

SENATE BILL 754

S2, E4, P1

EMERGENCY BILL

2lr1504
CF HB 1202

By: ~~Senator Hester~~ Senators Hester, Hershey, Jennings, Jackson, Rosapepe, Lee, and Watson

Introduced and read first time: February 7, 2022

Assigned to: Education, Health, and Environmental Affairs

Committee Report: Favorable with amendments

Senate action: Adopted with floor amendments

Read second time: March 27, 2022

CHAPTER _____

1 AN ACT concerning

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

4 FOR the purpose of establishing the Cyber Preparedness Unit in the Maryland Department
5 of Emergency Management; establishing certain responsibilities of the Unit;
6 requiring ~~certain local entities~~ local governments to report certain cybersecurity
7 incidents in a certain manner and under certain circumstances; requiring the
8 ~~Maryland Joint Operations Center~~ State Security Operations Center to notify
9 appropriate agencies of a cybersecurity incident in a certain manner; ~~establishing~~
10 ~~the Cybersecurity Fusion Center in the Maryland Department of Emergency~~
11 ~~Management; establishing certain responsibilities of the Fusion Center; establishing~~
12 ~~the Local Cybersecurity Support Fund, the purposes of the Fund, and certain~~
13 ~~eligibility requirements to receive assistance from the Fund; establishing the Office~~
14 of Security Management within the Department of Information Technology and
15 certain Office positions; establishing certain responsibilities and authority of the
16 Office; requiring ~~each unit of the Legislative or Judicial Branch of State government,~~
17 each unit of local government, and any local agencies that use a certain network to
18 certify certain compliance to the Department of Information Technology ~~on or before~~
19 ~~a certain date each year; requiring certain local entities to submit a certain report to~~
20 ~~the Office on or before a certain date each year; in a certain manner; requiring the~~
21 ~~Office to submit a certain report to the Governor and certain committees of the~~
22 ~~General Assembly on or before a certain date each year; requiring the Office to~~
23 ~~submit a certain report to the Governor and certain committees of the General~~
24 Assembly on or before a certain date each year; establishing the Information Sharing

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.



1 and Analysis Center in the Department of Information Technology; establishing
2 certain responsibilities for the Center; requiring the State Chief Information
3 Security Officer and the Secretary of Emergency Management to conduct a certain
4 review, make recommendations, establish certain guidance, and submit a certain
5 report on or before a certain date; requiring the State Chief Information Security
6 Officer to commission a certain feasibility study and report recommendations on or
7 before a certain date; requiring the Governor to include an appropriation in a certain
8 annual budget to cover the cost of the feasibility study; authorizing funds to be
9 transferred by budget amendment from the Dedicated Purpose Account in a certain
10 fiscal year to implement the Act; and generally relating to local government
11 cybersecurity coordination and operations.

12 BY renumbering

13 Article – State Finance and Procurement
14 Section 3A–101 through 3A–702, respectively, and the title “Title 3A. Department of
15 Information Technology”
16 to be Section 3.5–101 through 3.5–702, respectively, and the title “Title 3.5.
17 Department of Information Technology”
18 Annotated Code of Maryland
19 (2021 Replacement Volume)

20 BY repealing and reenacting, with amendments,

21 Article – Criminal Procedure
22 Section 10–221(b)
23 Annotated Code of Maryland
24 (2018 Replacement Volume and 2021 Supplement)

25 BY repealing and reenacting, with amendments,

26 Article – Health – General
27 Section 21–2C–03(h)(2)(i)
28 Annotated Code of Maryland
29 (2019 Replacement Volume and 2021 Supplement)

30 BY repealing and reenacting, with amendments,

31 Article – Human Services
32 Section 7–806(a), (b)(1), (c)(1), (d)(1) and (2)(i), and (g)(1)
33 Annotated Code of Maryland
34 (2019 Replacement Volume and 2021 Supplement)

35 BY repealing and reenacting, with amendments,

36 Article – Insurance
37 Section 31–103(a)(2)(i) and (b)(2)
38 Annotated Code of Maryland
39 (2017 Replacement Volume and 2021 Supplement)

