HOUSE BILL 1202

E4, P1 *EMERGENCY BILL* (2lr1778)
ENROLLED BILL

— Health and Government Operations/Education, Health, and Environmental Affairs —

Introduced by **Delegates P. Young, Kerr, Feldmark, Bartlett, Kelly, Kipke, Ebersole, Hornberger, ~~and McIntosh~~ McIntosh, Bagnall, Bhandari, Carr, Chisholm, Cullison, Hill, Johnson, Kaiser, Landis, R. Lewis, Morgan, Pena–Melnyk, Pendergrass, Reilly, Rosenberg, Saab, Sample–Hughes, Szeliga, and K. Young**

Read and Examined by Proofreaders:

_____
Proofreader.

_____
Proofreader.

Sealed with the Great Seal and presented to the Governor, for his approval this _____ day of _____ at _____ o'clock, _____M.

_____
Speaker.

CHAPTER _____

AN ACT concerning

Local Government Cybersecurity – Coordination and Operations
(Local Cybersecurity Support Act of 2022)

FOR the purpose of establishing the Cyber Preparedness Unit in the Maryland Department of Emergency Management; establishing certain responsibilities of the Unit; requiring ~~certain local entities~~ local governments to report certain cybersecurity incidents in a certain manner and under certain circumstances; requiring the ~~Maryland Joint~~ *State Security* Operations Center to notify appropriate agencies of a cybersecurity incident in a certain manner; ~~establishing the Cybersecurity Fusion Center in the Maryland Department of Emergency Management; establishing~~

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.
Italics indicate opposite chamber/conference committee amendments.

~~certain responsibilities of the Fusion Center; establishing the Local Cybersecurity Support Fund, the purposes of the Fund, and certain eligibility requirements to receive assistance from the Fund;~~ establishing the Office of Security Management within the Department of Information Technology and certain Office positions; establishing certain responsibilities and authority of the Office; requiring ~~each unit of the Legislative or Judicial Branch of State government,~~ each unit of local government, and any local agencies that use a certain network to certify certain compliance to the Department of Information Technology ~~on or before a certain date each year~~ *in a certain manner*; ~~requiring certain local entities to submit a certain report to the Office on or before a certain date each year;~~ 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; *establishing the Information Sharing and Analysis Center in the Department of Information Technology; establishing certain responsibilities for the Center;* requiring the State Chief Information Security Officer and the Secretary of Emergency Management to conduct a certain review, make recommendations, establish certain guidance, and submit a certain report on or before a certain date; requiring the State Chief Information Security Officer to commission a certain feasibility study and report recommendations on or before a certain date; requiring the Governor to include an appropriation in a certain annual budget to cover the cost of the feasibility study; *authorizing funds to be transferred by budget amendment from the Dedicated Purpose Account in a certain fiscal year to implement the Act;* and generally relating to local government cybersecurity coordination and operations.

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 – Public Safety
Section 14–103
Annotated Code of Maryland
(2018 Replacement Volume and 2021 Supplement)

BY adding to
Article – Public Safety
Section 14–104.1
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–04 to be under the new subtitle "Subtitle 2A. Office of Security Management"; and *3.5–315,* 3.5–405*, and 4–308* ~~and 6–226(a)(2)(ii)146.~~
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(c)(2)(ii)2., 3.5–307(a)(2), 3.5–309(c)(2), (i)(3), and (l)(1)(i), 3.5–311(a)(2)(i), and 3.5–404

Annotated Code of Maryland
(2021 Replacement Volume)
(As enacted by Section 1 of this Act)

~~BY repealing and reenacting, without amendments,~~
~~Article – State Finance and Procurement~~
~~Section 6–226(a)(2)(i)~~
~~Annotated Code of Maryland~~
~~(2021 Replacement Volume)~~

~~BY repealing and reenacting, with amendments,~~
~~Article – State Finance and Procurement~~
~~Section 6–226(a)(2)(ii)144. and 145. and 12–107(b)(2)(i)10. and 11.~~
~~Annotated Code of Maryland~~
~~(2021 Replacement Volume)~~

BY repealing and reenacting, with amendments,
Article – State Government
Section 2–1224(f)
Annotated Code of Maryland
(2021 Replacement Volume)

BY adding to
Article – State Government
Section 2–1224(i)
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 – Public Safety

14–103.

