

HOUSE BILL 1202

E4, P1

2lr1778
CF SB 754

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

Introduced and read first time: February 11, 2022

Assigned to: Health and Government Operations

Committee Report: Favorable with amendments

House action: Adopted

Read second time: March 13, 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 to notify appropriate agencies of a cybersecurity
9 incident in a certain manner; ~~establishing the Cybersecurity Fusion Center in the~~
10 ~~Maryland Department of Emergency Management; establishing certain~~
11 ~~responsibilities of the Fusion Center; establishing the Local Cybersecurity Support~~
12 ~~Fund, the purposes of the Fund, and certain eligibility requirements to receive~~
13 ~~assistance from the Fund;~~ establishing the Office of Security Management within
14 the Department of Information Technology and certain Office positions; establishing
15 certain responsibilities and authority of the Office; requiring ~~each unit of the~~
16 ~~Legislative or Judicial Branch of State government,~~ each unit of local government,
17 and any local agencies that use a certain network to certify certain compliance to the
18 Department of Information Technology on or before a certain date each year;
19 requiring certain local entities to submit a certain report to the Office on or before a
20 certain date each year; requiring the Office to submit a certain report to the Governor
21 and certain committees of the General Assembly on or before a certain date each

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 year; requiring the State Chief Information Security Officer and the Secretary of
2 Emergency Management to conduct a certain review, make recommendations,
3 establish certain guidance, and submit a certain report on or before a certain date;
4 requiring the State Chief Information Security Officer to commission a certain
5 feasibility study and report recommendations on or before a certain date; requiring
6 the Governor to include an appropriation in a certain annual budget to cover the cost
7 of the feasibility study; and generally relating to local government cybersecurity
8 coordination and operations.

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

17 BY repealing and reenacting, with amendments,
18 Article – Criminal Procedure
19 Section 10–221(b)
20 Annotated Code of Maryland
21 (2018 Replacement Volume and 2021 Supplement)

22 BY repealing and reenacting, with amendments,
23 Article – Health – General
24 Section 21–2C–03(h)(2)(i)
25 Annotated Code of Maryland
26 (2019 Replacement Volume and 2021 Supplement)

27 BY repealing and reenacting, with amendments,
28 Article – Human Services
29 Section 7–806(a), (b)(1), (c)(1), (d)(1) and (2)(i), and (g)(1)
30 Annotated Code of Maryland
31 (2019 Replacement Volume and 2021 Supplement)

32 BY repealing and reenacting, with amendments,
33 Article – Insurance
34 Section 31–103(a)(2)(i) and (b)(2)
35 Annotated Code of Maryland
36 (2017 Replacement Volume and 2021 Supplement)

37 BY repealing and reenacting, with amendments,
38 Article – Natural Resources
39 Section 1–403(c)
40 Annotated Code of Maryland
41 (2018 Replacement Volume and 2021 Supplement)

- 1 BY repealing and reenacting, without amendments,
2 Article – Public Safety
3 Section 14–103
4 Annotated Code of Maryland
5 (2018 Replacement Volume and 2021 Supplement)
- 6 BY adding to
7 Article – Public Safety
8 Section 14–104.1
9 Annotated Code of Maryland
10 (2018 Replacement Volume and 2021 Supplement)
- 11 BY repealing and reenacting, without amendments,
12 Article – State Finance and Procurement
13 Section 3.5–101(a) and (e) and 3.5–301(a)
14 Annotated Code of Maryland
15 (2021 Replacement Volume)
16 (As enacted by Section 1 of this Act)
- 17 BY adding to
18 Article – State Finance and Procurement
19 Section 3.5–2A–01 through 3.5–2A–04 to be under the new subtitle “Subtitle 2A.
20 Office of Security Management”; and 3.5–405 ~~and 6–226(a)(2)(ii)146.~~
21 Annotated Code of Maryland
22 (2021 Replacement Volume)
- 23 BY repealing and reenacting, with amendments,
24 Article – State Finance and Procurement
25 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),
26 and (l)(1)(i), 3.5–311(a)(2)(i), and 3.5–404
27 Annotated Code of Maryland
28 (2021 Replacement Volume)
29 (As enacted by Section 1 of this Act)
- 30 ~~BY repealing and reenacting, without amendments,
31 Article – State Finance and Procurement
32 Section 6–226(a)(2)(i)
33 Annotated Code of Maryland
34 (2021 Replacement Volume)~~
- 35 ~~BY repealing and reenacting, with amendments,
36 Article – State Finance and Procurement
37 Section 6–226(a)(2)(ii)144. and 145. and 12–107(b)(2)(i)10. and 11.
38 Annotated Code of Maryland
39 (2021 Replacement Volume)~~

1 BY repealing and reenacting, with amendments,

2 Article – State Government
3 Section 2–1224(f)
4 Annotated Code of Maryland
5 (2021 Replacement Volume)

6 BY adding to

7 Article – State Government
8 Section 2–1224(i)
9 Annotated Code of Maryland
10 (2021 Replacement Volume)

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

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

18 **Article – Criminal Procedure**

19 10–221.

