

HOUSE BILL 1346

S2, P1, P2

2lr1409
CF SB 812

By: Delegates P. Young, Kerr, Bartlett, ~~and Kelly~~ Kelly, Bagnall, Bhandari, Carr, Chisholm, Cullison, Hill, Johnson, Kaiser, Kipke, 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 **State Government – Cybersecurity – Coordination and Governance**

3 FOR the purpose of ~~establishing the Cybersecurity Coordination and Operations Office in~~
4 ~~the Maryland Department of Emergency Management; requiring the Secretary of~~
5 ~~Emergency Management to appoint an Executive Director as head of the~~
6 ~~Cybersecurity Coordination and Operations Office; requiring the Office of Security~~
7 ~~Management to be provided with staff for the Cybersecurity Coordination and~~
8 ~~Operations Office; requiring the Cybersecurity Coordination and Operations Office~~
9 ~~to establish regional assistance groups to deliver or coordinate support services to~~
10 ~~political subdivisions, agencies, or regions in accordance with certain requirements;~~
11 ~~requiring the Cybersecurity Coordination and Operations Office to offer certain~~
12 ~~training opportunities for counties and municipalities;~~ establishing the Office of
13 Security Management within the Department of Information Technology (DoIT);
14 establishing certain responsibilities and authority of the Office of Security
15 Management; ~~centralizing authority and control of the procurement of all~~
16 ~~information technology for the Executive Branch of State government in DoIT;~~
17 establishing the Cybersecurity Coordination and Operations Unit in DoIT; requiring
18 the Secretary of Information Technology to appoint an Executive Director as head of
19 the Cybersecurity Coordination and Operations Unit; requiring the Office of Security
20 Management to provide staff for the Cybersecurity Coordination and Operations
21 Unit; requiring the Cybersecurity Coordination and Operations Unit to establish
22 regional assistance groups to deliver or coordinate support services to political

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 subdivisions, agencies, or regions in accordance with certain requirements; requiring
 2 the Cybersecurity Coordination and Operations Unit to offer certain training
 3 opportunities for counties and municipalities; requiring the Secretary of Information
 4 Technology to develop and maintain a statewide cybersecurity master plan;
 5 requiring DoIT to develop and require basic security requirements to be included in
 6 certain contracts; ~~requiring each unit of the Legislative or Judicial Branch of State~~
 7 ~~government and any division of the University System of Maryland that uses a~~
 8 ~~certain network to certify certain compliance to DoIT on or before a certain date each~~
 9 ~~year;~~ requiring each unit of the Executive Branch of State government and certain
 10 local entities to report certain cybersecurity incidents in a certain manner and under
 11 certain circumstances; requiring the Maryland Joint Operations Center to notify
 12 certain agencies of a cybersecurity incident reported in a certain manner;
 13 establishing the Maryland Cybersecurity Coordinating Council; ~~exempting meetings~~
 14 ~~of the Council from the Open Meetings Act;~~ requiring the Council to study aspects of
 15 the State's cybersecurity vulnerabilities and procurement potential, including
 16 partnerships with other states; requiring the Council to promote certain education
 17 and training opportunities; requiring DoIT to complete implementation of a certain
 18 governance, risk, and compliance module on or before a certain date; ~~transferring~~
 19 ~~certain appropriations, books and records, and employees to DoIT;~~ and generally
 20 relating to State cybersecurity coordination.

21 BY renumbering

22 Article – State Finance and Procurement

23 Section 3A–101 through 3A–702, respectively, and the title “Title 3A. Department of
 24 Information Technology”

25 to be Section 3.5–101 through 3.5–702, respectively, and the title “Title 3.5.
 26 Department of Information Technology”

27 Annotated Code of Maryland
 28 (2021 Replacement Volume)

29 BY repealing and reenacting, with amendments,

30 Article – Criminal Procedure

31 Section 10–221(b)

32 Annotated Code of Maryland

33 (2018 Replacement Volume and 2021 Supplement)

34 BY repealing and reenacting, with amendments,

35 Article – Health – General

36 Section 21–2C–03(h)(2)(i)

37 Annotated Code of Maryland

38 (2019 Replacement Volume and 2021 Supplement)

39 BY repealing and reenacting, with amendments,

40 Article – Human Services

41 Section 7–806(a), (b)(1), (c)(1), (d)(1) and (2)(i), and (g)(1)

42 Annotated Code of Maryland

43 (2019 Replacement Volume and 2021 Supplement)

1 BY repealing and reenacting, with amendments,
 2 Article – Insurance
 3 Section 31–103(a)(2)(i) and (b)(2)
 4 Annotated Code of Maryland
 5 (2017 Replacement Volume and 2021 Supplement)

6 BY repealing and reenacting, with amendments,
 7 Article – Natural Resources
 8 Section 1–403(c)
 9 Annotated Code of Maryland
 10 (2018 Replacement Volume and 2021 Supplement)

11 ~~BY adding to~~
 12 ~~Article – Public Safety~~
 13 ~~Section 14–104.1~~
 14 ~~Annotated Code of Maryland~~
 15 ~~(2018 Replacement Volume and 2021 Supplement)~~

16 BY repealing and reenacting, without amendments,
 17 Article – State Finance and Procurement
 18 Section 3.5–101(a) and (e) and 3.5–301(a)
 19 Annotated Code of Maryland
 20 (2021 Replacement Volume)
 21 (As enacted by Section 1 of this Act)

22 BY adding to
 23 Article – State Finance and Procurement
 24 Section 3.5–2A–01 through ~~3.5–2A–07~~ 3.5–2A–08 to be under the new subtitle
 25 “Subtitle 2A. Office of Security Management”; and 3.5–405 and
 26 ~~12–107(b)(2)(i)~~ 3.5–406
 27 Annotated Code of Maryland
 28 (2021 Replacement Volume)

29 BY repealing and reenacting, with amendments,
 30 Article – State Finance and Procurement
 31 Section 3.5–301(j), ~~3.5–302(c)~~ 3.5–302, 3.5–303, ~~3.5–305~~, 3.5–307 through ~~3.5–314~~,
 32 3.5–309(c), (i), and (l), 3.5–311(a)(2)(i), and 3.5–401, and ~~3.5–404~~
 33 Annotated Code of Maryland
 34 (2021 Replacement Volume)
 35 (As enacted by Section 1 of this Act)

36 ~~BY repealing~~
 37 ~~Article – State Finance and Procurement~~
 38 ~~Section 3.5–306~~
 39 ~~Annotated Code of Maryland~~
 40 ~~(2021 Replacement Volume)~~

~~(As enacted by Section 1 of this Act)~~

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

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

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

Article – Criminal Procedure

10–221.

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

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

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

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

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

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

(i) accurate and complete; and

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

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

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

4 Article – Health – General

5 21–2C–03.

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

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

11 Article – Human Services

12 7–806.

13 (a) (1) Subject to paragraph (2) of this subsection, the programs under §
14 7–804(a) of this subtitle, § 7–902(a) of this title, and [§ 3A–702] § 3.5–702 of the State
15 Finance and Procurement Article shall be funded as provided in the State budget.