(a) There is a Maryland Department of Emergency Management established as a principal department of the Executive Branch of State government.

(b) The Department has primary responsibility and authority for developing emergency management policies and is responsible for coordinating disaster risk reduction, consequence management, and disaster recovery activities.

(c) The Department may act to:

(1) reduce the disaster risk and vulnerability of persons and property located in the State;

(2) develop and coordinate emergency planning and preparedness; and

(3) coordinate emergency management activities and operations:

(i) relating to an emergency that involves two or more State agencies;

(ii) between State agencies and political subdivisions;

(iii) with local governments;

(iv) with agencies of the federal government and other states; and

(v) with private and nonprofit entities.

14–104.1.

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

~~**(2) "FUND" MEANS THE LOCAL CYBERSECURITY SUPPORT FUND.**~~

~~**(3) "FUSION CENTER" MEANS THE CYBERSECURITY FUSION CENTER.**~~

~~**(4)**~~ **(2) "LOCAL GOVERNMENT" INCLUDES LOCAL SCHOOL SYSTEMS, LOCAL SCHOOL BOARDS, AND LOCAL HEALTH DEPARTMENTS.**

~~**(5)**~~ **(3) "UNIT" MEANS THE CYBER PREPAREDNESS UNIT.**

(B) (1) THERE IS A CYBER PREPAREDNESS UNIT IN THE DEPARTMENT.

(2) IN COORDINATION WITH THE STATE CHIEF INFORMATION SECURITY OFFICER, THE UNIT SHALL:

(I) SUPPORT LOCAL GOVERNMENTS IN DEVELOPING A VULNERABILITY ASSESSMENT AND CYBER ASSESSMENT ~~**THROUGH THE MARYLAND NATIONAL GUARD'S INNOVATIVE READINESS TRAINING PROGRAM OR THE U.S. DEPARTMENT OF HOMELAND SECURITY CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY**~~**, INCLUDING PROVIDING LOCAL GOVERNMENTS WITH THE RESOURCES AND INFORMATION ON BEST PRACTICES TO COMPLETE THE ASSESSMENTS;**

(II) DEVELOP AND REGULARLY UPDATE AN ONLINE DATABASE OF CYBERSECURITY TRAINING RESOURCES FOR LOCAL GOVERNMENT PERSONNEL, INCLUDING TECHNICAL TRAINING RESOURCES, CYBERSECURITY CONTINUITY OF OPERATIONS TEMPLATES, CONSEQUENCE MANAGEMENT PLANS, AND TRAININGS ON MALWARE AND RANSOMWARE DETECTION;

~~(III) ESTABLISH AND PROVIDE STAFF FOR A STATEWIDE HELPLINE TO PROVIDE REAL-TIME EMERGENCY ASSISTANCE AND RESOURCE INFORMATION TO ANY LOCAL GOVERNMENT THAT HAS EXPERIENCED A CYBER INCIDENT OR ATTACK;~~

~~(IV)~~ *(III)* **ASSIST LOCAL GOVERNMENTS IN:**

1. THE DEVELOPMENT OF CYBERSECURITY PREPAREDNESS AND RESPONSE PLANS; ~~**AND**~~

2. IMPLEMENTING BEST PRACTICES AND GUIDANCE DEVELOPED BY THE STATE CHIEF INFORMATION SECURITY OFFICER; ***AND***

3. IDENTIFYING AND ACQUIRING RESOURCES TO COMPLETE APPROPRIATE CYBERSECURITY VULNERABILITY ASSESSMENTS;

~~(V)~~ *(IV)* **CONNECT LOCAL GOVERNMENTS TO APPROPRIATE RESOURCES FOR ANY OTHER PURPOSE RELATED TO CYBERSECURITY PREPAREDNESS AND RESPONSE;**