40 BY repealing and reenacting, with amendments,

41 Article – Natural Resources

- 1 Section 1–403(c)
 2 Annotated Code of Maryland
 3 (2018 Replacement Volume and 2021 Supplement)
- 4 BY repealing and reenacting, without amendments,
 5 Article – Public Safety
 6 Section 14–103
 7 Annotated Code of Maryland
 8 (2018 Replacement Volume and 2021 Supplement)
- 9 BY adding to
 10 Article – Public Safety
 11 Section 14–104.1
 12 Annotated Code of Maryland
 13 (2018 Replacement Volume and 2021 Supplement)
- 14 BY repealing and reenacting, without amendments,
 15 Article – State Finance and Procurement
 16 Section 3.5–101(a) and (e) and 3.5–301(a)
 17 Annotated Code of Maryland
 18 (2021 Replacement Volume)
 19 (As enacted by Section 1 of this Act)
- 20 BY adding to
 21 Article – State Finance and Procurement
 22 Section 3.5–2A–01 through 3.5–2A–04 to be under the new subtitle “Subtitle 2A.
 23 Office of Security Management”; and 3.5–315, 3.5–405, and 4–308 ~~and~~
 24 ~~6–226(a)(2)(i)146.~~
 25 Annotated Code of Maryland
 26 (2021 Replacement Volume)
- 27 BY repealing and reenacting, with amendments,
 28 Article – State Finance and Procurement
 29 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),
 30 and (l)(1)(i), 3.5–311(a)(2)(i), and 3.5–404
 31 Annotated Code of Maryland
 32 (2021 Replacement Volume)
 33 (As enacted by Section 1 of this Act)
- 34 ~~BY repealing and reenacting, without amendments,~~
 35 ~~Article – State Finance and Procurement~~
 36 ~~Section 6–226(a)(2)(i)~~
 37 ~~Annotated Code of Maryland~~
 38 ~~(2021 Replacement Volume)~~
- 39 ~~BY repealing and reenacting, with amendments,~~
 40 ~~Article – State Finance and Procurement~~

1 ~~Section 6-226(a)(2)(ii)144. and 145. and 12-107(b)(2)(i)10. and 11.~~
 2 ~~Annotated Code of Maryland~~
 3 ~~(2021 Replacement Volume)~~

4 BY repealing and reenacting, with amendments,
 5 Article – State Government
 6 Section 2-1224(f)
 7 Annotated Code of Maryland
 8 (2021 Replacement Volume)

9 BY adding to
 10 Article – State Government
 11 Section 2-1224(i)
 12 Annotated Code of Maryland
 13 (2021 Replacement Volume)

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

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

21 **Article – Criminal Procedure**

22 10-221.

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

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

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

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

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

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

1 (i) accurate and complete; and

2 (ii) collected, reported, and disseminated in accordance with Subtitle
3 1 of this title and this subtitle;

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

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

9 Article – Health – General

10 21–2C–03.

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

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

16 Article – Human Services

17 7–806.

18 (a) (1) Subject to paragraph (2) of this subsection, the programs under §
19 7–804(a) of this subtitle, § 7–902(a) of this title, and [§ 3A–702] § 3.5–702 of the State
20 Finance and Procurement Article shall be funded as provided in the State budget.

21 (2) For fiscal year 2019 and each fiscal year thereafter, the program under
22 [§ 3A–702] § 3.5–702 of the State Finance and Procurement Article shall be funded at an
23 amount that:

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

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

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

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

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

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

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

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

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

12 (d) (1) The Secretary shall annually certify to the Public Service Commission
13 the costs of the programs under § 7-804(a) of this subtitle, § 7-902(a) of this title, and [§
14 3A-702] § 3.5-702 of the State Finance and Procurement Article to be paid by the
15 Universal Service Trust Fund for the following fiscal year.

16 (2) (i) The Public Service Commission shall determine the surcharge
17 for the following fiscal year necessary to fund the programs under § 7-804(a) of this subtitle,
18 § 7-902(a) of this title, and [§ 3A-702] § 3.5-702 of the State Finance and Procurement
19 Article.

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

24 Article - Insurance

25 31-103.