16 (2) For fiscal year 2019 and each fiscal year thereafter, the program under
17 [§ 3A–702] § 3.5–702 of the State Finance and Procurement Article shall be funded at an
18 amount that:

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

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

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

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

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

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

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

4 (i) a surcharge to be paid by the subscribers to a communications
 5 service; and

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

7 (d) (1) The Secretary shall annually certify to the Public Service Commission
 8 the costs of the programs under § 7–804(a) of this subtitle, § 7–902(a) of this title, and [§
 9 3A–702] § 3.5–702 of the State Finance and Procurement Article to be paid by the
 10 Universal Service Trust Fund for the following fiscal year.

11 (2) (i) The Public Service Commission shall determine the surcharge
 12 for the following fiscal year necessary to fund the programs under § 7–804(a) of this subtitle,
 13 § 7–902(a) of this title, and [§ 3A–702] § 3.5–702 of the State Finance and Procurement
 14 Article.

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

19 Article – Insurance

20 31–103.

21 (a) The Exchange is subject to:

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

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

26 (b) The Exchange is not subject to:

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

30 Article – Natural Resources

31 1–403.

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

4 ~~Article—Public Safety~~

5 ~~14-104.1.~~

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

8 (2) ~~“OFFICE” MEANS THE CYBERSECURITY COORDINATION AND~~
9 ~~OPERATIONS OFFICE ESTABLISHED WITHIN THE DEPARTMENT.~~

10 (3) ~~“REGION” MEANS A COLLECTION OF POLITICAL SUBDIVISIONS.~~

11 (B) ~~THERE IS A CYBERSECURITY COORDINATION AND OPERATIONS~~
12 ~~OFFICE WITHIN THE DEPARTMENT.~~

13 (C) ~~THE PURPOSE OF THE OFFICE IS TO:~~

14 (1) ~~IMPROVE LOCAL, REGIONAL, AND STATEWIDE CYBERSECURITY~~
15 ~~READINESS AND RESPONSE;~~

16 (2) ~~ASSIST POLITICAL SUBDIVISIONS, SCHOOL BOARDS, AND~~
17 ~~AGENCIES IN THE DEVELOPMENT OF CYBERSECURITY DISRUPTION PLANS;~~

18 (3) ~~IN CONSULTATION WITH THE DEPARTMENT OF INFORMATION~~
19 ~~TECHNOLOGY, COORDINATE WITH POLITICAL SUBDIVISIONS, LOCAL AGENCIES,~~
20 ~~AND STATE AGENCIES ON THE IMPLEMENTATION OF CYBERSECURITY BEST~~
21 ~~PRACTICES;~~

22 (4) ~~COORDINATE WITH POLITICAL SUBDIVISIONS AND AGENCIES ON~~
23 ~~THE IMPLEMENTATION OF THE STATEWIDE MASTER PLAN DEVELOPED BY THE~~
24 ~~DEPARTMENT OF INFORMATION TECHNOLOGY UNDER TITLE 3.5, SUBTITLE 3 OF~~
25 ~~THE STATE FINANCE AND PROCUREMENT ARTICLE; AND~~

26 (5) ~~CONSULT WITH THE STATE CHIEF INFORMATION SECURITY~~
27 ~~OFFICER AND THE SECRETARY OF INFORMATION TECHNOLOGY TO CONNECT~~
28 ~~POLITICAL SUBDIVISIONS AND AGENCIES TO THE APPROPRIATE RESOURCES FOR~~
29 ~~ANY OTHER PURPOSE RELATED TO CYBERSECURITY READINESS AND RESPONSE.~~

30 (D) (1) ~~THE HEAD OF THE OFFICE IS THE EXECUTIVE DIRECTOR, WHO~~
31 ~~SHALL BE APPOINTED BY THE DIRECTOR.~~

1 ~~(2) THE OFFICE OF SECURITY MANAGEMENT SHALL PROVIDE STAFF~~
2 ~~FOR THE OFFICE.~~

3 ~~(E) (1) THE OFFICE SHALL ESTABLISH REGIONAL ASSISTANCE GROUPS~~
4 ~~TO DELIVER OR COORDINATE SUPPORT SERVICES TO POLITICAL SUBDIVISIONS,~~
5 ~~AGENCIES, OR REGIONS.~~

6 ~~(2) THE OFFICE MAY HIRE OR PROCURE REGIONAL COORDINATORS~~
7 ~~TO DELIVER OR COORDINATE THE SERVICES UNDER PARAGRAPH (1) OF THIS~~
8 ~~SUBSECTION.~~

9 ~~(3) THE OFFICE SHALL PROVIDE OR COORDINATE SUPPORT~~
10 ~~SERVICES UNDER PARAGRAPH (1) OF THIS SUBSECTION THAT INCLUDE:~~

11 ~~(I) CONNECTING MULTIPLE POLITICAL SUBDIVISIONS AND~~
12 ~~AGENCIES WITH EACH OTHER TO SHARE BEST PRACTICES OR OTHER INFORMATION~~
13 ~~TO INCREASE READINESS OR RESPONSE EFFECTIVENESS;~~

14 ~~(II) PROVIDING TECHNICAL SERVICES FOR THE~~
15 ~~IMPLEMENTATION OF CYBERSECURITY BEST PRACTICES IN ACCORDANCE WITH~~
16 ~~SUBSECTION (C)(3) OF THIS SECTION;~~

17 ~~(III) COMPLETING CYBERSECURITY RISK ASSESSMENTS;~~

18 ~~(IV) DEVELOPING CYBER SCORECARDS AND REPORTS ON~~
19 ~~REGIONAL READINESS;~~

20 ~~(V) CREATING AND UPDATING CYBERSECURITY DISRUPTION~~
21 ~~PLANS IN ACCORDANCE WITH SUBSECTION (C)(2) OF THIS SECTION; AND~~

22 ~~(VI) CONDUCTING REGIONAL EXERCISES IN COORDINATION~~
23 ~~WITH THE NATIONAL GUARD, THE DEPARTMENT, THE DEPARTMENT OF~~
24 ~~INFORMATION TECHNOLOGY, LOCAL EMERGENCY MANAGERS, AND OTHER STATE~~
25 ~~AND LOCAL ENTITIES.~~

26 ~~(F) (1) THE OFFICE SHALL PROVIDE REGULAR TRAINING~~
27 ~~OPPORTUNITIES FOR COUNTIES AND MUNICIPAL CORPORATIONS IN THE STATE.~~

28 ~~(2) TRAINING OPPORTUNITIES OFFERED BY THE OFFICE SHALL:~~

29 ~~(I) BE DESIGNED TO ENSURE STAFF FOR COUNTIES AND~~
30 ~~MUNICIPAL CORPORATIONS ARE CAPABLE OF COOPERATING EFFECTIVELY WITH~~
31 ~~THE DEPARTMENT IN THE EVENT OF A CYBERSECURITY EMERGENCY; AND~~

~~(H) INCORPORATE BEST PRACTICES AND GUIDELINES FOR STATE AND LOCAL GOVERNMENTS PROVIDED BY THE MULTI-STATE INFORMATION SHARING AND ANALYSIS CENTER AND THE CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY.~~

~~(G) ON OR BEFORE DECEMBER 1 EACH YEAR, THE OFFICE SHALL REPORT TO THE GOVERNOR AND, IN ACCORDANCE WITH § 2-1257 OF THE STATE GOVERNMENT ARTICLE, THE GENERAL ASSEMBLY ON THE ACTIVITIES OF THE OFFICE.~~

Article – State Finance and Procurement

3.5–101.