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

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

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

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

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

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

33 (i) accurate and complete; and

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

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

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

8 Article – Health – General

9 21–2C–03.

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

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

15 Article – Human Services

16 7–806.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

22 Article – Insurance

23 31-103.

24 (a) The Exchange is subject to:

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

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

29 (b) The Exchange is not subject to:

30 (2) Title [3A] 3.5, Subtitle 3 (Information Processing) of the State Finance
31 and Procurement Article, except to the extent determined by the Secretary of Information
32 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.~~

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

3 ~~(4)~~ (2) “LOCAL GOVERNMENT” INCLUDES LOCAL SCHOOL
4 SYSTEMS, LOCAL SCHOOL BOARDS, AND LOCAL HEALTH DEPARTMENTS.

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

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

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

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

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

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

25 (IV) ASSIST LOCAL GOVERNMENTS IN:

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

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

30 (V) CONNECT LOCAL GOVERNMENTS TO APPROPRIATE
31 RESOURCES FOR ANY OTHER PURPOSE RELATED TO CYBERSECURITY
32 PREPAREDNESS AND RESPONSE;

1 (VI) DEVELOP APPROPRIATE REPORTS ON LOCAL
2 CYBERSECURITY PREPAREDNESS;

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

6 (VIII) ESTABLISH REGIONAL ASSISTANCE GROUPS TO DELIVER
7 AND COORDINATE SUPPORT SERVICES TO LOCAL GOVERNMENTS, AGENCIES, OR
8 REGIONS.

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

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

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

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

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

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

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

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

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

1 ~~(H) WITH THE OFFICE OF SECURITY MANAGEMENT IN THE~~
2 ~~DEPARTMENT OF INFORMATION TECHNOLOGY, SUPPORT CYBERSECURITY~~
3 ~~COORDINATION BETWEEN LOCAL UNITS OF GOVERNMENT THROUGH EXISTING~~
4 ~~LOCAL GOVERNMENT STAKEHOLDER ORGANIZATIONS;~~

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

27 ~~(8) EXPENDITURES FROM THE FUND MAY BE MADE ONLY IN~~
28 ~~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 **(1) AT A MINIMUM, HOLD A BACHELOR'S DEGREE;**

2 **(2) HOLD APPROPRIATE INFORMATION TECHNOLOGY OR**
3 **CYBERSECURITY CERTIFICATIONS;**

4 **(3) HAVE EXPERIENCE:**

5 **(I) IDENTIFYING, IMPLEMENTING, AND ASSESSING SECURITY**
6 **CONTROLS;**

7 **(II) IN INFRASTRUCTURE, SYSTEMS ENGINEERING, AND**
8 **CYBERSECURITY;**

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

12 **(IV) WORKING WITH COMMON INFORMATION SECURITY**
13 **MANAGEMENT FRAMEWORKS;**

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

19 **(5) HAVE KNOWLEDGE OF CURRENT SECURITY REGULATIONS AND**
20 **LEGISLATIVE CONTENT.**

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

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

27 **(II) THE DIRECTOR OF LOCAL CYBERSECURITY SHALL WORK**
28 **IN COORDINATION WITH THE MARYLAND DEPARTMENT OF EMERGENCY**
29 **MANAGEMENT TO PROVIDE TECHNICAL ASSISTANCE, COORDINATE RESOURCES,**
30 **AND IMPROVE CYBERSECURITY PREPAREDNESS FOR UNITS OF LOCAL**
31 **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 ~~**(F)**~~ **(F) THE DEPARTMENT SHALL PROVIDE THE OFFICE WITH**
7 **SUFFICIENT STAFF TO PERFORM THE FUNCTIONS OF THIS SUBTITLE.**

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

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

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

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

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

20 **(III) SUPPORTING THE MARYLAND DEPARTMENT OF**
21 **EMERGENCY MANAGEMENT CYBER PREPAREDNESS UNIT DURING EMERGENCY**
22 **RESPONSE EFFORTS.**