26 (a) The Exchange is subject to:

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

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

31 (b) The Exchange is not subject to:

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

4 **Article – Natural Resources**

5 1–403.

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

9 **Article – Public Safety**

10 14–103.

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

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

16 (c) The Department may act to:

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

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

20 (3) coordinate emergency management activities and operations:

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

23 (ii) between State agencies and political subdivisions;

24 (iii) with local governments;

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

26 (v) with private and nonprofit entities.

27 **14–104.1.**

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

1 ~~(2)~~ ~~“FUND” MEANS THE LOCAL CYBERSECURITY SUPPORT FUND.~~

2 ~~(3)~~ ~~“FUSION CENTER” MEANS THE CYBERSECURITY FUSION~~
3 ~~CENTER.~~

4 ~~(4)~~ (2) “LOCAL GOVERNMENT” INCLUDES LOCAL SCHOOL
5 SYSTEMS, LOCAL SCHOOL BOARDS, AND LOCAL HEALTH DEPARTMENTS.

6 ~~(5)~~ (3) “UNIT” MEANS THE CYBER PREPAREDNESS UNIT.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

23 **(2) FOR THE REPORTING OF CYBERSECURITY INCIDENTS UNDER**
24 **PARAGRAPH (1) OF THIS SUBSECTION, THE ~~DEPARTMENT~~ STATE CHIEF**
25 **INFORMATION SECURITY OFFICER SHALL DETERMINE:**

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

28 **(II) THE MANNER IN WHICH TO REPORT; AND**

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

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

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

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

8 **(I) \$220,335 FOR 3 PINS FOR ADMINISTRATOR III POSITIONS;**
 9 **AND**

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

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

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

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

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

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

24 ~~**(IV) SUPPORT RISK-BASED PLANNING FOR THE USE OF**~~
 25 ~~**FEDERAL RESOURCES; AND**~~

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

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

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

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

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

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

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

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

10 ~~(H) ASSIST LOCAL GOVERNMENTS APPLYING FOR FEDERAL~~
11 ~~CYBERSECURITY PREPAREDNESS GRANTS.~~

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

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

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

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

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

20 ~~(II) INTEREST EARNINGS; AND~~

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

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

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

26 ~~1. UPDATING CURRENT DEVICES AND NETWORKS WITH~~
27 ~~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;~~

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

~~(HH) 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.~~

~~(H) 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.

1 IN THIS SUBTITLE, "OFFICE" MEANS THE OFFICE OF SECURITY
2 MANAGEMENT.

3 3.5-2A-02.

4 THERE IS AN OFFICE OF SECURITY MANAGEMENT WITHIN THE DEPARTMENT.

5 3.5-2A-03.

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

8 (B) THE STATE CHIEF INFORMATION SECURITY OFFICER SHALL:

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

11 (2) SERVE AT THE PLEASURE OF THE GOVERNOR;

12 (3) BE SUPERVISED BY THE SECRETARY; AND

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

15 (C) AN INDIVIDUAL APPOINTED AS THE STATE CHIEF INFORMATION
16 SECURITY OFFICER UNDER SUBSECTION (B) OF THIS SECTION SHALL:

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

18 (2) HOLD APPROPRIATE INFORMATION TECHNOLOGY OR
19 CYBERSECURITY CERTIFICATIONS;

20 (3) HAVE EXPERIENCE:

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

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

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

1 (IV) WORKING WITH COMMON INFORMATION SECURITY
 2 MANAGEMENT FRAMEWORKS;

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

8 (5) HAVE KNOWLEDGE OF CURRENT SECURITY REGULATIONS.

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

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

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

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

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

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

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

29 3.5-2A-04.