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

(e) “Unit of State government” means an agency or unit of the Executive Branch of State government.

SUBTITLE 2A. OFFICE OF SECURITY MANAGEMENT.

3.5–2A–01.

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

(B) “COUNCIL” MEANS THE MARYLAND CYBERSECURITY COORDINATING COUNCIL.

(C) “OFFICE” MEANS THE OFFICE OF SECURITY MANAGEMENT.

(D) “REGION” MEANS A COLLECTION OF POLITICAL SUBDIVISIONS.

(E) “UNIT” MEANS THE CYBERSECURITY COORDINATION AND OPERATIONS UNIT.

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.

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

2 (1) BE APPOINTED BY THE GOVERNOR WITH THE ADVICE AND
3 CONSENT OF THE SENATE;

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

5 (3) BE SUPERVISED BY THE SECRETARY; AND

6 (4) SERVE AS THE CHIEF INFORMATION SECURITY OFFICER OF THE
7 DEPARTMENT.

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

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

11 (2) HOLD APPROPRIATE INFORMATION TECHNOLOGY OR
12 CYBERSECURITY CERTIFICATIONS;

13 (3) HAVE EXPERIENCE:

14 (I) IDENTIFYING, IMPLEMENTING, AND ASSESSING SECURITY
15 CONTROLS;

16 (II) IN INFRASTRUCTURE, SYSTEMS ENGINEERING, AND
17 CYBERSECURITY;

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

21 (IV) WORKING WITH COMMON INFORMATION SECURITY
22 MANAGEMENT FRAMEWORKS;

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

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

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

4 ~~(D)~~ (E) (1) (I) THERE IS A DIRECTOR OF LOCAL CYBERSECURITY
5 WHO SHALL BE APPOINTED BY THE STATE CHIEF INFORMATION SECURITY
6 OFFICER.

7 (II) THE DIRECTOR OF LOCAL CYBERSECURITY SHALL WORK
8 IN COORDINATION WITH THE MARYLAND DEPARTMENT OF EMERGENCY
9 MANAGEMENT TO PROVIDE TECHNICAL ASSISTANCE, COORDINATE RESOURCES,
10 AND IMPROVE CYBERSECURITY PREPAREDNESS FOR UNITS OF LOCAL
11 GOVERNMENT.

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

14 (II) THE DIRECTOR OF STATE CYBERSECURITY IS
15 RESPONSIBLE FOR IMPLEMENTATION OF THIS SECTION WITH RESPECT TO UNITS OF
16 STATE GOVERNMENT.

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

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

21 **3.5-2A-04.**

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

23 ~~(1)~~ (1) THE DIRECTION, COORDINATION, AND IMPLEMENTATION
24 OF THE OVERALL CYBERSECURITY STRATEGY AND POLICY FOR UNITS OF STATE
25 GOVERNMENT; ~~AND~~

26 ~~(2)~~ (II) THE COORDINATION OF RESOURCES AND EFFORTS TO
27 IMPLEMENT CYBERSECURITY BEST PRACTICES AND IMPROVE OVERALL
28 CYBERSECURITY PREPAREDNESS AND RESPONSE FOR UNITS OF LOCAL
29 GOVERNMENT, LOCAL SCHOOL BOARDS, LOCAL SCHOOL SYSTEMS, AND LOCAL
30 HEALTH DEPARTMENTS; AND

31 (III) SUPPORTING THE MARYLAND DEPARTMENT OF
32 EMERGENCY MANAGEMENT CYBER PREPAREDNESS UNIT DURING EMERGENCY
33 RESPONSE EFFORTS.

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

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

7 **(1) ESTABLISH STANDARDS TO CATEGORIZE ALL INFORMATION**
8 **COLLECTED OR MAINTAINED BY OR ON BEHALF OF EACH UNIT OF STATE**
9 **GOVERNMENT;**

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

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

14 **(4) ESTABLISH SECURITY REQUIREMENTS FOR INFORMATION AND**
15 **INFORMATION SYSTEMS IN EACH CATEGORY;**

16 **(5) ASSESS THE CATEGORIZATION OF INFORMATION AND**
17 **INFORMATION SYSTEMS AND THE ASSOCIATED IMPLEMENTATION OF THE SECURITY**
18 **REQUIREMENTS ESTABLISHED UNDER ITEM (4) OF THIS SUBSECTION;**

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

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

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

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

1 **(10) DEVELOP AND MAINTAIN INFORMATION TECHNOLOGY SECURITY**
2 **POLICY, STANDARDS, AND GUIDANCE DOCUMENTS, CONSISTENT WITH BEST**
3 **PRACTICES DEVELOPED BY THE NATIONAL INSTITUTE OF STANDARDS AND**
4 **TECHNOLOGY;**

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

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

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

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

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

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

20 **(I) THE DEVELOPMENT OF CYBERSECURITY PREPAREDNESS**
21 **AND RESPONSE PLANS; AND**

22 **(II) IMPLEMENTING BEST PRACTICES AND GUIDANCE**
23 **DEVELOPED BY THE DEPARTMENT;**

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

27 **(3) DEVELOP APPROPRIATE REPORTS ON LOCAL CYBERSECURITY**
28 **PREPAREDNESS.**

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

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

4 **(2) ESTABLISH REGIONAL ASSISTANCE GROUPS TO DELIVER OR**
5 **COORDINATE SUPPORT SERVICES TO LOCAL POLITICAL SUBDIVISIONS, AGENCIES,**
6 **OR REGIONS.**

7 **(E) ON OR BEFORE DECEMBER 31 EACH YEAR, THE OFFICE SHALL REPORT**
8 **TO THE GOVERNOR AND, IN ACCORDANCE WITH § 2-1257 OF THE STATE**
9 **GOVERNMENT ARTICLE, THE SENATE BUDGET AND TAXATION COMMITTEE, THE**
10 **SENATE EDUCATION, HEALTH, AND ENVIRONMENTAL AFFAIRS COMMITTEE, THE**
11 **HOUSE APPROPRIATIONS COMMITTEE, THE HOUSE HEALTH AND GOVERNMENT**
12 **OPERATIONS COMMITTEE, AND THE JOINT COMMITTEE ON CYBERSECURITY,**
13 **INFORMATION TECHNOLOGY, AND BIOTECHNOLOGY ON THE ACTIVITIES OF THE**
14 **OFFICE AND THE STATE OF CYBERSECURITY PREPAREDNESS IN MARYLAND,**
15 **INCLUDING:**

16 **(1) THE ACTIVITIES AND ACCOMPLISHMENTS OF THE OFFICE DURING**
17 **THE PREVIOUS 12 MONTHS AT THE STATE AND LOCAL LEVELS; AND**

18 **(2) A COMPILATION AND ANALYSIS OF THE DATA FROM THE**
19 **INFORMATION CONTAINED IN THE REPORTS RECEIVED BY THE OFFICE UNDER §**
20 **3.5-405 OF THIS TITLE, INCLUDING:**

21 **(I) A SUMMARY OF THE ISSUES IDENTIFIED BY THE**
22 **CYBERSECURITY PREPAREDNESS ASSESSMENTS CONDUCTED THAT YEAR;**

23 **(II) THE STATUS OF VULNERABILITY ASSESSMENTS OF ALL**
24 **UNITS OF STATE GOVERNMENT AND A TIMELINE FOR COMPLETION AND COST TO**
25 **REMEDiate ANY VULNERABILITIES EXPOSED;**

