–307, AND 3.5–308** 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, St. Mary's College of Maryland, and Baltimore City Community College.

3.5–303.

(a) The Secretary is responsible for carrying out the following duties:

(1) developing, maintaining, revising, and enforcing information technology policies, procedures, and standards;

(2) providing technical assistance, advice, and recommendations to the Governor and any unit of State government concerning information technology matters;

(3) reviewing the annual project plan for each unit of State government to make information and services available to the public over the Internet;

(4) developing and maintaining a statewide information technology master plan that will:

(i) **[**be the basis for**]** **CENTRALIZE** the management and direction of information technology within the Executive Branch of State government **UNDER THE CONTROL OF THE DEPARTMENT**;

(ii) include all aspects of State information technology including telecommunications, security, data processing, and information management;

(iii) consider interstate transfers as a result of federal legislation and regulation;

(iv) **[**work jointly with the Secretary of Budget and Management to ensure that information technology plans and budgets are consistent;

(v)**]** ensure that **THE** State information technology **[**plans, policies,**]** **PLAN AND RELATED POLICIES** and standards are consistent with State goals, objectives, and resources, and represent a long–range vision for using information technology to improve the overall effectiveness of State government; and

[(vi)**]** **(V)** include standards to assure nonvisual access to the information and services made available to the public over the Internet;

(5) PROVIDE OR COORDINATE THE PROCUREMENT OF MANAGED CYBERSECURITY SERVICES THAT ARE PAID FOR BY THE STATE AND USED BY LOCAL GOVERNMENTS;

(6) WITH THE ADVICE OF THE CYBERSECURITY MASTER PLAN SUBCOMMITTEE OF THE MARYLAND CYBERSECURITY COUNCIL, DEVELOP AND MAINTAIN A STATEWIDE CYBERSECURITY MASTER PLAN THAT WILL:

(I) CENTRALIZE THE MANAGEMENT AND DIRECTION OF CYBERSECURITY STRATEGY WITHIN THE EXECUTIVE BRANCH OF STATE GOVERNMENT UNDER THE CONTROL OF THE DEPARTMENT; AND

(II) SERVE AS THE BASIS FOR BUDGET ALLOCATIONS FOR CYBERSECURITY PREPAREDNESS FOR THE EXECUTIVE BRANCH OF STATE GOVERNMENT;

[(5)**] (7)** adopting by regulation and enforcing nonvisual access standards to be used in the procurement of information technology services **[**by or**]** on behalf of units of State government in accordance with subsection **[**(b)**] (C)** of this section;

[(6)**] (8)** in consultation with the Attorney General, advising and overseeing a consistent cybersecurity strategy for units of State government, including institutions under the control of the governing boards of the public institutions of higher education;

[(7)**] (9)** advising and consulting with the Legislative and Judicial branches of State government regarding a cybersecurity strategy; and

[(8)**] (10)** in consultation with the Attorney General, developing guidance on consistent cybersecurity strategies for counties, municipal corporations, school systems, and all other political subdivisions of the State.

(b) Nothing in subsection (a) of this section may be construed as establishing a mandate for any entity listed in subsection **[**(a)(8)**] (A)(10)** of this section.

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

(1) adopt new nonvisual access procurement standards that:

(i) provide an individual with disabilities with nonvisual access in a way that is fully and equally accessible to and independently usable by the individual with disabilities so that the individual is able to acquire the same information, engage in the same interactions, and enjoy the same services as users without disabilities, with substantially equivalent ease of use; and

(ii) are consistent with the standards of § 508 of the federal Rehabilitation Act of 1973; and

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

(i) determine whether information technology meets the nonvisual access standards adopted under item (1) of this subsection; and

(ii) 1. for information technology procured by a State unit before January 1, 2020, and still used by the State unit on or after January 1, 2020, work with the vendor to modify the information technology to meet the nonvisual access standards, if practicable; or

2. for information technology procured by a State unit **OR THE DEPARTMENT** on or after January 1, 2020, enforce the nonvisual access clause

developed under **[**§ 3A–311**] § 3.5–310** of this subtitle, including the enforcement of the civil penalty described in **[**§ 3A–311(a)(2)(iii)1**] § 3.5–310(A)(2)(III)1** of this subtitle.