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

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

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

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

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

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

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

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

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

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

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

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

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

32 **(12) ~~REVIEW AND CERTIFY~~ SUPPORT LOCAL GOVERNMENTS**
33 **DEVELOPING LOCAL CYBERSECURITY PREPAREDNESS AND RESPONSE PLANS;**

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

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

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

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

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

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

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

17 **(3) DEVELOP APPROPRIATE REPORTS ON LOCAL CYBERSECURITY**
18 **PREPAREDNESS.**

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

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

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

27 **~~(C)~~ (E) ON OR BEFORE DECEMBER 31 EACH YEAR, THE OFFICE SHALL**
28 **REPORT TO THE GOVERNOR AND, IN ACCORDANCE WITH § 2-1257 OF THE STATE**
29 **GOVERNMENT ARTICLE, THE SENATE BUDGET AND TAXATION COMMITTEE, THE**
30 **SENATE EDUCATION, HEALTH, AND ENVIRONMENTAL AFFAIRS COMMITTEE, THE**
31 **HOUSE APPROPRIATIONS COMMITTEE, THE HOUSE HEALTH AND GOVERNMENT**
32 **OPERATIONS COMMITTEE, AND THE JOINT COMMITTEE ON CYBERSECURITY,**
33 **INFORMATION TECHNOLOGY, AND BIOTECHNOLOGY ON THE ACTIVITIES OF THE**

1 OFFICE AND THE STATE OF CYBERSECURITY PREPAREDNESS IN MARYLAND,
2 INCLUDING:

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

5 (2) A COMPILATION AND ANALYSIS OF THE DATA FROM THE
6 INFORMATION CONTAINED IN THE REPORTS RECEIVED BY THE OFFICE UNDER §
7 3.5-405 OF THIS TITLE, INCLUDING:

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

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

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

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

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

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

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

28 3.5-301.

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

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

1 3.5–302.

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

8 3.5–303.

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

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

11 (ii) 2. for information technology procured by a State unit on or
12 after January 1, 2020, enforce the nonvisual access clause developed under [§ 3A–311] §
13 **3.5–311** of this subtitle, including the enforcement of the civil penalty described in [§
14 3A–311(a)(2)(iii)1] **§ 3.5–311(A)(2)(III)1** of this subtitle.

15 3.5–307.

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

19 3.5–309.

20 (c) The Secretary:

21 (2) subject to the provisions of § 2–201 of this article and [§ 3A–307] §
22 **3.5–307** of this subtitle, may receive and accept contributions, grants, or gifts of money or
23 property.

24 (i) The Fund may be used:

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

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

1 (i) the State telecommunication and computer network established
2 under ~~[\S 3A-404]~~ **\S 3.5-404** of this title, including program development for these
3 activities; and

4 3.5-311.

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

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

11 3.5-404.

12 (a) The General Assembly declares that:

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

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

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

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

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

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

30 (2) The network shall consist of:

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

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

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

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

12 **3.5-405.**

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

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

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

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

22 (3) REPORT TO THE OFFICE:

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

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

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

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

31 (C) THE ASSESSMENT REQUIRED UNDER PARAGRAPH (B)(2) OF THIS
32 SECTION MAY, IN ACCORDANCE WITH THE PREFERENCE OF EACH COUNTY

1 GOVERNMENT, BE PERFORMED BY THE DEPARTMENT OR A VENDOR AUTHORIZED
 2 BY THE DEPARTMENT.

3 ~~6-226.~~

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

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

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

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

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

16 ~~12-107.~~

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

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

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

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

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

25 **Article – State Government**

26 2-1224.

27 (f) [After] **EXCEPT AS PROVIDED IN SUBSECTION (I) OF THIS SECTION,**
 28 **AFTER** the expiration of any period that the Joint Audit and Evaluation Committee
 29 specifies, a report of the Legislative Auditor is available to the public under Title 4,
 30 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 IN A MANNER CONSISTENT WITH**
3 **AUDITING BEST PRACTICES BEFORE THE REPORT IS MADE AVAILABLE TO THE**
4 **PUBLIC.**

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

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

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

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

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

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

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

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

22 (2) report any recommendations to the Governor and, in accordance with §
23 2–1257 of the State Government Article, the General Assembly.

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

27 SECTION 5. AND BE IT FURTHER ENACTED, That this Act shall take effect July
28 1, 2022.