26 **(III) RECENT AUDIT FINDINGS OF ALL UNITS OF STATE**
27 **GOVERNMENT AND OPTIONS TO IMPROVE FINDINGS IN FUTURE AUDITS, INCLUDING**
28 **RECOMMENDATIONS FOR STAFF, BUDGET, AND TIMING;**

29 **(IV) ANALYSIS OF THE STATE'S EXPENDITURE ON**
30 **CYBERSECURITY RELATIVE TO OVERALL INFORMATION TECHNOLOGY SPENDING**
31 **FOR THE PRIOR 3 YEARS AND RECOMMENDATIONS FOR CHANGES TO THE BUDGET,**
32 **INCLUDING AMOUNT, PURPOSE, AND TIMING TO IMPROVE STATE AND LOCAL**
33 **CYBERSECURITY PREPAREDNESS;**

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

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

4 (VII) ANY ADDITIONAL RECOMMENDATIONS FOR IMPROVING
5 STATE AND LOCAL CYBERSECURITY PREPAREDNESS.

6 **3.5-2A-05.**

7 (A) THERE IS A MARYLAND CYBERSECURITY COORDINATING COUNCIL.

8 (B) (1) THE COUNCIL CONSISTS OF THE FOLLOWING MEMBERS:

9 ~~(1) THE SECRETARY OF BUDGET AND MANAGEMENT, OR THE~~
10 ~~SECRETARY'S DESIGNEE;~~

11 ~~(2) THE SECRETARY OF GENERAL SERVICES, OR THE SECRETARY'S~~
12 ~~DESIGNEE;~~

13 ~~(3) THE SECRETARY OF HEALTH, OR THE SECRETARY'S DESIGNEE;~~

14 ~~(4) THE SECRETARY OF HUMAN SERVICES, OR THE SECRETARY'S~~
15 ~~DESIGNEE;~~

16 ~~(5) THE SECRETARY OF PUBLIC SAFETY AND CORRECTIONAL~~
17 ~~SERVICES, OR THE SECRETARY'S DESIGNEE;~~

18 ~~(6) THE SECRETARY OF TRANSPORTATION, OR THE SECRETARY'S~~
19 ~~DESIGNEE;~~

20 ~~(7) THE SECRETARY OF DISABILITIES, OR THE SECRETARY'S~~
21 ~~DESIGNEE;~~

22 (1) THE SECRETARY OF EACH OF THE PRINCIPAL
23 DEPARTMENTS LISTED IN § 8-201 OF THE STATE GOVERNMENT ARTICLE, OR A
24 SECRETARY'S DESIGNEE;

25 ~~(8)~~ (II) THE STATE CHIEF INFORMATION SECURITY OFFICER;

26 ~~(9)~~ (III) THE ADJUTANT GENERAL OF THE MARYLAND NATIONAL
27 GUARD, OR THE ADJUTANT GENERAL'S DESIGNEE;

28 ~~(10) THE SECRETARY OF EMERGENCY MANAGEMENT, OR THE~~
29 ~~SECRETARY'S DESIGNEE;~~

1 ~~(11)~~ (IV) THE SUPERINTENDENT OF STATE POLICE, OR THE
2 SUPERINTENDENT'S DESIGNEE;

3 ~~(12)~~ (V) THE DIRECTOR OF THE GOVERNOR'S OFFICE OF
4 HOMELAND SECURITY, OR THE DIRECTOR'S DESIGNEE;

5 ~~(13)~~ (VI) THE EXECUTIVE DIRECTOR OF THE DEPARTMENT OF
6 LEGISLATIVE SERVICES, OR THE EXECUTIVE DIRECTOR'S DESIGNEE;

7 ~~(14)~~ (VII) ONE REPRESENTATIVE OF THE ADMINISTRATIVE OFFICE
8 OF THE COURTS;

9 ~~(15)~~ (VIII) THE CHANCELLOR OF THE UNIVERSITY SYSTEM OF
10 MARYLAND, OR THE CHANCELLOR'S DESIGNEE; AND

11 ~~(16)~~ (IX) ANY OTHER STAKEHOLDER THAT THE STATE CHIEF
12 INFORMATION SECURITY OFFICER DEEMS APPROPRIATE.

13 (2) IF A DESIGNEE SERVES ON THE COUNCIL IN PLACE OF AN
14 OFFICIAL LISTED IN PARAGRAPH (1) OF THIS SUBSECTION, THE DESIGNEE SHALL
15 REPORT INFORMATION FROM THE COUNCIL MEETINGS AND OTHER
16 COMMUNICATIONS TO THE OFFICIAL.

17 (C) THE CHAIR OF THE COUNCIL IS THE STATE CHIEF INFORMATION
18 SECURITY OFFICER.

19 (D) ~~(1)~~ THE COUNCIL SHALL MEET AT LEAST QUARTERLY AT THE
20 REQUEST OF THE CHAIR.

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

23 (E) THE COUNCIL SHALL:

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

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

28 (II) BUILDING AND SUSTAINING THE CAPABILITY OF THE STATE
29 TO IDENTIFY AND MITIGATE CYBERSECURITY RISK AND RESPOND TO AND RECOVER
30 FROM CYBERSECURITY-RELATED INCIDENTS.

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

6 **(F) IN CARRYING OUT THE DUTIES OF THE COUNCIL, THE COUNCIL ~~MAY~~**
7 **SHALL CONSULT WITH OUTSIDE EXPERTS, INCLUDING EXPERTS IN THE PRIVATE**
8 **SECTOR, GOVERNMENT AGENCIES, AND INSTITUTIONS OF HIGHER EDUCATION.**

9 **3.5-2A-06.**

10 **THE COUNCIL SHALL STUDY THE SECURITY AND FINANCIAL IMPLICATIONS OF**
11 **EXECUTING PARTNERSHIPS WITH OTHER STATES TO PROCURE INFORMATION**
12 **TECHNOLOGY AND CYBERSECURITY PRODUCTS AND SERVICES, INCLUDING THE**
13 **IMPLICATIONS FOR POLITICAL SUBDIVISIONS OF THE STATE.**

14 **3.5-2A-07.**

15 **THE COUNCIL SHALL:**

16 **(1) PROMOTE CYBERSECURITY EDUCATION AND TRAINING**
17 **OPPORTUNITIES TO STRENGTHEN THE STATE'S CYBERSECURITY CAPABILITIES BY**
18 **EXPANDING EXISTING AGREEMENTS WITH EDUCATIONAL INSTITUTIONS;**

19 **(2) UTILIZE RELATIONSHIPS WITH INSTITUTIONS OF HIGHER**
20 **EDUCATION TO ADVERTISE CYBERSECURITY CAREERS AND JOB POSITIONS**
21 **AVAILABLE IN STATE OR LOCAL GOVERNMENT, INCLUDING THE MARYLAND**
22 **TECHNOLOGY INTERNSHIP PROGRAM ESTABLISHED UNDER TITLE 18, SUBTITLE 30**
23 **OF THE EDUCATION ARTICLE; AND**