(D) (1) THE GOVERNOR SHALL INCLUDE AN APPROPRIATION IN THE ANNUAL BUDGET IN AN AMOUNT NECESSARY TO COVER THE COSTS OF IMPLEMENTING THE STATEWIDE CYBERSECURITY MASTER PLAN DEVELOPED UNDER SUBSECTION (A) OF THIS SECTION.

(2) ON OR BEFORE JANUARY 31 EACH YEAR, THE GOVERNOR SHALL SUBMIT A REPORT IN ACCORDANCE WITH § 2–1257 OF THE STATE GOVERNMENT ARTICLE TO THE SENATE BUDGET AND TAXATION COMMITTEE AND THE HOUSE APPROPRIATIONS COMMITTEE THAT INCLUDES:

(I) SPECIFIC INFORMATION ON THE INFORMATION TECHNOLOGY BUDGET AND CYBERSECURITY BUDGET THAT THE GOVERNOR HAS SUBMITTED TO THE GENERAL ASSEMBLY FOR THE UPCOMING FISCAL YEAR; AND

(II) HOW THE BUDGETS LISTED UNDER ITEM (I) OF THIS PARAGRAPH COMPARE TO THE ANNUAL OVERVIEW OF THE U.S. PRESIDENT'S BUDGET SUBMISSION ON INFORMATION TECHNOLOGY AND CYBERSECURITY TO CONGRESS CONDUCTED BY THE U.S. OFFICE OF MANAGEMENT AND BUDGET.

3.5–305.

(a) **[**Except as provided in subsection (b) of this section, in accordance with guidelines established by the Secretary, each unit of State government shall develop and submit to the Secretary:

(1) information technology policies and standards;

(2) an information technology plan; and

(3) an annual project plan outlining the status of efforts to make information and services available to the public over the Internet.

(b) (1)**]** The governing boards of the public institutions of higher education shall develop and submit information technology policies and standards and an information technology plan for their respective institutions or systems to the Secretary.

[(2)**] (B)** If the Secretary finds that the submissions required under this **[**subsection**] SECTION** are consistent with the master plan, the Secretary shall incorporate those submissions into the master plan.

[(3)**] (C)** If the Secretary finds that the submissions required under this **[**subsection**] SECTION** are not consistent with the master plan:

[(i)**] (1)** the Secretary shall return the submissions to the governing boards; and

[(ii)**] (2)** the governing boards shall revise the submissions as appropriate and submit the revised policies, standards, and plans to the Secretary.

[3.5–306.

Information technology of each unit of State government shall be consistent with the master plan.**]**

[3.5–307.**] 3.5–306.**

(a) (1) **[**A unit of State government**] THE DEPARTMENT** may not purchase, lease, or rent information technology **ON BEHALF OF A UNIT OF STATE GOVERNMENT** unless consistent with the master plan.

(2) A unit of State government other than a public institution of higher education **[**may not make**] SHALL SUBMIT REQUESTS FOR** expenditures for major information technology development projects **[**except**]** as provided in **[**§ 3A–308**] § 3.5–307** of this subtitle.

(b) **[**(1)**]** The Secretary may review any information technology project for consistency with the master plan.

[(2) Any information technology project selected for review may not be implemented without the approval of the Secretary.**]**

(c) (1) A unit of State government shall advise the Secretary of any information technology proposal involving resource sharing, the exchange of goods or services, or a gift, contribution, or grant of real or personal property.

(2) The Secretary shall determine if the value of the resources, services, and property to be obtained by the State under the terms of any proposal submitted in accordance with the provisions of paragraph (1) of this subsection equals or exceeds $100,000.