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

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

4 ~~(2) THE COORDINATION OF RESOURCES AND EFFORTS TO~~
5 ~~IMPLEMENT CYBERSECURITY BEST PRACTICES AND IMPROVE OVERALL~~
6 ~~CYBERSECURITY PREPAREDNESS AND RESPONSE FOR UNITS OF LOCAL~~
7 ~~GOVERNMENT, LOCAL SCHOOL BOARDS, LOCAL SCHOOL SYSTEMS, AND LOCAL~~
8 ~~HEALTH DEPARTMENTS; AND~~

9 **(II) SUPPORTING THE MARYLAND DEPARTMENT OF**
10 **EMERGENCY MANAGEMENT CYBER PREPAREDNESS UNIT DURING EMERGENCY**
11 **RESPONSE EFFORTS.**

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

17 **(B) THE OFFICE SHALL:**

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

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

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

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

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

30 **(6) IF THE STATE CHIEF INFORMATION SECURITY OFFICER**
31 **DETERMINES THAT THERE ARE SECURITY VULNERABILITIES OR DEFICIENCIES IN**
32 ~~THE IMPLEMENTATION OF THE SECURITY REQUIREMENTS ESTABLISHED UNDER~~
33 ~~ITEM (4) OF THIS SUBSECTION, DETERMINE WHETHER AN INFORMATION SYSTEM~~
34 ~~SHOULD BE ALLOWED TO CONTINUE TO OPERATE OR BE CONNECTED TO THE~~

~~1 NETWORK ESTABLISHED IN ACCORDANCE WITH § 3.5-404 OF THIS TITLE; ANY~~
~~2 INFORMATION SYSTEMS, DETERMINE AND DIRECT OR TAKE ACTIONS NECESSARY TO~~
~~3 CORRECT OR REMEDIATE THE VULNERABILITIES OR DEFICIENCIES, WHICH MAY~~
~~4 INCLUDE REQUIRING THE INFORMATION SYSTEM TO BE DISCONNECTED;~~

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

~~10 (7) (8)~~ MANAGE SECURITY AWARENESS TRAINING FOR ALL
11 APPROPRIATE EMPLOYEES OF UNITS OF STATE GOVERNMENT;

~~12 (8) (9)~~ ASSIST IN THE DEVELOPMENT OF DATA MANAGEMENT,
13 DATA GOVERNANCE, AND DATA SPECIFICATION STANDARDS TO PROMOTE
14 STANDARDIZATION AND REDUCE RISK;

~~15 (9) (10)~~ ASSIST IN THE DEVELOPMENT OF A DIGITAL IDENTITY
16 STANDARD AND SPECIFICATION APPLICABLE TO ALL PARTIES COMMUNICATING,
17 INTERACTING, OR CONDUCTING BUSINESS WITH OR ON BEHALF OF A UNIT OF STATE
18 GOVERNMENT;

~~19 (10) (11)~~ DEVELOP AND MAINTAIN INFORMATION TECHNOLOGY
20 SECURITY POLICY, STANDARDS, AND GUIDANCE DOCUMENTS, CONSISTENT WITH
21 BEST PRACTICES DEVELOPED BY THE NATIONAL INSTITUTE OF STANDARDS AND
22 TECHNOLOGY;

~~23 (11) (12)~~ TO THE EXTENT PRACTICABLE, SEEK, IDENTIFY, AND
24 INFORM RELEVANT STAKEHOLDERS OF ANY AVAILABLE FINANCIAL ASSISTANCE
25 PROVIDED BY THE FEDERAL GOVERNMENT OR NON-STATE ENTITIES TO SUPPORT
26 THE WORK OF THE OFFICE;

~~27 (12) REVIEW AND CERTIFY LOCAL CYBERSECURITY PREPAREDNESS~~
28 ~~AND RESPONSE PLANS;~~

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

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

1 **(C) THE OFFICE, IN COORDINATION WITH THE MARYLAND DEPARTMENT**
2 **OF EMERGENCY MANAGEMENT, SHALL:**

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

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

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

9 **(2) CONNECT LOCAL ENTITIES TO APPROPRIATE RESOURCES FOR**
10 **ANY OTHER PURPOSE RELATED TO CYBERSECURITY PREPAREDNESS AND**
11 **RESPONSE.**

