

# SENATE BILL 812

S2, P1, P2

2lr1779  
CF 2lr1409

---

By: **Senator Hester**

Introduced and read first time: February 7, 2022

Assigned to: Education, Health, and Environmental Affairs

---

## A BILL ENTITLED

1 AN ACT concerning

2 **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 requiring the Secretary of Information Technology to develop and maintain a  
18 statewide cybersecurity master plan; requiring DoIT to develop and require basic  
19 security requirements to be included in certain contracts; requiring each unit of the  
20 Legislative or Judicial Branch of State government and any division of the  
21 University System of Maryland that uses a certain network to certify certain  
22 compliance to DoIT on or before a certain date each year; requiring each unit of the  
23 Executive Branch of State government and certain local entities to report certain  
24 cybersecurity incidents in a certain manner and under certain circumstances;  
25 establishing the Maryland Cybersecurity Coordinating Council; exempting meetings  
26 of the Council from the Open Meetings Act; requiring the Council to study aspects of  
27 the State's cybersecurity vulnerabilities and procurement potential, including  
28 partnerships with other states; requiring the Council to promote certain education  
29 and training opportunities; requiring DoIT to complete implementation of a certain  
30 governance, risk, and compliance module on or before a certain date; transferring

---

EXPLANATION: CAPITALS INDICATE MATTER ADDED TO EXISTING LAW.

[Brackets] indicate matter deleted from existing law.



- 1 certain appropriations, books and records, and employees to DoIT; and generally  
2 relating to State cybersecurity coordination.
- 3 BY renumbering  
4 Article – State Finance and Procurement  
5 Section 3A–101 through 3A–702, respectively, and the title “Title 3A. Department of  
6 Information Technology”  
7 to be Section 3.5–101 through 3.5–702, respectively, and the title “Title 3.5.  
8 Department of Information Technology”  
9 Annotated Code of Maryland  
10 (2021 Replacement Volume)
- 11 BY repealing and reenacting, with amendments,  
12 Article – Criminal Procedure  
13 Section 10–221(b)  
14 Annotated Code of Maryland  
15 (2018 Replacement Volume and 2021 Supplement)
- 16 BY repealing and reenacting, with amendments,  
17 Article – Health – General  
18 Section 21–2C–03(h)(2)(i)  
19 Annotated Code of Maryland  
20 (2019 Replacement Volume and 2021 Supplement)
- 21 BY repealing and reenacting, with amendments,  
22 Article – Human Services  
23 Section 7–806(a), (b)(1), (c)(1), (d)(1) and (2)(i), and (g)(1)  
24 Annotated Code of Maryland  
25 (2019 Replacement Volume and 2021 Supplement)
- 26 BY repealing and reenacting, with amendments,  
27 Article – Insurance  
28 Section 31–103(a)(2)(i) and (b)(2)  
29 Annotated Code of Maryland  
30 (2017 Replacement Volume and 2021 Supplement)
- 31 BY repealing and reenacting, with amendments,  
32 Article – Natural Resources  
33 Section 1–403(c)  
34 Annotated Code of Maryland  
35 (2018 Replacement Volume and 2021 Supplement)
- 36 BY adding to  
37 Article – Public Safety  
38 Section 14–104.1  
39 Annotated Code of Maryland  
40 (2018 Replacement Volume and 2021 Supplement)

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

7 BY adding to  
8 Article – State Finance and Procurement  
9 Section 3.5–2A–01 through 3.5–2A–07 to be under the new subtitle “Subtitle 2A.  
10 Office of Security Management”; and 3.5–405 and 12–107(b)(2)(i)12.  
11 Annotated Code of Maryland  
12 (2021 Replacement Volume)

13 BY repealing and reenacting, with amendments,  
14 Article – State Finance and Procurement  
15 Section 3.5–301(j), 3.5–302(c), 3.5–303, 3.5–305, 3.5–307 through 3.5–314, 3.5–401,  
16 and 3.5–404  
17 Annotated Code of Maryland  
18 (2021 Replacement Volume)  
19 (As enacted by Section 1 of this Act)

20 BY repealing  
21 Article – State Finance and Procurement  
22 Section 3.5–306  
23 Annotated Code of Maryland  
24 (2021 Replacement Volume)  
25 (As enacted by Section 1 of this Act)

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

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

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

38 **Article – Criminal Procedure**

1 10–221.