(3) If the value of any proposal submitted in accordance with this subsection equals or exceeds $100,000 and the Secretary and unit agree to proceed with the proposal, information on the proposal shall be:

(i) advertised for a period of at least 30 days in the eMaryland Marketplace; and

(ii) submitted, simultaneously with the advertisement, to the Legislative Policy Committee for a 60–day review and comment period, during which time the Committee may recommend that the proposal be treated as a procurement contract under Division II of this article.

(4) Following the period for review and comment by the Legislative Policy Committee under paragraph (3) of this subsection, the proposal is subject to approval by the Board of Public Works.

(5) This subsection may not be construed as authorizing an exception from the requirements of Division II of this article for any contract that otherwise would be subject to the State procurement process.

[3.5–308.**] 3.5–307.**

(a) This section does not apply to a public institution of higher education.

(b) In submitting its information technology project requests, a unit of State government shall designate projects which are major information technology development projects.

(c) In reviewing information technology project requests, the Secretary may change a unit's designation of a major information technology development project.

(d) The Secretary shall review and, with the advice of the Secretary of Budget and Management, approve major information technology development projects and specifications for consistency with all statewide plans, policies, and standards, including a systems development life cycle plan.

(e) The Secretary shall be responsible for overseeing the implementation of major information technology development projects**[**, regardless of fund source**]**.

(f) With the advice of the Secretary of Budget and Management, expenditures for major information technology development projects shall be subject to the approval of the Secretary who shall approve expenditures only when those projects are consistent with statewide plans, policies, and standards.

(g) (1) The Secretary shall approve funding for major information technology development projects only when those projects are supported by an approved systems development life cycle plan.

(2) An approved systems development life cycle plan shall include submission of:

(i) a project planning request that details initial planning for the project, including:

1. the project title, appropriation code, and summary;

2. a description of:

A. the needs addressed by the project;

B. the potential risks associated with the project;

C. possible alternatives; and

D. the scope and complexity of the project; and

3. an estimate of:

A. the total costs required to complete through planning; and

B. the fund sources available to support planning costs; and

(ii) a project implementation request to begin full design, development, and implementation of the project after the completion of planning, including:

1. the project title, appropriation code, and summary;

2. a description of:

A. the needs addressed by the project;

B. the potential risks associated with the project;

C. possible alternatives;

D. the scope and complexity of the project; and

E. how the project meets the goals of the statewide master plan; and

3. an estimate of:

A. the total project cost; and

B. the fund sources available.

(3) The Secretary may approve funding incrementally, consistent with the systems development life cycle plan.

[3.5–309.**] 3.5–308.**

(a) There is a Major Information Technology Development Project Fund.

(b) The purpose of the Fund is to support major information technology development projects.

(c) The Secretary:

(1) shall administer the Fund in accordance with this section; and

(2) subject to the provisions of § 2–201 of this article and **[**§ 3A–307**] § 3.5–306** of this subtitle, may receive and accept contributions, grants, or gifts of money or property.

(d) (1) The Fund is a special, nonlapsing fund that is not subject to § 7–302 of this article.

(2) The State Treasurer shall hold the Fund separately and the Comptroller shall account for the Fund.

(3) The State Treasurer shall invest and reinvest the money of the Fund in the same manner as other State money may be invested.

(4) Any investment earnings of the Fund shall be paid into the Fund.

(e) Except as provided in subsection (f) of this section, the Fund consists of:

(1) money appropriated in the State budget to the Fund;

(2) as approved by the Secretary, money received from:

(i) the sale, lease, or exchange of communication sites, communication facilities, or communication frequencies for information technology purposes; or

(ii) an information technology agreement involving resource sharing;

(3) that portion of money earned from pay phone commissions to the extent that the commission rates exceed those in effect in December 1993;

(4) money received and accepted as contributions, grants, or gifts as authorized under subsection (c) of this section;

(5) general funds appropriated for major information technology development projects of any unit of State government other than a public institution of higher education that:

(i) are unencumbered and unexpended at the end of a fiscal year;

(ii) have been abandoned; or

(iii) have been withheld by the General Assembly or the Secretary;

(6) any investment earnings; and

(7) any other money from any source accepted for the benefit of the Fund.

