

SENATE BILL 754

S2, E4, P1

2lr1504
CF 2lr1778

By: **Senator Hester**

Introduced and read first time: February 7, 2022

Assigned to: Education, Health, and Environmental Affairs

A BILL ENTITLED

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 to report certain cybersecurity incidents in a certain
7 manner and under certain circumstances; requiring the Maryland Joint Operations
8 Center to notify appropriate agencies of a cybersecurity incident in a certain manner;
9 establishing the Cybersecurity Fusion Center in the Maryland Department of
10 Emergency Management; establishing certain responsibilities of the Fusion Center;
11 establishing the Local Cybersecurity Support Fund, the purposes of the Fund, and
12 certain eligibility requirements to receive assistance from the Fund; establishing the
13 Office of Security Management within the Department of Information Technology
14 and certain Office positions; establishing certain responsibilities and authority of the
15 Office; requiring each unit of the Legislative or Judicial Branch of State government,
16 each unit of local government, and any local agencies that use a certain network to
17 certify certain compliance to the Department of Information Technology on or before
18 a certain date each year; requiring certain local entities to submit a certain report to
19 the Office on or before a certain date each year; requiring the Office to submit a
20 certain report to the Governor and certain committees of the General Assembly on
21 or before a certain date each year; requiring the State Chief Information Security
22 Officer and the Secretary of Emergency Management to conduct a certain review,
23 make recommendations, establish certain guidance, and submit a certain report on
24 or before a certain date; requiring the State Chief Information Security Officer to
25 commission a certain feasibility study and report recommendations on or before a
26 certain date; requiring the Governor to include an appropriation in a certain annual
27 budget to cover the cost of the feasibility study; and generally relating to local
28 government cybersecurity coordination and operations.

29 BY renumbering

30 Article – State Finance and Procurement

EXPLANATION: CAPITALS INDICATE MATTER ADDED TO EXISTING LAW.

[Brackets] indicate matter deleted from existing law.



- 1 Section 3A–101 through 3A–702, respectively, and the title “Title 3A. Department of
2 Information Technology”
3 to be Section 3.5–101 through 3.5–702, respectively, and the title “Title 3.5.
4 Department of Information Technology”
5 Annotated Code of Maryland
6 (2021 Replacement Volume)
- 7 BY repealing and reenacting, with amendments,
8 Article – Criminal Procedure
9 Section 10–221(b)
10 Annotated Code of Maryland
11 (2018 Replacement Volume and 2021 Supplement)
- 12 BY repealing and reenacting, with amendments,
13 Article – Health – General
14 Section 21–2C–03(h)(2)(i)
15 Annotated Code of Maryland
16 (2019 Replacement Volume and 2021 Supplement)
- 17 BY repealing and reenacting, with amendments,
18 Article – Human Services
19 Section 7–806(a), (b)(1), (c)(1), (d)(1) and (2)(i), and (g)(1)
20 Annotated Code of Maryland
21 (2019 Replacement Volume and 2021 Supplement)
- 22 BY repealing and reenacting, with amendments,
23 Article – Insurance
24 Section 31–103(a)(2)(i) and (b)(2)
25 Annotated Code of Maryland
26 (2017 Replacement Volume and 2021 Supplement)
- 27 BY repealing and reenacting, with amendments,
28 Article – Natural Resources
29 Section 1–403(c)
30 Annotated Code of Maryland
31 (2018 Replacement Volume and 2021 Supplement)
- 32 BY repealing and reenacting, without amendments,
33 Article – Public Safety
34 Section 14–103
35 Annotated Code of Maryland
36 (2018 Replacement Volume and 2021 Supplement)
- 37 BY adding to
38 Article – Public Safety
39 Section 14–104.1
40 Annotated Code of Maryland

1 (2018 Replacement Volume and 2021 Supplement)

2 BY repealing and reenacting, without amendments,
3 Article – State Finance and Procurement
4 Section 3.5–101(a) and (e) and 3.5–301(a)
5 Annotated Code of Maryland
6 (2021 Replacement Volume)
7 (As enacted by Section 1 of this Act)

8 BY adding to
9 Article – State Finance and Procurement
10 Section 3.5–2A–01 through 3.5–2A–04 to be under the new subtitle “Subtitle 2A.
11 Office of Security Management”; and 3.5–405 and 6–226(a)(2)(ii)146.
12 Annotated Code of Maryland
13 (2021 Replacement Volume)