~~(VI) DEVELOP APPROPRIATE REPORTS ON LOCAL CYBERSECURITY PREPAREDNESS;~~

~~(VII)~~ *(V)* **AS NECESSARY AND IN COORDINATION WITH THE NATIONAL GUARD, LOCAL EMERGENCY MANAGERS, AND OTHER STATE AND LOCAL ENTITIES, CONDUCT REGIONAL CYBERSECURITY PREPAREDNESS EXERCISES; AND**

~~(VIII)~~ *(VI)* **ESTABLISH REGIONAL ASSISTANCE GROUPS TO DELIVER AND COORDINATE SUPPORT SERVICES TO LOCAL GOVERNMENTS, AGENCIES, OR REGIONS.**

(3) THE UNIT SHALL SUPPORT THE OFFICE OF SECURITY MANAGEMENT IN THE DEPARTMENT OF INFORMATION TECHNOLOGY DURING EMERGENCY RESPONSE EFFORTS.

(C) (1) EACH LOCAL GOVERNMENT SHALL REPORT A CYBERSECURITY INCIDENT, INCLUDING AN ATTACK ON A STATE SYSTEM BEING USED BY THE LOCAL GOVERNMENT~~**, TO TO THE APPROPRIATE LOCAL EMERGENCY MANAGER, THE SECURITY OPERATIONS CENTER IN THE DEPARTMENT OF INFORMATION TECHNOLOGY, AND THE MARYLAND JOINT OPERATIONS CENTER IN THE DEPARTMENT**~~***, TO THE APPROPRIATE LOCAL EMERGENCY MANAGER AND THE STATE SECURITY OPERATIONS CENTER IN THE DEPARTMENT OF INFORMATION TECHNOLOGY*** **IN ACCORDANCE WITH PARAGRAPH (2) OF THIS SUBSECTION.**

(2) FOR THE REPORTING OF CYBERSECURITY INCIDENTS UNDER PARAGRAPH (1) OF THIS SUBSECTION, THE ~~DEPARTMENT~~ 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.

(3) THE ~~MARYLAND JOINT OPERATIONS CENTER~~ *STATE SECURITY OPERATIONS CENTER* SHALL IMMEDIATELY NOTIFY APPROPRIATE AGENCIES OF A CYBERSECURITY INCIDENT REPORTED UNDER THIS SUBSECTION THROUGH THE STATE SECURITY OPERATIONS CENTER.

(D) (1) FIVE POSITION IDENTIFICATION NUMBERS (PINS) SHALL BE CREATED FOR THE PURPOSE OF HIRING STAFF TO CONDUCT THE DUTIES OF THE MARYLAND DEPARTMENT OF EMERGENCY MANAGEMENT CYBERSECURITY PREPAREDNESS UNIT.

(2) FOR FISCAL YEAR 2024 AND EACH FISCAL YEAR THEREAFTER, THE GOVERNOR SHALL INCLUDE IN THE ANNUAL BUDGET BILL AN APPROPRIATION OF AT LEAST:

(I) $220,335 FOR 3 PINS FOR ADMINISTRATOR III POSITIONS; AND

(II) $137,643 FOR 2 PINS FOR ADMINISTRATOR II POSITIONS.

~~**(D) (1) THERE IS A CYBERSECURITY FUSION CENTER IN THE DEPARTMENT.**~~

~~**(2) THE FUSION CENTER SHALL:**~~

~~**(I) COORDINATE INFORMATION ON CYBERSECURITY BY SERVING AS A CENTRAL LOCATION FOR INFORMATION SHARING ACROSS STATE AND LOCAL GOVERNMENT, FEDERAL GOVERNMENT PARTNERS, AND PRIVATE ENTITIES;**~~