(f) The Fund does not include any money:

(1) received by the Department of Transportation, the Maryland Transportation Authority, Baltimore City Community College, or the Maryland Public Broadcasting Commission;

(2) received by the Judicial or Legislative branches of State government; or

(3) generated from pay phone commissions that are credited to other accounts or funds in accordance with other provisions of law or are authorized for other purposes in the State budget or through an approved budget amendment.

(g) The Governor shall submit with the State budget:

(1) a summary showing the unencumbered balance in the Fund as of the close of the prior fiscal year and a listing of any encumbrances;

(2) an estimate of projected revenue from each of the sources specified in subsection (e) of this section for the fiscal year for which the State budget is submitted; and

(3) a descriptive listing of projects reflecting projected costs for the fiscal year for which the State budget is submitted and any estimated future year costs.

(h) Expenditures from the Fund shall be made only:

(1) in accordance with an appropriation approved by the General Assembly in the annual State budget; or

(2) through an approved State budget amendment under Title 7, Subtitle 2, Part II of this article, provided that a State budget amendment for any project not requested as part of the State budget submission or for any project for which the scope or cost has increased by more than 5% or $250,000 shall be submitted to the budget committees allowing a 30–day period for their review and comment.

(i) The Fund may be used:

(1) for major information technology development projects;

(2) as provided in subsections (j) and (l) of this section; or

(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.

(j) Notwithstanding subsection (b) of this section and except for the cost incurred in administering the Fund, each fiscal year up to $1,000,000 of this Fund may be used for:

(1) educationally related information technology projects;

(2) application service provider initiatives as provided for in Title 9, Subtitle 22 of the State Government Article; or

(3) information technology projects, including:

(i) pilots; and

(ii) prototypes.

(k) A unit of **[**State government or**]** local government may submit a request to the Secretary to support the cost of an information technology project with money under subsection (j) of this section.

(l) (1) Notwithstanding subsection (b) of this section and in accordance with paragraph (2) of this subsection, money paid into the Fund under subsection (e)(2) of this section shall be used to support:

(i) the State telecommunication and computer network established under **[**§ 3A–404**] § 3.5–404** of this title, including program development for these activities; and

(ii) the Statewide Public Safety Interoperability Radio System, also known as Maryland First (first responder interoperable radio system team), under Title 1, Subtitle 5 of the Public Safety Article.

(2) The Secretary may determine the portion of the money paid into the Fund that shall be allocated to each program described in paragraph (1) of this subsection.

(m) (1) On or before November 1 of each year, the Secretary shall report to the Governor, the Secretary of Budget and Management, and to the budget committees of the General Assembly and submit a copy of the report to the General Assembly, in accordance with § 2–1257 of the State Government Article.

(2) The report shall include:

(i) the financial status of the Fund and a summary of its operations for the preceding fiscal year;

(ii) an accounting for the preceding fiscal year of all money from each of the revenue sources specified in subsection (e) of this section, including any expenditures made from the Fund; and

(iii) for each project receiving money from the Fund in the preceding fiscal year and for each major information technology development project receiving funding from any source other than the Fund in the preceding fiscal year:

1. the status of the project;

2. a comparison of estimated and actual costs of the project;

3. any known or anticipated changes in scope or costs of the project;

4. an evaluation of whether the project is using best practices; and

5. a summary of any monitoring and oversight of the project from outside the agency in which the project is being developed, including a description of any problems identified by any external review and any corrective actions taken.

(n) On or before January 15 of each year, for each major information technology development project currently in development or for which operations and maintenance funding is being provided in accordance with subsection (i)(3) of this section, subject to § 2–1257 of the State Government Article, the Secretary shall provide a summary report to the Department of Legislative Services with the most up–to–date project information including:

(1) project status;

(2) any schedule, cost, and scope changes since the last annual report;

(3) a risk assessment including any problems identified by any internal or external review and any corrective actions taken; and

(4) any change in the monitoring or oversight status.

[3.5–310.**] 3.5–309.**

This subtitle may not be construed to give the Secretary authority over:

(1) the content of educational applications or curriculum at the State or local level; or

(2) the entities that may participate in such educational programs.