12 **(D) THE OFFICE, IN COORDINATION WITH THE MARYLAND DEPARTMENT**
13 **OF EMERGENCY MANAGEMENT, MAY:**

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

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

20 ~~(C)~~ **(E) (1) ON OR BEFORE DECEMBER 31 EACH YEAR, THE OFFICE**
21 **SHALL REPORT TO THE GOVERNOR AND, IN ACCORDANCE WITH § 2-1257 OF THE**
22 **STATE GOVERNMENT ARTICLE, THE SENATE BUDGET AND TAXATION COMMITTEE,**
23 **THE SENATE EDUCATION, HEALTH, AND ENVIRONMENTAL AFFAIRS COMMITTEE,**
24 **THE HOUSE APPROPRIATIONS COMMITTEE, THE HOUSE HEALTH AND**
25 **GOVERNMENT OPERATIONS COMMITTEE, AND THE JOINT COMMITTEE ON**
26 **CYBERSECURITY, INFORMATION TECHNOLOGY, AND BIOTECHNOLOGY ON THE**
27 **ACTIVITIES OF THE OFFICE AND THE STATE OF CYBERSECURITY PREPAREDNESS IN**
28 **MARYLAND, INCLUDING:**

29 ~~(1)~~ **(I) THE ACTIVITIES AND ACCOMPLISHMENTS OF THE OFFICE**
30 **DURING THE PREVIOUS 12 MONTHS AT THE STATE AND LOCAL LEVELS; AND**

31 ~~(2)~~ **(II) A COMPILATION AND ANALYSIS OF THE DATA FROM THE**
32 **INFORMATION CONTAINED IN THE REPORTS RECEIVED BY THE OFFICE UNDER §**
33 **3.5-405 OF THIS TITLE, INCLUDING:**

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

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

6 ~~(III)~~ 3. RECENT AUDIT FINDINGS OF ALL UNITS OF STATE
7 GOVERNMENT AND OPTIONS TO IMPROVE FINDINGS IN FUTURE AUDITS, INCLUDING
8 RECOMMENDATIONS FOR STAFF, BUDGET, AND TIMING;

9 ~~(IV)~~ 4. ANALYSIS OF THE STATE'S EXPENDITURE ON
10 CYBERSECURITY RELATIVE TO OVERALL INFORMATION TECHNOLOGY SPENDING
11 FOR THE PRIOR 3 YEARS AND RECOMMENDATIONS FOR CHANGES TO THE BUDGET,
12 INCLUDING AMOUNT, PURPOSE, AND TIMING TO IMPROVE STATE AND LOCAL
13 CYBERSECURITY PREPAREDNESS;

14 ~~(V)~~ 5. EFFORTS TO SECURE FINANCIAL SUPPORT FOR
15 CYBER RISK MITIGATION FROM FEDERAL OR OTHER NON-STATE RESOURCES;

16 ~~(VI)~~ 6. KEY PERFORMANCE INDICATORS ON THE
17 CYBERSECURITY STRATEGIES IN THE DEPARTMENT'S INFORMATION TECHNOLOGY
18 MASTER PLAN, INCLUDING TIME, BUDGET, AND STAFF REQUIRED FOR
19 IMPLEMENTATION; AND

20 ~~(VII)~~ 7. ANY ADDITIONAL RECOMMENDATIONS FOR
21 IMPROVING STATE AND LOCAL CYBERSECURITY PREPAREDNESS.

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

25 3.5-301.

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

27 (j) "Nonvisual access" means the ability, through keyboard control, synthesized
28 speech, Braille, or other methods not requiring sight to receive, use, and manipulate
29 information and operate controls necessary to access information technology in accordance
30 with standards adopted under [§ 3A-303(b)] **§ 3.5-303(B)** of this subtitle.

31 3.5-302.

32 (c) Notwithstanding any other provision of law, except as provided in subsection
33 (a) of this section and [§§ 3A-307(a)(2), 3A-308, and 3A-309] **§§ 3.5-307(A)(2), 3.5-308,**

1 **AND 3.5–309** of this subtitle, this subtitle applies to all units of the Executive Branch of
2 State government including public institutions of higher education other than Morgan
3 State University, the University System of Maryland, St. Mary’s College of Maryland, and
4 Baltimore City Community College.

5 3.5–303.