~~**(II) WITH THE OFFICE OF SECURITY MANAGEMENT IN THE DEPARTMENT OF INFORMATION TECHNOLOGY, SUPPORT CYBERSECURITY COORDINATION BETWEEN LOCAL UNITS OF GOVERNMENT THROUGH EXISTING LOCAL GOVERNMENT STAKEHOLDER ORGANIZATIONS;**~~

~~(III) PROVIDE SUPPORT TO THE STATE CHIEF INFORMATION SECURITY OFFICER AND THE UNIT DURING CYBERSECURITY INCIDENTS THAT AFFECT STATE AND LOCAL GOVERNMENTS;~~

~~(IV) SUPPORT RISK–BASED PLANNING FOR THE USE OF FEDERAL RESOURCES; AND~~

~~(V) CONDUCT ANALYSIS OF CYBERSECURITY INCIDENTS.~~

~~(E) (1) THERE IS A LOCAL CYBERSECURITY SUPPORT FUND.~~

~~(2) THE PURPOSE OF THE FUND IS TO:~~

~~(I) PROVIDE FINANCIAL ASSISTANCE TO LOCAL GOVERNMENTS TO IMPROVE CYBERSECURITY PREPAREDNESS, INCLUDING:~~

~~1. UPDATING CURRENT DEVICES AND NETWORKS WITH THE MOST UP–TO–DATE CYBERSECURITY PROTECTIONS;~~

~~2. SUPPORTING THE PURCHASE OF NEW HARDWARE, SOFTWARE, DEVICES, AND FIREWALLS TO IMPROVE CYBERSECURITY PREPAREDNESS;~~

~~3. RECRUITING AND HIRING INFORMATION TECHNOLOGY STAFF FOCUSED ON CYBERSECURITY; AND~~

~~4. PAYING OUTSIDE VENDORS FOR CYBERSECURITY STAFF TRAINING; AND~~

~~(II) ASSIST LOCAL GOVERNMENTS APPLYING FOR FEDERAL CYBERSECURITY PREPAREDNESS GRANTS.~~

~~(3) THE SECRETARY SHALL ADMINISTER THE FUND.~~

~~(4) (I) THE FUND IS A SPECIAL, NONLAPSING FUND THAT IS NOT SUBJECT TO § 7–302 OF THE STATE FINANCE AND PROCUREMENT ARTICLE.~~

~~(II) THE STATE TREASURER SHALL HOLD THE FUND SEPARATELY, AND THE COMPTROLLER SHALL ACCOUNT FOR THE FUND.~~

~~(5) THE FUND CONSISTS OF:~~

~~(I) MONEY APPROPRIATED IN THE STATE BUDGET TO THE FUND;~~

~~(II) INTEREST EARNINGS; AND~~

~~(III) ANY OTHER MONEY FROM ANY OTHER SOURCE ACCEPTED FOR THE BENEFIT OF THE FUND.~~

~~(6) THE FUND MAY BE USED ONLY:~~

~~(I) TO PROVIDE FINANCIAL ASSISTANCE TO LOCAL GOVERNMENTS TO IMPROVE CYBERSECURITY PREPAREDNESS, INCLUDING:~~

~~1. UPDATING CURRENT DEVICES AND NETWORKS WITH THE MOST UP–TO–DATE CYBERSECURITY PROTECTIONS;~~

~~2. SUPPORTING THE PURCHASE OF NEW HARDWARE, SOFTWARE, DEVICES, AND FIREWALLS TO IMPROVE CYBERSECURITY PREPAREDNESS;~~

~~3. RECRUITING AND HIRING INFORMATION TECHNOLOGY STAFF FOCUSED ON CYBERSECURITY; AND~~

~~4. PAYING OUTSIDE VENDORS FOR CYBERSECURITY STAFF TRAINING;~~

~~(II) TO ASSIST LOCAL GOVERNMENTS APPLYING FOR FEDERAL CYBERSECURITY PREPAREDNESS GRANTS; AND~~

~~(III) FOR ADMINISTRATIVE EXPENSES ASSOCIATED WITH PROVIDING THE ASSISTANCE DESCRIBED UNDER ITEM (I) OF THIS PARAGRAPH.~~