[3.5–311.**] 3.5–310.**

(a) (1) The Secretary or the Secretary's designee, in consultation with other units of State government, and after public comment, shall develop a nonvisual access clause for use in the procurement of information technology and information technology services that specifies that the technology and services:

(i) must provide equivalent access for effective use by both visual and nonvisual means;

(ii) will present information, including prompts used for interactive communications, in formats intended for both visual and nonvisual use;

(iii) can be integrated into networks for obtaining, retrieving, and disseminating information used by individuals who are not blind or visually impaired; and

(iv) shall be obtained, whenever possible, without modification for compatibility with software and hardware for nonvisual access.

(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;

(ii) if the information technology does not meet the nonvisual access standards, the Secretary, or the Secretary's designee, will notify the vendor in writing that the vendor, at the vendor's own expense, has 12 months after the date of the notification to modify the information technology in order to meet the nonvisual access standards; and

(iii) if the vendor fails to modify the information technology to meet the nonvisual access standards within 12 months after the date of the notification, the vendor:

1. may be subject to a civil penalty of:

A. for a first offense, a fine not exceeding $5,000; and

B. for a subsequent offense, a fine not exceeding $10,000; and

2. shall indemnify the State for liability resulting from the use of information technology that does not meet the nonvisual access standards.

[3.5–312.**] 3.5–311.**

The Secretary may delegate the duties set forth in this subtitle to carry out its purposes.

[3.5–313.**] 3.5–312.**

(a) (1) In this section the following words have the meanings indicated.

(2) "Agency" includes a unit of State government that receives funds that are not appropriated in the annual budget bill.

(3) (i) "Payee" means any party who receives from the State an aggregate payment of $25,000 in a fiscal year.

(ii) "Payee" does not include:

1. a State employee with respect to the employee's compensation; or

2. a State retiree with respect to the retiree's retirement allowance.

(4) "Searchable website" means a website created in accordance with this section that displays and searches State payment data.

(b) (1) The Department shall develop and operate a single searchable website, accessible to the public at no cost through the Internet.

(2) On or before the 15th day of the month that follows the month in which an agency makes a payment to a payee, the Department shall update the payment data on the searchable website.

(c) The searchable website shall contain State payment data, including:

(1) the name of a payee receiving a payment;

(2) the location of a payee by postal zip code;

(3) the amount of a payment; and

(4) the name of an agency making a payment.

(d) The searchable website shall allow the user to:

(1) search data for fiscal year 2008 and each year thereafter; and

(2) search by the following data fields:

(i) a payee receiving a payment;

(ii) an agency making a payment; and

(iii) the zip code of a payee receiving a payment.

(e) State agencies shall provide appropriate assistance to the Secretary to ensure the existence and ongoing operation of the single website.

(f) This section may not be construed to require the disclosure of information that is confidential under State or federal law.

(g) This section shall be known and may be cited as the "Maryland Funding Accountability and Transparency Act".

[3.5–314.**] 3.5–313.**

(a) In this section, "security–sensitive data" means information that is protected against unwarranted disclosure.

(b) In accordance with guidelines established by the Secretary, each unit of State government shall develop a plan to:

(1) identify unit personnel who handle security–sensitive data; and

(2) establish annual security overview training or refresher security training for each employee who handles security–sensitive data as part of the employee's duties.

3.5–401.

(a) The Department shall:

(1) coordinate the development, procurement, management, and operation of telecommunication equipment, systems, and services by State government;

(2) TO ADDRESS PREPAREDNESS AND RESPONSE CAPABILITIES OF LOCAL JURISDICTIONS, COORDINATE THE PROCUREMENT OF MANAGED CYBERSECURITY SERVICES PROCURED BY LOCAL GOVERNMENTS WITH STATE FUNDING;

[(2)**] (3)** acquire and manage common user telecommunication equipment, systems, or services and charge units of State government for their

proportionate share of the costs of installation, maintenance, and operation of the common user telecommunication equipment, systems, or services;