24 **(3) ASSIST INTERESTED CANDIDATES WITH APPLYING FOR**
25 **CYBERSECURITY POSITIONS IN STATE OR LOCAL GOVERNMENT.**

26 **3.5-2A-08.**

27 **(A) THERE IS A CYBERSECURITY COORDINATION AND OPERATIONS UNIT**
28 **WITHIN THE DEPARTMENT.**

29 **(B) THE PURPOSE OF THE UNIT IS TO:**

30 **(1) IMPROVE LOCAL, REGIONAL, AND STATEWIDE CYBERSECURITY**
31 **READINESS AND RESPONSE;**

1 **(2) ASSIST POLITICAL SUBDIVISIONS, SCHOOL BOARDS, AND**
2 **AGENCIES IN THE DEVELOPMENT OF CYBERSECURITY DISRUPTION PLANS;**

3 **(3) IN CONSULTATION WITH THE MARYLAND DEPARTMENT OF**
4 **EMERGENCY MANAGEMENT, COORDINATE WITH POLITICAL SUBDIVISIONS, LOCAL**
5 **AGENCIES, AND STATE AGENCIES ON THE IMPLEMENTATION OF CYBERSECURITY**
6 **BEST PRACTICES;**

7 **(4) COORDINATE WITH POLITICAL SUBDIVISIONS AND AGENCIES ON**
8 **THE IMPLEMENTATION OF THE STATEWIDE MASTER PLAN DEVELOPED BY THE**
9 **DEPARTMENT UNDER SUBTITLE 3 OF THIS TITLE; AND**

10 **(5) CONSULT WITH THE STATE CHIEF INFORMATION SECURITY**
11 **OFFICER AND THE SECRETARY TO CONNECT POLITICAL SUBDIVISIONS AND**
12 **AGENCIES TO THE APPROPRIATE RESOURCES FOR ANY OTHER PURPOSE RELATED**
13 **TO CYBERSECURITY READINESS AND RESPONSE.**

14 **(C) (1) THE HEAD OF THE UNIT IS THE EXECUTIVE DIRECTOR, WHO**
15 **SHALL BE APPOINTED BY THE SECRETARY.**

16 **(2) THE OFFICE SHALL PROVIDE STAFF FOR THE UNIT.**

17 **(D) (1) THE UNIT SHALL ESTABLISH REGIONAL ASSISTANCE GROUPS TO**
18 **DELIVER OR COORDINATE SUPPORT SERVICES TO POLITICAL SUBDIVISIONS,**
19 **AGENCIES, OR REGIONS.**

20 **(2) THE UNIT MAY HIRE OR PROCURE REGIONAL COORDINATORS TO**
21 **DELIVER OR COORDINATE THE SERVICES UNDER PARAGRAPH (1) OF THIS**
22 **SUBSECTION.**

23 **(3) THE UNIT SHALL PROVIDE OR COORDINATE SUPPORT SERVICES**
24 **UNDER PARAGRAPH (1) OF THIS SUBSECTION THAT INCLUDE:**

25 **(I) CONNECTING MULTIPLE POLITICAL SUBDIVISIONS AND**
26 **AGENCIES WITH EACH OTHER TO SHARE BEST PRACTICES OR OTHER INFORMATION**
27 **TO INCREASE READINESS OR RESPONSE EFFECTIVENESS;**

28 **(II) PROVIDING TECHNICAL SERVICES FOR THE**
29 **IMPLEMENTATION OF CYBERSECURITY BEST PRACTICES IN ACCORDANCE WITH**
30 **SUBSECTION (C)(3) OF THIS SECTION;**

31 **(III) COMPLETING CYBERSECURITY RISK ASSESSMENTS;**

1 **(IV) DEVELOPING CYBER SCORECARDS AND REPORTS ON**
2 **REGIONAL READINESS;**

3 **(V) CREATING AND UPDATING CYBERSECURITY DISRUPTION**
4 **PLANS IN ACCORDANCE WITH SUBSECTION (C)(2) OF THIS SECTION; AND**

5 **(VI) CONDUCTING REGIONAL EXERCISES IN COORDINATION**
6 **WITH THE NATIONAL GUARD, THE DEPARTMENT, THE MARYLAND DEPARTMENT OF**
7 **EMERGENCY MANAGEMENT, LOCAL EMERGENCY MANAGERS, AND OTHER STATE**
8 **AND LOCAL ENTITIES.**

9 **(E) (1) THE UNIT SHALL PROVIDE REGULAR TRAINING OPPORTUNITIES**
10 **FOR COUNTIES AND MUNICIPAL CORPORATIONS IN THE STATE.**

11 **(2) TRAINING OPPORTUNITIES OFFERED BY THE UNIT SHALL:**

12 **(I) BE DESIGNED TO ENSURE STAFF FOR COUNTIES AND**
13 **MUNICIPAL CORPORATIONS ARE CAPABLE OF COOPERATING EFFECTIVELY WITH**
14 **THE DEPARTMENT IN THE EVENT OF A CYBERSECURITY EMERGENCY; AND**

15 **(II) INCORPORATE BEST PRACTICES AND GUIDELINES FOR**
16 **STATE AND LOCAL GOVERNMENTS PROVIDED BY THE MULTI-STATE INFORMATION**
17 **SHARING AND ANALYSIS CENTER AND THE CYBERSECURITY AND**
18 **INFRASTRUCTURE SECURITY AGENCY.**

19 **(F) ON OR BEFORE DECEMBER 1 EACH YEAR, THE UNIT SHALL REPORT TO**
20 **THE GOVERNOR AND, IN ACCORDANCE WITH § 2-1257 OF THE STATE GOVERNMENT**
21 **ARTICLE, THE GENERAL ASSEMBLY ON THE ACTIVITIES OF THE UNIT.**

22 3.5-301.

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

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

28 3.5-302.

29 (a) This subtitle does not apply to changes relating to or the purchase, lease, or
30 rental of information technology by:

31 **(1) public institutions of higher education solely for academic or research**
32 **purposes;**

- 1 (2) the Maryland Port Administration;
- 2 (3) the University System of Maryland;
- 3 (4) St. Mary's College of Maryland;
- 4 (5) Morgan State University;
- 5 (6) the Maryland Stadium Authority; [or]
- 6 (7) Baltimore City Community College;
- 7 (8) THE STATE BOARD OF ELECTIONS;
- 8 (9) THE OFFICE OF THE ATTORNEY GENERAL;
- 9 (10) THE COMPTROLLER;
- 10 (11) THE STATE TREASURER;
- 11 (12) THE LEGISLATIVE BRANCH OF STATE GOVERNMENT; OR
- 12 (13) THE JUDICIAL BRANCH OF STATE GOVERNMENT.

13 (b) Except as provided in subsection (a) of this section, this subtitle applies to any
 14 project of a unit of the Executive Branch of State government that involves an agreement
 15 with a public institution of higher education for a portion of the development of the project,
 16 whether the work on the development is done directly or indirectly by the public institution
 17 of higher education.

18 (c) Notwithstanding any other provision of law, except as provided in subsection
 19 (a) of this section and [§§ 3A-307(a)(2), 3A-308, and 3A-309] **§§ 3.5-306(A)(2), 3.5-307,**
 20 **AND 3.5-308** of this subtitle, this subtitle applies to all units of the Executive Branch of
 21 State government including public institutions of higher education other than Morgan
 22 State University, the University System of Maryland, St. Mary's College of Maryland, and
 23 Baltimore City Community College.