~~(7) (I) THE STATE TREASURER SHALL INVEST THE MONEY OF THE FUND IN THE SAME MANNER AS OTHER STATE MONEY MAY BE INVESTED.~~

~~(II) ANY INTEREST EARNINGS OF THE FUND SHALL BE CREDITED TO THE FUND.~~

~~(8) EXPENDITURES FROM THE FUND MAY BE MADE ONLY IN ACCORDANCE WITH THE STATE BUDGET.~~

~~(F) TO BE ELIGIBLE TO RECEIVE ASSISTANCE FROM THE FUND, EACH LOCAL GOVERNMENT THAT USES THE NETWORK ESTABLISHED IN ACCORDANCE WITH § 3.5–404 OF THE STATE FINANCE AND PROCUREMENT ARTICLE SHALL MEET~~

~~THE REQUIREMENTS OF §§ 3.5–404(D) AND 3.5–405 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.

IN THIS SUBTITLE, "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) AN INDIVIDUAL APPOINTED AS THE STATE CHIEF INFORMATION SECURITY OFFICER UNDER SUBSECTION (B) OF THIS SECTION SHALL:

(1) AT A MINIMUM, HOLD A BACHELOR'S DEGREE;

(2) HOLD APPROPRIATE INFORMATION TECHNOLOGY OR CYBERSECURITY CERTIFICATIONS;

(3) HAVE EXPERIENCE:

(I) IDENTIFYING, IMPLEMENTING, ~~AND~~ *OR* ASSESSING SECURITY CONTROLS;

(II) IN INFRASTRUCTURE, SYSTEMS ENGINEERING, ~~AND~~ *OR* CYBERSECURITY;

(III) MANAGING HIGHLY TECHNICAL SECURITY, SECURITY OPERATIONS CENTERS, AND INCIDENT RESPONSE TEAMS IN A COMPLEX CLOUD ENVIRONMENT AND SUPPORTING MULTIPLE SITES; AND

(IV) WORKING WITH COMMON INFORMATION SECURITY MANAGEMENT FRAMEWORKS;

(4) HAVE EXTENSIVE KNOWLEDGE OF INFORMATION TECHNOLOGY AND CYBERSECURITY FIELD CONCEPTS, BEST PRACTICES, AND PROCEDURES, WITH AN UNDERSTANDING OF EXISTING ENTERPRISE CAPABILITIES AND LIMITATIONS TO ENSURE THE SECURE INTEGRATION AND OPERATION OF SECURITY NETWORKS AND SYSTEMS; AND

(5) HAVE KNOWLEDGE OF CURRENT SECURITY REGULATIONS ~~AND LEGISLATIVE CONTENT~~.

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

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

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

3.5–2A–04.

(A) (1) THE OFFICE IS RESPONSIBLE FOR:

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

~~(2)~~ (II) ~~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.; AND~~ *AND*

~~(III)~~ *(II)* ~~SUPPORTING~~ *COORDINATING WITH* THE MARYLAND DEPARTMENT OF EMERGENCY MANAGEMENT CYBER PREPAREDNESS UNIT DURING EMERGENCY RESPONSE EFFORTS.

(2) THE OFFICE IS NOT RESPONSIBLE FOR THE INFORMATION TECHNOLOGY INSTALLATION AND MAINTENANCE OPERATIONS NORMALLY CONDUCTED BY A UNIT OF STATE GOVERNMENT, A UNIT OF LOCAL GOVERNMENT, A LOCAL SCHOOL BOARD, A LOCAL SCHOOL SYSTEM, OR A LOCAL HEALTH DEPARTMENT.