[(3)**] (4)** promote compatibility of telecommunication systems by developing policies, procedures, and standards for the **[**acquisition and**]** use of telecommunication equipment, systems, and services by units of State government;

[(4)**] (5)** coordinate State government telecommunication systems and services by reviewing requests by units of State government for**, AND ACQUIRING ON BEHALF OF UNITS OF STATE GOVERNMENT,** telecommunication equipment, systems, or services;

[(5)**] (6)** advise units of State government about planning**[**, acquisition,**]** and operation of telecommunication equipment, systems, or services; and

[(6)**] (7)** provide radio frequency coordination for State and local governments in accordance with regulations of the Federal Communications Commission.

(b) The Department may make arrangement for a user other than a unit of State government to have access to and use of State telecommunication equipment, systems, and services and shall charge the user any appropriate amount to cover the cost of installation, maintenance, and operation of the telecommunication equipment, system, or service provided.

(C) (1) THE DEPARTMENT SHALL DEVELOP AND REQUIRE BASIC SECURITY REQUIREMENTS TO BE INCLUDED IN A CONTRACT:

(I) IN WHICH A THIRD–PARTY CONTRACTOR WILL HAVE ACCESS TO AND USE STATE TELECOMMUNICATION EQUIPMENT, SYSTEMS, OR SERVICES; OR

(II) BY A UNIT OF STATE GOVERNMENT THAT IS LESS THAN $50,000 FOR SYSTEMS OR DEVICES THAT WILL CONNECT TO STATE TELECOMMUNICATION EQUIPMENT, SYSTEMS, OR SERVICES.

(2) THE SECURITY REQUIREMENTS DEVELOPED UNDER PARAGRAPH (1) OF THIS SUBSECTION SHALL BE CONSISTENT WITH A WIDELY RECOGNIZED SECURITY STANDARD, INCLUDING NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY SP 800–171, ISO27001, OR CYBERSECURITY MATURITY MODEL CERTIFICATION.

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 AND ANY DIVISION OF THE UNIVERSITY SYSTEM OF MARYLAND THAT USES THE NETWORK ESTABLISHED UNDER SUBSECTION (B) OF THIS SECTION SHALL CERTIFY TO THE DEPARTMENT THAT THE UNIT OR DIVISION 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 OF SECURITY MANAGEMENT; 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 OBTAIN AN EXTERNAL VULNERABILITY AND RISK ASSESSMENT AT LEAST ONCE EVERY 2 YEARS.

(2) THE UNIT SHALL REPORT THE RESULTS OF THE ASSESSMENT OBTAINED UNDER PARAGRAPH (1) OF THIS SUBSECTION TO THE OFFICE OF SECURITY MANAGEMENT.

(3) IF THE ASSESSMENT OBTAINED UNDER PARAGRAPH (1) OF THIS SUBSECTION IDENTIFIES NEEDED REMEDIATION, THE UNIT SHALL REPORT TO THE OFFICE OF SECURITY MANAGEMENT AT THE TIME THE REMEDIATION IS COMPLETED.

(C) (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.

(D) (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 OF SECURITY MANAGEMENT; AND

(III) REPORT TO THE OFFICE OF SECURITY MANAGEMENT:

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; **AND**

12. MANAGED CYBERSECURITY SERVICES, AS PROVIDED IN TITLE 3.5, SUBTITLE 3 OF THIS ARTICLE;

Article – State Government

9–2901.

(b) There is a Maryland Cybersecurity Council.

(g) The Attorney General, or the Attorney General's designee, shall chair the Council.

(K) THE CHAIR OF THE COUNCIL SHALL APPOINT A CYBERSECURITY MASTER PLAN SUBCOMMITTEE OF THE COUNCIL TO PROVIDE ADVICE TO THE SECRETARY OF INFORMATION TECHNOLOGY ON THE CREATION OF THE CYBERSECURITY MASTER PLAN UNDER § 3.5–303 OF THE STATE FINANCE AND PROCUREMENT ARTICLE.