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

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

8 (ii) 2. for information technology procured by a State unit on or
9 after January 1, 2020, enforce the nonvisual access clause developed under [§ 3A–311] §
10 **3.5–311** of this subtitle, including the enforcement of the civil penalty described in [§
11 3A–311(a)(2)(iii)1] **§ 3.5–311(A)(2)(III)1** of this subtitle.

12 3.5–307.

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

17 3.5–309.

18 (c) The Secretary:

19 (2) subject to the provisions of § 2–201 of this article and [§ 3A–307] §
20 **3.5–307** of this subtitle, may receive and accept contributions, grants, or gifts of money or
21 property.

22 (i) The Fund may be used:

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

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

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

32 3.5–311.

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

3 (i) within 18 months after the award of the procurement, the
4 Secretary, or the Secretary's designee, will determine whether the information technology
5 meets the nonvisual access standards adopted in accordance with [§ 3A-303(b)] §
6 **3.5-303(B)** of this subtitle;

7 **3.5-315.**

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

10 **(B) THE INFORMATION SHARING AND ANALYSIS CENTER SHALL:**

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

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

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

21 **(4) SUPPORT RISK-BASED PLANNING FOR THE USE OF FEDERAL**
22 **RESOURCES; AND**

23 **(5) CONDUCT ANALYSES OF CYBERSECURITY INCIDENTS.**

24 **3.5-404.**

25 (a) The General Assembly declares that:

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

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

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

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

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

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

13 (2) The network shall consist of:

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

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

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

21 **(D) ~~ON OR BEFORE DECEMBER 1 EACH YEAR~~ IN A MANNER AND FREQUENCY**
22 **~~ESTABLISHED IN REGULATIONS ADOPTED BY THE DEPARTMENT, EACH UNIT OF THE~~**
23 **~~LEGISLATIVE OR JUDICIAL BRANCH OF STATE GOVERNMENT, EACH UNIT OF LOCAL~~**
24 **GOVERNMENT, AND ANY LOCAL AGENCIES THAT USE THE NETWORK ESTABLISHED**
25 **UNDER SUBSECTION (B) OF THIS SECTION SHALL CERTIFY TO THE DEPARTMENT**
26 **THAT THE UNIT IS IN COMPLIANCE WITH THE DEPARTMENT'S MINIMUM SECURITY**
27 **STANDARDS.**

28 **3.5-405.**

29 **(A) THIS SECTION DOES NOT APPLY TO MUNICIPAL GOVERNMENTS.**

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

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

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

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

8 ~~(i) THE NUMBER OF INFORMATION TECHNOLOGY STAFF~~
 9 ~~POSITIONS, INCLUDING VACANCIES;~~

10 ~~(ii) THE ENTITY'S CYBERSECURITY BUDGET AND OVERALL~~
 11 ~~INFORMATION TECHNOLOGY BUDGET;~~

12 ~~(iii) THE NUMBER OF EMPLOYEES WHO HAVE RECEIVED~~
 13 ~~CYBERSECURITY TRAINING; AND~~

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

16 4-308.

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

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

24 ~~6-226.~~

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

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

1 ~~144. the Health Equity Resource Community Reserve Fund;~~

2 ~~[and]~~

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

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

5 ~~12-107.~~

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

8 ~~(2) the Department of General Services may:~~

9 ~~(i) engage in or control procurement of:~~

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

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

14 Article – State Government

15 2–1224.

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

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

24 SECTION 3. AND BE IT FURTHER ENACTED, That, on or before December 1,
25 2022, the State Chief Information Security Officer and the Secretary of Emergency
26 Management shall:

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

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

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

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

5 SECTION 4. AND BE IT FURTHER ENACTED, That:

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

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

11 (2) report any recommendations to the Governor and, in accordance with §
12 2–1257 of the State Government Article, the General Assembly.

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

16 ~~SECTION 5. AND BE IT FURTHER ENACTED, That this Act shall take effect July~~
17 ~~1, 2022.~~

18 SECTION 5. AND BE IT FURTHER ENACTED, That:

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

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

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

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

34 SECTION 7. AND BE IT FURTHER ENACTED, That:

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

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

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

Approved:

Governor.

President of the Senate.

Speaker of the House of Delegates.