(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;~~ *ANY INFORMATION SYSTEMS, DETERMINE AND DIRECT OR TAKE ACTIONS NECESSARY TO CORRECT OR REMEDIATE THE VULNERABILITIES OR DEFICIENCIES, WHICH MAY INCLUDE REQUIRING THE INFORMATION SYSTEM TO BE DISCONNECTED;*

(7) IF THE STATE CHIEF INFORMATION SECURITY OFFICER DETERMINES THAT THERE IS A CYBERSECURITY THREAT CAUSED BY AN ENTITY CONNECTED TO THE NETWORK ESTABLISHED UNDER § 3.5–404 OF THIS TITLE THAT INTRODUCES A SERIOUS RISK TO ENTITIES CONNECTED TO THE NETWORK OR TO THE STATE, TAKE OR DIRECT ACTIONS REQUIRED TO MITIGATE THE THREAT;

~~(7)~~ *(8)* MANAGE SECURITY AWARENESS TRAINING FOR ALL APPROPRIATE EMPLOYEES OF UNITS OF STATE GOVERNMENT;

~~(8)~~ *(9)* ASSIST IN THE DEVELOPMENT OF DATA MANAGEMENT, DATA GOVERNANCE, AND DATA SPECIFICATION STANDARDS TO PROMOTE STANDARDIZATION AND REDUCE RISK;

~~(9)~~ *(10)* 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)~~ *(11)* 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)~~ *(12)* **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 SUPPORT LOCAL GOVERNMENTS DEVELOPING 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 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; *AND*

(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.

~~(C)~~ (E) *(1)* 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 SENATE EDUCATION, HEALTH, AND ENVIRONMENTAL AFFAIRS COMMITTEE, THE HOUSE APPROPRIATIONS COMMITTEE, THE HOUSE HEALTH AND GOVERNMENT OPERATIONS 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)~~ *(I)* THE ACTIVITIES AND ACCOMPLISHMENTS OF THE OFFICE DURING THE PREVIOUS 12 MONTHS AT THE STATE AND LOCAL LEVELS; AND

~~(2)~~ *(II)* 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)~~ *1.* A SUMMARY OF THE ISSUES IDENTIFIED BY THE CYBERSECURITY PREPAREDNESS ASSESSMENTS CONDUCTED THAT YEAR;

~~(II)~~ *2.* THE STATUS OF VULNERABILITY ASSESSMENTS OF ALL UNITS OF STATE GOVERNMENT AND A TIMELINE FOR COMPLETION AND COST TO REMEDIATE ANY VULNERABILITIES EXPOSED;

~~(III)~~ *3.* 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)~~ *4.* 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)~~ *5.* EFFORTS TO SECURE FINANCIAL SUPPORT FOR CYBER RISK MITIGATION FROM FEDERAL OR OTHER NON–STATE RESOURCES;

~~(VI)~~ *6.* 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)~~ *7.* ANY ADDITIONAL RECOMMENDATIONS FOR IMPROVING STATE AND LOCAL CYBERSECURITY PREPAREDNESS.

(2) A REPORT SUBMITTED UNDER THIS SUBSECTION MAY NOT CONTAIN INFORMATION THAT REVEALS CYBERSECURITY VULNERABILITIES AND RISKS IN THE STATE.

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**] §§ 3.5–307(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, St. Mary's College of Maryland, and Baltimore City Community College.

3.5–303.

(c) 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 ***OR CYBERSECURITY 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) (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

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;

3.5–315.

(A) THERE IS AN INFORMATION SHARING AND ANALYSIS CENTER IN THE DEPARTMENT.

(B) THE INFORMATION SHARING AND ANALYSIS CENTER SHALL:

(1) COORDINATE INFORMATION ON CYBERSECURITY BY SERVING AS A CENTRAL LOCATION FOR INFORMATION SHARING ACROSS STATE AND LOCAL GOVERNMENT, FEDERAL GOVERNMENT PARTNERS, AND PRIVATE ENTITIES;

(2) WITH THE OFFICE OF SECURITY MANAGEMENT, SUPPORT CYBERSECURITY COORDINATION BETWEEN LOCAL UNITS OF GOVERNMENT THROUGH EXISTING LOCAL GOVERNMENT STAKEHOLDER ORGANIZATIONS;