24 3.5-303.

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

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

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

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

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

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

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

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

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

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

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

22 **(VI) ALLOWS A STATE AGENCY TO MAINTAIN THE AGENCY'S OWN**
23 **INFORMATION TECHNOLOGY UNIT THAT PROVIDES FOR INFORMATION**
24 **TECHNOLOGY SERVICES, INCLUDING THE PROCUREMENT OF INFORMATION**
25 **TECHNOLOGY EQUIPMENT AND SERVICES, TO SUPPORT THE MISSION OF THE**
26 **AGENCY.**

27 **(5) PROVIDING OR COORDINATING THE PROCUREMENT OF MANAGED**
28 **CYBERSECURITY SERVICES THAT ARE PAID FOR BY THE STATE AND USED BY LOCAL**
29 **GOVERNMENTS;**

30 **(6) DEVELOPING AND MAINTAINING A STATEWIDE CYBERSECURITY**
31 **MASTER PLAN THAT WILL:**

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

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

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

10 **[(6)] (8)** in consultation with the [Attorney General,] **MARYLAND**
11 **CYBERSECURITY COORDINATING COUNCIL**, advising and overseeing a consistent
12 cybersecurity strategy for units of State government, including institutions under the
13 control of the governing boards of the public institutions of higher education;

14 **[(7)] (9)** advising and consulting with the Legislative and Judicial
15 branches of State government regarding a cybersecurity strategy; and

16 **[(8)] (10)** in consultation with the [Attorney General,] **MARYLAND**
17 **CYBERSECURITY COORDINATING COUNCIL**, developing guidance on consistent
18 cybersecurity strategies for counties, municipal corporations, school systems, and all other
19 political subdivisions of the State.

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

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

23 (1) adopt new nonvisual access procurement standards that:

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

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

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

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

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

5 2. for information technology procured by a State unit on or
 6 after January 1, 2020, enforce the nonvisual access clause developed under [§ 3A-311] §
 7 ~~3.5-310~~ 3.5-311 of this subtitle, including the enforcement of the civil penalty described
 8 in [§ 3A-311(a)(2)(iii)1] § ~~3.5-310(A)(2)(III)1~~ 3.5-311(A)(2)(III)1 of this subtitle.

9 (D) (1) THE GOVERNOR SHALL INCLUDE AN APPROPRIATION IN THE
 10 ANNUAL BUDGET BILL IN AN AMOUNT NECESSARY TO COVER THE COSTS OF
 11 IMPLEMENTING THE STATEWIDE CYBERSECURITY MASTER PLAN DEVELOPED
 12 UNDER SUBSECTION (A) OF THIS SECTION WITHOUT THE NEED FOR THE
 13 DEPARTMENT TO OPERATE A CHARGE-BACK MODEL FOR CYBERSECURITY
 14 SERVICES PROVIDED TO OTHER UNITS OF STATE GOVERNMENT OR UNITS OF LOCAL
 15 GOVERNMENT.

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

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

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

27 ~~3.5-305.~~

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

31 (1) ~~information technology policies and standards;~~

32 (2) ~~an information technology plan; and~~

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

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

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

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

9 (i) ~~the Secretary shall return the submissions to the governing~~
 10 ~~boards; and~~

11 (ii) ~~the governing boards shall revise the submissions as appropriate~~
 12 ~~and submit the revised policies, standards, and plans to the Secretary.~~

13 ~~[3.5-306.~~

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

16 ~~[3.5-307.] 3.5-306.~~

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

20 (2) A unit of State government other than a public institution of higher
 21 education ~~[may not make]~~ ~~SHALL SUBMIT REQUESTS FOR~~ expenditures for major
 22 information technology development projects OR CYBERSECURITY PROJECTS except as
 23 provided in [§ 3A-308] ~~§ 3.5-307~~ 3.5-308 of this subtitle.

24 (b) [(1)] The Secretary may review any information technology project OR
 25 CYBERSECURITY PROJECT for consistency with the master plan AND THE
 26 CYBERSECURITY MASTER PLAN.

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

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

1 (2) The Secretary shall determine if the value of the resources, services,
2 and property to be obtained by the State under the terms of any proposal submitted in
3 accordance with the provisions of paragraph (1) of this subsection equals or exceeds
4 \$100,000.

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

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

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

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

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

20 ~~[3.5 308.] 3.5 307.~~

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

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

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

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

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

33 ~~(f) With the advice of the Secretary of Budget and Management, expenditures for~~
34 ~~major information technology development projects shall be subject to the approval of the~~

1 ~~Secretary who shall approve expenditures only when those projects are consistent with~~
 2 ~~statewide plans, policies, and standards.~~

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

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

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

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

11 ~~2. a description of:~~

12 ~~A. the needs addressed by the project;~~

13 ~~B. the potential risks associated with the project;~~

14 ~~C. possible alternatives; and~~

15 ~~D. the scope and complexity of the project; and~~

16 ~~3. an estimate of:~~

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

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

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

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

22 ~~2. a description of:~~

23 ~~A. the needs addressed by the project;~~

24 ~~B. the potential risks associated with the project;~~

25 ~~C. possible alternatives;~~

26 ~~D. the scope and complexity of the project; and~~

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

3 ~~F. an estimate of:~~

4 ~~A. the total project cost; and~~

5 ~~B. the fund sources available.~~

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

8 ~~[3.5-309.] 3.5-308.~~

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

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

12 ~~(c) The Secretary:~~

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

14 ~~(2) subject to the provisions of § 2-201 of this article and [§ 3A-307] §~~
 15 ~~3.5-306 3.5-307 of this subtitle, may receive and accept contributions, grants, or gifts of~~
 16 ~~money or property.~~

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

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

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

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

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

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

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

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

1 (ii) ~~an information technology agreement involving resource~~
2 ~~sharing;~~

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

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

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

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

11 (ii) ~~have been abandoned; or~~

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

13 (6) ~~any investment earnings; and~~

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

15 (f) ~~The Fund does not include any money:~~

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

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

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

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

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

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

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

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

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

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

9 (i) The Fund may be used:

10 (1) for major information technology development projects;

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

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

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

17 ~~(1) educationally related information technology projects;~~

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

20 ~~(3) information technology projects, including:~~

21 ~~(i) pilots; and~~

22 ~~(ii) prototypes.~~

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

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

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

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

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

10 ~~(2) The report shall include:~~

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

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

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

19 ~~1. the status of the project;~~

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

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

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

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

28 ~~(n) On or before January 15 of each year, for each major information technology~~
 29 ~~development project currently in development or for which operations and maintenance~~
 30 ~~funding is being provided in accordance with subsection (i)(3) of this section, subject to §~~
 31 ~~2-1257 of the State Government Article, the Secretary shall provide a summary report to~~
 32 ~~the Department of Legislative Services with the most up-to-date project information~~
 33 ~~including:~~

34 ~~(1) project status;~~

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

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

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

~~[3A-310.] 3.5-309.~~

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

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

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

~~[3.5-311.] 3.5-310.~~

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

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

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

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

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

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

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

~~(ii) if the information technology does not meet the nonvisual access standards, the Secretary, or the Secretary's designee, will notify the vendor in writing that~~

~~the vendor, at the vendor's own expense, has 12 months after the date of the notification to modify the information technology in order to meet the nonvisual access standards; and~~