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

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

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

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

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

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

15 (i) accurate and complete; and

16 (ii) collected, reported, and disseminated in accordance with Subtitle  
17 1 of this title and this subtitle;

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

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

### 23 **Article – Health – General**

24 21–2C–03.

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

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

### 30 **Article – Human Services**

31 7–806.

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

4 (2) For fiscal year 2019 and each fiscal year thereafter, the program under  
5 [§ 3A–702] § 3.5–702 of the State Finance and Procurement Article shall be funded at an  
6 amount that:

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

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

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

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

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

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

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

23 (i) a surcharge to be paid by the subscribers to a communications  
24 service; and

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

26 (d) (1) The Secretary shall annually certify to the Public Service Commission  
27 the costs of the programs under § 7–804(a) of this subtitle, § 7–902(a) of this title, and [§  
28 3A–702] § 3.5–702 of the State Finance and Procurement Article to be paid by the  
29 Universal Service Trust Fund for the following fiscal year.

30 (2) (i) The Public Service Commission shall determine the surcharge  
31 for the following fiscal year necessary to fund the programs under § 7–804(a) of this subtitle,  
32 § 7–902(a) of this title, and [§ 3A–702] § 3.5–702 of the State Finance and Procurement  
33 Article.

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

#### Article – Insurance

31–103.

(a) The Exchange is subject to:

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

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

(b) The Exchange is not subject to:

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

#### Article – Natural Resources

1–403.

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

#### Article – Public Safety

14–104.1.

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

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

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

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

1           **(C) THE PURPOSE OF THE OFFICE IS TO:**

2                   **(1) IMPROVE LOCAL, REGIONAL, AND STATEWIDE CYBERSECURITY**  
3 **READINESS AND RESPONSE;**

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

6                   **(3) IN CONSULTATION WITH THE DEPARTMENT OF INFORMATION**  
7 **TECHNOLOGY, COORDINATE WITH POLITICAL SUBDIVISIONS, LOCAL AGENCIES,**  
8 **AND STATE AGENCIES ON THE IMPLEMENTATION OF CYBERSECURITY BEST**  
9 **PRACTICES;**

10                   **(4) COORDINATE WITH POLITICAL SUBDIVISIONS AND AGENCIES ON**  
11 **THE IMPLEMENTATION OF THE STATEWIDE MASTER PLAN DEVELOPED BY THE**  
12 **DEPARTMENT OF INFORMATION TECHNOLOGY UNDER TITLE 3.5, SUBTITLE 3 OF**  
13 **THE STATE FINANCE AND PROCUREMENT ARTICLE; AND**

14                   **(5) CONSULT WITH THE STATE CHIEF INFORMATION SECURITY**  
15 **OFFICER AND THE SECRETARY OF INFORMATION TECHNOLOGY TO CONNECT**  
16 **POLITICAL SUBDIVISIONS AND AGENCIES TO THE APPROPRIATE RESOURCES FOR**  
17 **ANY OTHER PURPOSE RELATED TO CYBERSECURITY READINESS AND RESPONSE.**

18           **(D) (1) THE HEAD OF THE OFFICE IS THE EXECUTIVE DIRECTOR, WHO**  
19 **SHALL BE APPOINTED BY THE DIRECTOR.**

20                   **(2) THE OFFICE OF SECURITY MANAGEMENT SHALL PROVIDE STAFF**  
21 **FOR THE OFFICE.**

22           **(E) (1) THE OFFICE SHALL ESTABLISH REGIONAL ASSISTANCE GROUPS**  
23 **TO DELIVER OR COORDINATE SUPPORT SERVICES TO POLITICAL SUBDIVISIONS,**  
24 **AGENCIES, OR REGIONS.**