(3) PROVIDE SUPPORT TO THE STATE CHIEF INFORMATION SECURITY OFFICER AND THE CYBER PREPAREDNESS UNIT, IN THE MARYLAND DEPARTMENT OF EMERGENCY MANAGEMENT, DURING CYBERSECURITY INCIDENTS THAT AFFECT STATE AND LOCAL GOVERNMENTS;

(4) SUPPORT RISK–BASED PLANNING FOR THE USE OF FEDERAL RESOURCES; AND

(5) CONDUCT ANALYSES OF CYBERSECURITY INCIDENTS.

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~~ *IN A MANNER AND FREQUENCY ESTABLISHED IN REGULATIONS ADOPTED BY THE DEPARTMENT*, ~~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) THIS SECTION DOES NOT APPLY TO MUNICIPAL GOVERNMENTS.

(B) ~~ON OR BEFORE DECEMBER 1 EACH YEAR~~ *IN A MANNER AND FREQUENCY ESTABLISHED IN REGULATIONS ADOPTED BY THE DEPARTMENT*, EACH COUNTY GOVERNMENT, LOCAL SCHOOL SYSTEM, AND LOCAL HEALTH DEPARTMENT SHALL~~:~~

~~(1)~~ IN CONSULTATION WITH THE LOCAL EMERGENCY MANAGER, CREATE OR UPDATE A CYBERSECURITY PREPAREDNESS AND RESPONSE PLAN *AND COMPLETE A CYBERSECURITY PREPAREDNESS ASSESSMENT* ~~AND SUBMIT THE PLAN TO THE OFFICE OF SECURITY MANAGEMENT FOR APPROVAL;~~.

~~(2) COMPLETE A CYBERSECURITY PREPAREDNESS ASSESSMENT AND REPORT THE RESULTS TO THE OFFICE IN ACCORDANCE WITH GUIDELINES DEVELOPED BY THE OFFICE; AND~~

~~(3) REPORT TO THE OFFICE:~~

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

~~(II) THE ENTITY'S CYBERSECURITY BUDGET AND OVERALL INFORMATION TECHNOLOGY BUDGET;~~

~~(III) THE NUMBER OF EMPLOYEES WHO HAVE RECEIVED CYBERSECURITY TRAINING; AND~~

~~(IV) THE TOTAL NUMBER OF EMPLOYEES WITH ACCESS TO THE ENTITY'S COMPUTER SYSTEMS AND DATABASES.~~

~~(C) THE ASSESSMENT REQUIRED UNDER PARAGRAPH (B)(2) OF THIS SECTION MAY, IN ACCORDANCE WITH THE PREFERENCE OF EACH COUNTY GOVERNMENT, BE PERFORMED BY THE DEPARTMENT OR A VENDOR AUTHORIZED BY THE DEPARTMENT.~~

4–308.

(A) THE DEPARTMENT MAY ESTABLISH A PROGRAM THAT LEVERAGES STATE PURCHASING POWER TO OFFER FAVORABLE RATES TO UNITS OF LOCAL GOVERNMENT TO PROCURE INFORMATION TECHNOLOGY OR CYBERSECURITY SERVICES FROM CONTRACTORS.

(B) A UNIT OF LOCAL GOVERNMENT MAY NOT BE REQUIRED TO PARTICIPATE IN A PROGRAM ESTABLISHED UNDER SUBSECTION (A) OF THIS SECTION.

~~6–226.~~

~~(a) (2) (i) Notwithstanding any other provision of law, and unless inconsistent with a federal law, grant agreement, or other federal requirement or with the terms of a gift or settlement agreement, net interest on all State money allocated by the State Treasurer under this section to special funds or accounts, and otherwise entitled to receive interest earnings, as accounted for by the Comptroller, shall accrue to the General Fund of the State.~~

~~(ii) The provisions of subparagraph (i) of this paragraph do not apply to the following funds:~~

~~144. the Health Equity Resource Community Reserve Fund;~~ **[**~~and~~**]**

~~145. the Access to Counsel in Evictions Special Fund; AND~~

~~146. THE LOCAL CYBERSECURITY SUPPORT FUND.~~

~~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;~~

Article – State Government

2–1224.