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

~~1. may be subject to a civil penalty of:~~

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

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

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

~~(b) (1) Except as provided in paragraph (2) of this subsection, the nonvisual access clause required under subsection (a) of this section shall be included in each invitation for bids or request for proposals and in each procurement contract or modification or renewal of a contract issued under Title 13 of this article, without regard to the method chosen under Title 13, Subtitle 1 of this article for the purchase of new or upgraded information technology and information technology services.~~

~~(2) Except as provided in subsection (a)(4) of this section, the nonvisual access clause required under paragraph (1) of this subsection is not required if:~~

~~(i) the information technology is not available with nonvisual access because the essential elements of the information technology are visual and nonvisual equivalence cannot be developed; or~~

~~(ii) the cost of modifying the information technology for compatibility with software and hardware for nonvisual access would increase the price of the procurement by more than 15%.~~

~~[3.5 312.] 3.5 311.~~

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

~~[3.5 313.] 3.5 312.~~

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

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

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

3 ~~(ii) "Payee" does not include:~~

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

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

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

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

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

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

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

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

18 ~~(3) the amount of a payment; and~~

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

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

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

22 ~~(2) search by the following data fields:~~

23 ~~(i) a payee receiving a payment;~~

24 ~~(ii) an agency making a payment; and~~

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

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

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

3 ~~(g) This section shall be known and may be cited as the “Maryland Funding~~
 4 ~~Accountability and Transparency Act”.~~

5 ~~[3.5-314.] 3.5-313.~~

6 ~~(a) In this section, “security sensitive data” means information that is protected~~
 7 ~~against unwarranted disclosure.~~

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

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

11 ~~(2) establish annual security overview training or refresher security~~
 12 ~~training for each employee who handles security sensitive data as part of the employee’s~~
 13 ~~duties.~~

14 3.5-401.

15 (a) The Department shall:

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

18 **(2) TO ADDRESS PREPAREDNESS AND RESPONSE CAPABILITIES OF**
 19 **LOCAL JURISDICTIONS, ~~COORDINATE~~ ASSIST WITH THE PROCUREMENT OF**
 20 **MANAGED CYBERSECURITY SERVICES ~~PROCURED~~ BY LOCAL GOVERNMENTS WITH**
 21 **STATE FUNDING;**

22 **[(2)] (3)** acquire and manage common user telecommunication
 23 equipment, systems, or services and charge units of State government for their
 24 proportionate share of the costs of installation, maintenance, and operation of the common
 25 user telecommunication equipment, systems, or services;

26 **[(3)] (4)** promote compatibility of telecommunication systems by
 27 developing policies, procedures, and standards for the [acquisition and] use of
 28 telecommunication equipment, systems, and services by units of State government;

29 **[(4)] (5)** coordinate State government telecommunication systems and
 30 services by reviewing requests by units of State government for, **AND, ON REQUEST BY A**
 31 **UNIT, ACQUIRING ON BEHALF OF ~~UNITS~~ A UNIT OF STATE GOVERNMENT,**
 32 telecommunication equipment, systems, or services;

1 ~~[(5)] (6)~~ advise units of State government about [planning, acquisition,]
2 **PLANNING** and operation of telecommunication equipment, systems, or services; and

3 ~~[(6)] (7)~~ provide radio frequency coordination for State and local
4 governments in accordance with regulations of the Federal Communications Commission.

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

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

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

14 **(II) BY A UNIT OF STATE GOVERNMENT THAT IS LESS THAN**
15 **\$50,000 FOR SYSTEMS OR DEVICES THAT WILL CONNECT TO STATE**
16 **TELECOMMUNICATION EQUIPMENT, SYSTEMS, OR SERVICES.**

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

22 ~~3.5-404.~~

23 ~~(a) The General Assembly declares that:~~

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

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

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

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

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

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

~~(2) The network shall consist of:~~

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

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

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

~~(D) ON OR BEFORE DECEMBER 1 EACH YEAR, EACH UNIT OF THE LEGISLATIVE OR JUDICIAL BRANCH OF STATE GOVERNMENT AND ANY DIVISION OF THE UNIVERSITY SYSTEM OF MARYLAND THAT USE THE NETWORK ESTABLISHED UNDER SUBSECTION (B) OF THIS SECTION SHALL CERTIFY TO THE DEPARTMENT THAT THE UNIT OR DIVISION IS IN COMPLIANCE WITH THE DEPARTMENT'S MINIMUM SECURITY STANDARDS.~~

3.5-405.

(A) ON OR BEFORE DECEMBER 1 EACH YEAR, EACH UNIT OF STATE GOVERNMENT SHALL:

(1) COMPLETE A CYBERSECURITY PREPAREDNESS ASSESSMENT AND REPORT THE RESULTS OF ANY CYBERSECURITY PREPAREDNESS ASSESSMENTS PERFORMED IN THE PRIOR YEAR TO THE OFFICE OF SECURITY MANAGEMENT IN ACCORDANCE WITH GUIDELINES DEVELOPED BY THE OFFICE; AND

(2) SUBMIT A REPORT TO THE GOVERNOR AND THE OFFICE OF SECURITY MANAGEMENT THAT INCLUDES:

(I) AN INVENTORY OF ALL INFORMATION SYSTEMS AND APPLICATIONS USED OR MAINTAINED BY THE UNIT;

(II) A FULL DATA INVENTORY OF THE UNIT;

1 **(III) A LIST OF ALL CLOUD OR STATISTICAL ANALYSIS SYSTEM**
2 **SOLUTIONS USED BY THE UNIT;**

3 **(IV) A LIST OF ALL PERMANENT AND TRANSIENT VENDOR**
4 **INTERCONNECTIONS THAT ARE IN PLACE;**

5 **(V) THE NUMBER OF UNIT EMPLOYEES WHO HAVE RECEIVED**
6 **CYBERSECURITY TRAINING;**

7 **(VI) THE TOTAL NUMBER OF UNIT EMPLOYEES WHO USE THE**
8 **NETWORK;**

9 **(VII) THE NUMBER OF INFORMATION TECHNOLOGY STAFF**
10 **POSITIONS, INCLUDING VACANCIES;**

11 **(VIII) THE NUMBER OF NONINFORMATION TECHNOLOGY STAFF**
12 **POSITIONS, INCLUDING VACANCIES;**

13 **(IX) THE UNIT'S INFORMATION TECHNOLOGY BUDGET,**
14 **ITEMIZED TO INCLUDE THE FOLLOWING CATEGORIES:**

- 15 1. **SERVICES;**
- 16 2. **EQUIPMENT;**
- 17 3. **APPLICATIONS;**
- 18 4. **PERSONNEL;**
- 19 5. **SOFTWARE LICENSING;**
- 20 6. **DEVELOPMENT;**
- 21 7. **NETWORK PROJECTS;**
- 22 8. **MAINTENANCE; AND**
- 23 9. **CYBERSECURITY;**

24 **(X) ANY MAJOR INFORMATION TECHNOLOGY INITIATIVES TO**
25 **MODERNIZE THE UNIT'S INFORMATION TECHNOLOGY SYSTEMS OR IMPROVE**
26 **CUSTOMER ACCESS TO STATE AND LOCAL SERVICES;**

1 (XI) THE UNIT'S PLANS FOR FUTURE FISCAL YEARS TO
2 IMPLEMENT THE UNIT'S INFORMATION TECHNOLOGY GOALS;

3 (XII) COMPLIANCE WITH TIMELINES AND METRICS PROVIDED IN
4 THE DEPARTMENT'S MASTER PLAN; AND

5 (XIII) ANY OTHER KEY PERFORMANCE INDICATORS REQUIRED BY
6 THE OFFICE OF SECURITY MANAGEMENT TO TRACK COMPLIANCE OR CONSISTENCY
7 WITH THE DEPARTMENT'S STATEWIDE INFORMATION TECHNOLOGY MASTER PLAN.