14 BY repealing and reenacting, with amendments,
15 Article – State Finance and Procurement
16 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),
17 and (l)(1)(i), 3.5–311(a)(2)(i), and 3.5–404
18 Annotated Code of Maryland
19 (2021 Replacement Volume)
20 (As enacted by Section 1 of this Act)

21 BY repealing and reenacting, without amendments,
22 Article – State Finance and Procurement
23 Section 6–226(a)(2)(i)
24 Annotated Code of Maryland
25 (2021 Replacement Volume)

26 BY repealing and reenacting, with amendments,
27 Article – State Finance and Procurement
28 Section 6–226(a)(2)(ii)144. and 145. and 12–107(b)(2)(i)10. and 11.
29 Annotated Code of Maryland
30 (2021 Replacement Volume)

31 BY repealing and reenacting, with amendments,
32 Article – State Government
33 Section 2–1224(f)
34 Annotated Code of Maryland
35 (2021 Replacement Volume)

36 BY adding to
37 Article – State Government
38 Section 2–1224(i)
39 Annotated Code of Maryland
40 (2021 Replacement Volume)

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

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

8 **Article – Criminal Procedure**

9 10–221.

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

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

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

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

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

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

23 (i) accurate and complete; and

24 (ii) collected, reported, and disseminated in accordance with Subtitle
25 1 of this title and this subtitle;

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

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

31 **Article – Health – General**

1 21-2C-03.

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

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

7 **Article – Human Services**

8 7-806.

9 (a) (1) Subject to paragraph (2) of this subsection, the programs under §
10 7-804(a) of this subtitle, § 7-902(a) of this title, and [§ 3A-702] § 3.5-702 of the State
11 Finance and Procurement Article shall be funded as provided in the State budget.

12 (2) For fiscal year 2019 and each fiscal year thereafter, the program under
13 [§ 3A-702] § 3.5-702 of the State Finance and Procurement Article shall be funded at an
14 amount that:

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

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

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

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

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

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

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

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

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

2 (d) (1) The Secretary shall annually certify to the Public Service Commission
3 the costs of the programs under § 7–804(a) of this subtitle, § 7–902(a) of this title, and [§
4 3A–702] § 3.5–702 of the State Finance and Procurement Article to be paid by the
5 Universal Service Trust Fund for the following fiscal year.

6 (2) (i) The Public Service Commission shall determine the surcharge
7 for the following fiscal year necessary to fund the programs under § 7–804(a) of this subtitle,
8 § 7–902(a) of this title, and [§ 3A–702] § 3.5–702 of the State Finance and Procurement
9 Article.

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

14 Article – Insurance

15 31–103.

16 (a) The Exchange is subject to:

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

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

21 (b) The Exchange is not subject to:

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

25 Article – Natural Resources

26 1–403.

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

30 Article – Public Safety

1 14-103.

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

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

7 (c) The Department may act to:

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

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

11 (3) coordinate emergency management activities and operations:

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

14 (ii) between State agencies and political subdivisions;

15 (iii) with local governments;

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

17 (v) with private and nonprofit entities.

18 14-104.1.

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

21 (2) "FUND" MEANS THE LOCAL CYBERSECURITY SUPPORT FUND.

22 (3) "FUSION CENTER" MEANS THE CYBERSECURITY FUSION
23 CENTER.

24 (4) "LOCAL GOVERNMENT" INCLUDES LOCAL SCHOOL SYSTEMS,
25 LOCAL SCHOOL BOARDS, AND LOCAL HEALTH DEPARTMENTS.

26 (5) "UNIT" MEANS THE CYBER PREPAREDNESS UNIT.

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

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

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

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

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

19 **(IV) ASSIST LOCAL GOVERNMENTS IN:**

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

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

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

27 **(VI) DEVELOP APPROPRIATE REPORTS ON LOCAL**
28 **CYBERSECURITY PREPAREDNESS;**

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

1 (VIII) ESTABLISH REGIONAL ASSISTANCE GROUPS TO DELIVER
2 AND COORDINATE SUPPORT SERVICES TO LOCAL GOVERNMENTS, AGENCIES, OR
3 REGIONS.