(f) **[**After**]** **EXCEPT AS PROVIDED IN SUBSECTION (I) OF THIS SECTION, AFTER** the expiration of any period that the Joint Audit and Evaluation Committee specifies, a report of the Legislative Auditor is available to the public under Title 4, Subtitles 1 through 5 of the General Provisions Article.

(I) A REPORT AUDITING A UNIT OF STATE OR LOCAL GOVERNMENT SHALL HAVE ANY CYBERSECURITY FINDINGS REDACTED IN A MANNER CONSISTENT WITH AUDITING BEST PRACTICES BEFORE THE REPORT IS MADE AVAILABLE TO THE PUBLIC.

SECTION 3. AND BE IT FURTHER ENACTED, That, on or before December 1, 2022, the State Chief Information Security Officer and the Secretary of Emergency Management shall:

(1) review the State budget for efficiency and effectiveness of funding and resources to ensure that the State is equipped to respond to a cybersecurity attack;

(2) make recommendations for any changes to the budget needed to accomplish the goals under item (1) of this section;

(3) establish guidance for units of State government on use and access to State funding related to cybersecurity preparedness; and

(4) report any recommendations and guidance to the Governor and, in accordance with § 2–1257 of the State Government Article, the General Assembly.

SECTION 4. AND BE IT FURTHER ENACTED, That:

(a) On or before December 1, 2023, the State Chief Information Security Officer shall:

(1) commission a feasibility study on expanding the operations of the State Security Operations Center operated by the Department of Information Technology to include cybersecurity monitoring and alert services for units of local government; and

(2) report any recommendations to the Governor and, in accordance with § 2–1257 of the State Government Article, the General Assembly.

(b) For fiscal year 2024, the Governor shall include an appropriation in the annual budget to cover the cost of the feasibility study required under subsection (a) of this section.

~~SECTION 5. AND BE IT FURTHER ENACTED, That this Act shall take effect July 1, 2022.~~

SECTION 5. AND BE IT FURTHER ENACTED, That:

(a) (1) On or before June 30, 2023, each unit of local government shall certify to the Office of Security Management compliance with State minimum cybersecurity standards established by the Department of Information Technology.

(2) Certification shall be reviewed by independent auditors, and any findings must be remediated.

(b) If a unit of local government has not remediated any findings pertaining to State cybersecurity standards found by the independent audit required under subsection (1) of this section by July 1, 2024, the Office of Security Management shall ~~assume responsibility for a unit's cybersecurity through a shared service agreement, administrative privileges, or access to Network Maryland notwithstanding any federal law or regulation that forbids the Office of Security Management from managing a specific system.~~ provide guidance for the unit to achieve compliance with the cybersecurity standards.

SECTION 6. AND BE IT FURTHER ENACTED, That for fiscal year 2023, funds from the Dedicated Purpose Account may be transferred by budget amendment in accordance with § 7–310 of the State Finance and Procurement Article to implement this Act.

SECTION 7. AND BE IT FURTHER ENACTED, That:

(a) On or before ~~June~~ October 1, 2022, the State Chief Information Security Officer shall establish guidelines to determine when a cybersecurity incident shall be disclosed to the public.

(b) On or before November 1, 2022, the State Chief Information Security Officer shall submit a report on the guidelines established under subsection (a) of this section to the Governor and, in accordance with § 2–1257 of the State Government Article, the House Health and Government Operations Committee and the Senate Education, Health, and Environmental Affairs Committee.

SECTION 8. AND BE IT FURTHER ENACTED, That this Act is an emergency measure, is necessary for the immediate preservation of the public health or safety, has been passed by a yea and nay vote supported by three–fifths of all the members elected to each of the two Houses of the General Assembly, and shall take effect from the date it is enacted.