[(k)**] (L)** Beginning July 1, 2017, and every 2 years thereafter, the Council shall submit a report of its activities to the General Assembly in accordance with § 2–1257 of this article.

SECTION 3. AND BE IT FURTHER ENACTED, That, as a key enabler of the Department of Information Technology's cybersecurity risk management strategy, on or before December 31, 2022, the Department shall complete the implementation of a

governance, risk, and compliance module across the State Executive Branch enterprise that:

(1) has industry–standard capabilities;

(2) is based on NIST, ISO, or other recognized security frameworks or standards; and

(3) enables the Department to identify, monitor, and manage cybersecurity risk on a continuous basis.

SECTION 4. AND BE IT FURTHER ENACTED, That, on or before December 31, 2023, the State Chief Data Officer appointed under Executive Order 01.01.2021.09 shall:

(1) (i) contract with an independent third party to work with the State Chief Data Officer and units of the Executive Branch of State government to develop a statewide reporting framework based on the Cybersecurity Framework developed by the National Institute of Standards and Technology that:

1. defines a maturity model type assessment methodology; and

2. provides a dashboard for each unit of the Executive Branch of State government to use to report current cybersecurity maturity and improvements to the unit's cybersecurity program as the unit addresses cybersecurity issues, closes gaps, or addresses audit findings, that includes:

A. developing specific recovery time objectives and recovery point objectives;

B. the completion of regular vulnerability scans by the unit;

C. developing standards to describe sensitive information and establishing information sharing and data use agreements;

D. conducting regular backup operations and restoration testing;

E. implementing multifactor authentication practices for remote access and e–mail access;

F. conducting cybersecurity training that reflects best practices and is available to all regular and contractual employees of each unit; and

G. describing the remediation objective time for cybersecurity vulnerabilities based on varying degrees of severity of the vulnerability; and

(ii) run a baseline cybersecurity assessment of all units of State government under the reporting framework established under item (i) of this subsection to establish an initial dashboard for units to report cybersecurity status and establish a priority of budget requests to close identified cybersecurity gaps; and

(2) report recommendations 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 a monitoring program to ensure that all funds allocated to cybersecurity improvements are used efficiently and impact the cybersecurity assessment of units, as measured using the dashboard developed under item (1) of this section.

SECTION 5. AND BE IT FURTHER ENACTED, That, on the effective date of this Act, the following shall be transferred to the Department of Information Technology:

(1) all appropriations, including State and federal funds, held by a unit of the Executive Branch of State government for the purpose of information technology operations or cybersecurity for the unit on the effective date of this Act; and

(2) all books and records (including electronic records), real and personal property, equipment, fixtures, assets, liabilities, obligations, credits, rights, and privileges held by a unit of the Executive Branch of State government for the purpose of information technology operations or cybersecurity for the unit on the effective date of this Act.

SECTION 6. AND BE IT FURTHER ENACTED, That all employees of a unit of the Executive Branch of State government who are assigned more than 50% of the time to a function related to information technology operations or cybersecurity for the unit on the effective date of this Act shall, on the effective date of this Act, report to the Secretary of Information Technology or the Secretary's designee.

SECTION 7. AND BE IT FURTHER ENACTED, That any transaction affected by the transfer of oversight of information technology operations or cybersecurity of a unit of the Executive Branch of State government and validly entered into before the effective date of this Act, and every right, duty, or interest flowing from it, remains valid after the effective date of this Act and may be terminated, completed, consummated, or enforced under the law.

SECTION 8. AND BE IT FURTHER ENACTED, That all existing laws, regulations, proposed regulations, standards and guidelines, policies, orders and other directives, forms, plans, memberships, contracts, property, investigations, administrative and judicial responsibilities, rights to sue and be sued, and all other duties and responsibilities associated with information technology operations or cybersecurity of a unit of the Executive Branch of State government prior to the effective date of this Act shall continue and, as appropriate, are legal and binding on the Department of Information Technology until completed, withdrawn, canceled, modified, or otherwise changed under the law.

SECTION 9. AND BE IT FURTHER ENACTED, That this Act shall take effect October 1, 2022.