4 (C) (1) EACH LOCAL GOVERNMENT SHALL REPORT A CYBERSECURITY
5 INCIDENT, INCLUDING AN ATTACK ON A STATE SYSTEM BEING USED BY THE LOCAL
6 GOVERNMENT, TO THE MARYLAND JOINT OPERATIONS CENTER IN THE
7 DEPARTMENT IN ACCORDANCE WITH PARAGRAPH (2) OF THIS SUBSECTION.

8 (2) FOR THE REPORTING OF CYBERSECURITY INCIDENTS UNDER
9 PARAGRAPH (1) OF THIS SUBSECTION, THE DEPARTMENT SHALL DETERMINE:

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

12 (II) THE MANNER IN WHICH TO REPORT; AND

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

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

17 (D) (1) THERE IS A CYBERSECURITY FUSION CENTER IN THE
18 DEPARTMENT.

19 (2) THE FUSION CENTER SHALL:

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

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

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

30 (IV) SUPPORT RISK-BASED PLANNING FOR THE USE OF
31 FEDERAL RESOURCES; AND

1 (V) CONDUCT ANALYSIS OF CYBERSECURITY INCIDENTS.

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

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

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

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

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

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

13 4. PAYING OUTSIDE VENDORS FOR CYBERSECURITY
14 STAFF TRAINING; AND

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

17 (3) THE SECRETARY SHALL ADMINISTER THE FUND.

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

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

22 (5) THE FUND CONSISTS OF:

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

25 (II) INTEREST EARNINGS; AND

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

1 **(6) THE FUND MAY BE USED ONLY:**

2 **(I) TO PROVIDE FINANCIAL ASSISTANCE TO LOCAL**
3 **GOVERNMENTS TO IMPROVE CYBERSECURITY PREPAREDNESS, INCLUDING:**

4 **1. UPDATING CURRENT DEVICES AND NETWORKS WITH**
5 **THE MOST UP-TO-DATE CYBERSECURITY PROTECTIONS;**

6 **2. SUPPORTING THE PURCHASE OF NEW HARDWARE,**
7 **SOFTWARE, DEVICES, AND FIREWALLS TO IMPROVE CYBERSECURITY**
8 **PREPAREDNESS;**

9 **3. RECRUITING AND HIRING INFORMATION**
10 **TECHNOLOGY STAFF FOCUSED ON CYBERSECURITY; AND**

11 **4. PAYING OUTSIDE VENDORS FOR CYBERSECURITY**
12 **STAFF TRAINING;**

13 **(II) TO ASSIST LOCAL GOVERNMENTS APPLYING FOR FEDERAL**
14 **CYBERSECURITY PREPAREDNESS GRANTS; AND**

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

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

19 **(II) ANY INTEREST EARNINGS OF THE FUND SHALL BE**
20 **CREDITED TO THE FUND.**

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

23 **(F) TO BE ELIGIBLE TO RECEIVE ASSISTANCE FROM THE FUND, EACH**
24 **LOCAL GOVERNMENT THAT USES THE NETWORK ESTABLISHED IN ACCORDANCE**
25 **WITH § 3.5-404 OF THE STATE FINANCE AND PROCUREMENT ARTICLE SHALL MEET**
26 **THE REQUIREMENTS OF §§ 3.5-404(D) AND 3.5-405 OF THE STATE FINANCE AND**
27 **PROCUREMENT ARTICLE.**

28 **Article – State Finance and Procurement**

29 3.5-101.

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

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

4 **SUBTITLE 2A. OFFICE OF SECURITY MANAGEMENT.**

5 **3.5-2A-01.**

6 **IN THIS SUBTITLE, "OFFICE" MEANS THE OFFICE OF SECURITY**
7 **MANAGEMENT.**

8 **3.5-2A-02.**

9 **THERE IS AN OFFICE OF SECURITY MANAGEMENT WITHIN THE DEPARTMENT.**

10 **3.5-2A-03.**

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

13 **(B) THE STATE CHIEF INFORMATION SECURITY OFFICER SHALL:**

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

16 **(2) SERVE AT THE PLEASURE OF THE GOVERNOR;**

17 **(3) BE SUPERVISED BY THE SECRETARY; AND**

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

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

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

25 **(II) THE DIRECTOR OF LOCAL CYBERSECURITY SHALL WORK**
26 **IN COORDINATION WITH THE MARYLAND DEPARTMENT OF EMERGENCY**
27 **MANAGEMENT TO PROVIDE TECHNICAL ASSISTANCE, COORDINATE RESOURCES,**
28 **AND IMPROVE CYBERSECURITY PREPAREDNESS FOR UNITS OF LOCAL**
29 **GOVERNMENT.**