8 (B) (1) EACH UNIT OF STATE GOVERNMENT SHALL REPORT A
9 CYBERSECURITY INCIDENT IN ACCORDANCE WITH PARAGRAPH (2) OF THIS
10 SUBSECTION TO THE STATE CHIEF INFORMATION SECURITY OFFICER.

11 (2) FOR THE REPORTING OF CYBERSECURITY INCIDENTS UNDER
12 PARAGRAPH (1) OF THIS SUBSECTION, THE STATE CHIEF INFORMATION SECURITY
13 OFFICER SHALL DETERMINE:

14 (I) THE CRITERIA FOR DETERMINING WHEN AN INCIDENT MUST
15 BE REPORTED;

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

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

18 3.5-406.

19 ~~(C)~~ ~~(1)~~ (A) THIS SUBSECTION DOES NOT APPLY TO MUNICIPAL
20 GOVERNMENTS.

21 ~~(2)~~ (B) ON OR BEFORE DECEMBER 1 EACH YEAR, EACH COUNTY
22 GOVERNMENT, LOCAL SCHOOL SYSTEM, AND LOCAL HEALTH DEPARTMENT SHALL:

23 ~~(1)~~ (1) IN CONSULTATION WITH THE LOCAL EMERGENCY
24 MANAGER, CREATE OR UPDATE A CYBERSECURITY PREPAREDNESS AND RESPONSE
25 PLAN AND SUBMIT THE PLAN TO THE OFFICE OF SECURITY MANAGEMENT FOR
26 APPROVAL;

27 ~~(1)~~ (2) COMPLETE A CYBERSECURITY PREPAREDNESS
28 ASSESSMENT AND REPORT THE RESULTS TO THE OFFICE OF SECURITY
29 MANAGEMENT IN ACCORDANCE WITH GUIDELINES DEVELOPED BY THE OFFICE;
30 AND

1 ~~(H)~~ (3) REPORT TO THE OFFICE OF SECURITY
2 MANAGEMENT:

3 ~~1.~~ (I) THE NUMBER OF INFORMATION TECHNOLOGY STAFF
4 POSITIONS, INCLUDING VACANCIES;

5 ~~2.~~ (II) THE ENTITY'S CYBERSECURITY BUDGET AND
6 OVERALL INFORMATION TECHNOLOGY BUDGET;

7 ~~3.~~ (III) THE NUMBER OF EMPLOYEES WHO HAVE
8 RECEIVED CYBERSECURITY TRAINING; AND

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

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

15 ~~(3) (H) (D) (1)~~ EACH ~~COUNTY~~ LOCAL GOVERNMENT, ~~LOCAL~~
16 ~~SCHOOL SYSTEM, AND LOCAL HEALTH DEPARTMENT~~ SHALL REPORT A
17 CYBERSECURITY INCIDENT, INCLUDING AN ATTACK ON A STATE SYSTEM BEING
18 USED BY THE LOCAL GOVERNMENT, TO THE APPROPRIATE LOCAL EMERGENCY
19 MANAGER, THE SECURITY OPERATIONS CENTER, AND TO THE MARYLAND JOINT
20 OPERATIONS CENTER IN THE DEPARTMENT OF EMERGENCY MANAGEMENT IN
21 ACCORDANCE WITH SUBPARAGRAPH (H) PARAGRAPH (2) OF THIS PARAGRAPH
22 SUBSECTION TO THE APPROPRIATE LOCAL EMERGENCY MANAGER.

23 ~~(H) (2)~~ FOR THE REPORTING OF CYBERSECURITY INCIDENTS
24 TO LOCAL EMERGENCY MANAGERS UNDER SUBPARAGRAPH (I) OF THIS PARAGRAPH,
25 THE STATE CHIEF INFORMATION SECURITY OFFICER SHALL DETERMINE:

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

28 ~~2.~~ (II) THE MANNER IN WHICH TO REPORT; AND

29 ~~3.~~ (III) THE TIME PERIOD WITHIN WHICH A REPORT
30 MUST BE MADE.

31 (3) THE MARYLAND JOINT OPERATIONS CENTER SHALL
32 IMMEDIATELY NOTIFY THE APPROPRIATE AGENCIES OF A CYBERSECURITY

1 INCIDENT REPORTED UNDER THIS PARAGRAPH THROUGH THE STATE SECURITY
 2 OPERATIONS CENTER.

3 ~~12-107.~~

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

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

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

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

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

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

14 SECTION 3. AND BE IT FURTHER ENACTED, That, as a key enabler of the
 15 Department of Information Technology's cybersecurity risk management strategy, on or
 16 before December 31, 2022, the Department shall complete the implementation of a
 17 governance, risk, and compliance module across the Executive Branch of State government
 18 that:

19 (1) has industry-standard capabilities;

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

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

24 ~~SECTION 4. AND BE IT FURTHER ENACTED, That, on the effective date of this~~
 25 ~~Act, the following shall be transferred to the Department of Information Technology:~~

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

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

1 ~~SECTION 5. AND BE IT FURTHER ENACTED, That all employees of a unit of the~~
 2 ~~Executive Branch of State government who are assigned more than 50% of the time to a~~
 3 ~~function related to information technology operations or cybersecurity for the unit on the~~
 4 ~~effective date of this Act shall, on the effective date of this Act, report to the Secretary of~~
 5 ~~Information Technology or the Secretary's designee.~~

6 ~~SECTION 6. AND BE IT FURTHER ENACTED, That any transaction affected by~~
 7 ~~the transfer of oversight of information technology operations or cybersecurity of a unit of~~
 8 ~~the Executive Branch of State government and validly entered into before the effective date~~
 9 ~~of this Act, and every right, duty, or interest flowing from it, remains valid after the~~
 10 ~~effective date of this Act and may be terminated, completed, consummated, or enforced~~
 11 ~~under the law.~~

12 ~~SECTION 7. AND BE IT FURTHER ENACTED, That all existing laws, regulations,~~
 13 ~~proposed regulations, standards and guidelines, policies, orders and other directives, forms,~~
 14 ~~plans, memberships, contracts, property, investigations, administrative and judicial~~
 15 ~~responsibilities, rights to sue and be sued, and all other duties and responsibilities~~
 16 ~~associated with information technology operations or cybersecurity of a unit of the~~
 17 ~~Executive Branch of State government prior to the effective date of this Act shall continue~~
 18 ~~and, as appropriate, be legal and binding on the Department of Information Technology~~
 19 ~~until completed, withdrawn, canceled, modified, or otherwise changed under the law.~~

20 SECTION ~~8.~~ 4. AND BE IT FURTHER ENACTED, That this Act shall take effect
 21 October 1, 2022.

Approved:

Governor.

Speaker of the House of Delegates.

President of the Senate.