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

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

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

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

10 **3.5-2A-04.**

11 **(A) THE OFFICE IS RESPONSIBLE FOR:**

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

33 **(c) ON OR BEFORE DECEMBER 31 EACH YEAR, THE OFFICE SHALL REPORT**
34 **TO THE GOVERNOR AND, IN ACCORDANCE WITH § 2-1257 OF THE STATE**

1 GOVERNMENT ARTICLE, THE SENATE BUDGET AND TAXATION COMMITTEE, THE
2 HOUSE APPROPRIATIONS COMMITTEE, AND THE JOINT COMMITTEE ON
3 CYBERSECURITY, INFORMATION TECHNOLOGY, AND BIOTECHNOLOGY ON THE
4 ACTIVITIES OF THE OFFICE AND THE STATE OF CYBERSECURITY PREPAREDNESS IN
5 MARYLAND, INCLUDING:

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

8 (2) A COMPILATION AND ANALYSIS OF THE DATA FROM THE
9 INFORMATION CONTAINED IN THE REPORTS RECEIVED BY THE OFFICE UNDER §
10 3.5-405 OF THIS TITLE, INCLUDING:

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

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

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

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

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

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

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

31 3.5-301.

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

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

5 3.5-302.

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

12 3.5-303.

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

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

15 (ii) 2. for information technology procured by a State unit on or
16 after January 1, 2020, enforce the nonvisual access clause developed under [§ 3A-311] **§**
17 **3.5-311** of this subtitle, including the enforcement of the civil penalty described in [§
18 3A-311(a)(2)(iii)1] **§ 3.5-311(A)(2)(III)1** of this subtitle.

19 3.5-307.

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

23 3.5-309.

24 (c) The Secretary:

25 (2) subject to the provisions of § 2-201 of this article and [§ 3A-307] **§**
26 **3.5-307** of this subtitle, may receive and accept contributions, grants, or gifts of money or
27 property.

28 (i) The Fund may be used:

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

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

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

7 3.5-311.

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

10 (i) within 18 months after the award of the procurement, the
11 Secretary, or the Secretary's designee, will determine whether the information technology
12 meets the nonvisual access standards adopted in accordance with [~~§ 3A-303(b)~~] **§**
13 **3.5-303(B)** of this subtitle;

14 3.5-404.

15 (a) The General Assembly declares that:

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

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

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

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

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

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

33 (2) The network shall consist of:

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

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

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

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

14 **3.5-405.**

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

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

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

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

24 **(3) REPORT TO THE OFFICE:**

25 **(I) THE NUMBER OF INFORMATION TECHNOLOGY STAFF**
26 **POSITIONS, INCLUDING VACANCIES;**

27 **(II) THE ENTITY'S CYBERSECURITY BUDGET AND OVERALL**
28 **INFORMATION TECHNOLOGY BUDGET;**

29 **(III) THE NUMBER OF EMPLOYEES WHO HAVE RECEIVED**
30 **CYBERSECURITY TRAINING; AND**

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

1 6–226.

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

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

10 144. the Health Equity Resource Community Reserve Fund;
11 [and]

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

13 **146. THE LOCAL CYBERSECURITY SUPPORT FUND.**

14 12–107.

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

17 (2) the Department of General Services may:

18 (i) engage in or control procurement of:

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

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

23 **Article – State Government**

24 2–1224.

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

1 **(I) A REPORT AUDITING A UNIT OF STATE OR LOCAL GOVERNMENT SHALL**
2 **HAVE ANY CYBERSECURITY FINDINGS REDACTED BEFORE THE REPORT IS MADE**
3 **AVAILABLE TO THE PUBLIC.**

4 SECTION 3. AND BE IT FURTHER ENACTED, That, on or before December 1,
5 2022, the State Chief Information Security Officer and the Secretary of Emergency
6 Management shall:

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

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

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

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

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

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

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

21 (2) report any recommendations to the Governor and, in accordance with §
22 2–1257 of the State Government Article, the General Assembly.

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

26 SECTION 5. AND BE IT FURTHER ENACTED, That this Act shall take effect July
27 1, 2022.