25                   **(2) THE OFFICE MAY HIRE OR PROCURE REGIONAL COORDINATORS**  
26 **TO DELIVER OR COORDINATE THE SERVICES UNDER PARAGRAPH (1) OF THIS**  
27 **SUBSECTION.**

28                   **(3) THE OFFICE SHALL PROVIDE OR COORDINATE SUPPORT**  
29 **SERVICES UNDER PARAGRAPH (1) OF THIS SUBSECTION THAT INCLUDE:**

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

1 (II) PROVIDING TECHNICAL SERVICES FOR THE  
2 IMPLEMENTATION OF CYBERSECURITY BEST PRACTICES IN ACCORDANCE WITH  
3 SUBSECTION (C)(3) OF THIS SECTION;

4 (III) COMPLETING CYBERSECURITY RISK ASSESSMENTS;

5 (IV) DEVELOPING CYBER SCORECARDS AND REPORTS ON  
6 REGIONAL READINESS;

7 (V) CREATING AND UPDATING CYBERSECURITY DISRUPTION  
8 PLANS IN ACCORDANCE WITH SUBSECTION (C)(2) OF THIS SECTION; AND

9 (VI) CONDUCTING REGIONAL EXERCISES IN COORDINATION  
10 WITH THE NATIONAL GUARD, THE DEPARTMENT, THE DEPARTMENT OF  
11 INFORMATION TECHNOLOGY, LOCAL EMERGENCY MANAGERS, AND OTHER STATE  
12 AND LOCAL ENTITIES.

13 (F) (1) THE OFFICE SHALL PROVIDE REGULAR TRAINING  
14 OPPORTUNITIES FOR COUNTIES AND MUNICIPAL CORPORATIONS IN THE STATE.

15 (2) TRAINING OPPORTUNITIES OFFERED BY THE OFFICE SHALL:

16 (I) BE DESIGNED TO ENSURE STAFF FOR COUNTIES AND  
17 MUNICIPAL CORPORATIONS ARE CAPABLE OF COOPERATING EFFECTIVELY WITH  
18 THE DEPARTMENT IN THE EVENT OF A CYBERSECURITY EMERGENCY; AND

19 (II) INCORPORATE BEST PRACTICES AND GUIDELINES FOR  
20 STATE AND LOCAL GOVERNMENTS PROVIDED BY THE MULTI-STATE INFORMATION  
21 SHARING AND ANALYSIS CENTER AND THE CYBERSECURITY AND  
22 INFRASTRUCTURE SECURITY AGENCY.

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

27 **Article – State Finance and Procurement**

28 3.5-101.

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

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

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

4 **3.5-2A-01.**

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

7 (B) "COUNCIL" MEANS THE MARYLAND CYBERSECURITY COORDINATING  
8 COUNCIL.

9 (C) "OFFICE" MEANS THE OFFICE OF SECURITY MANAGEMENT.

10 **3.5-2A-02.**

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

12 **3.5-2A-03.**

13 (A) THE HEAD OF THE OFFICE IS THE STATE CHIEF INFORMATION  
14 SECURITY OFFICER.

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

16 (1) BE APPOINTED BY THE GOVERNOR WITH THE ADVICE AND  
17 CONSENT OF THE SENATE;

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

19 (3) BE SUPERVISED BY THE SECRETARY; AND

20 (4) SERVE AS THE CHIEF INFORMATION SECURITY OFFICER OF THE  
21 DEPARTMENT.

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

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

27 (II) THE DIRECTOR OF LOCAL CYBERSECURITY SHALL WORK  
28 IN COORDINATION WITH THE MARYLAND DEPARTMENT OF EMERGENCY

1 **MANAGEMENT TO PROVIDE TECHNICAL ASSISTANCE, COORDINATE RESOURCES,**  
2 **AND IMPROVE CYBERSECURITY PREPAREDNESS FOR UNITS OF LOCAL**  
3 **GOVERNMENT.**

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

6 **(II) THE DIRECTOR OF STATE CYBERSECURITY IS**  
7 **RESPONSIBLE FOR IMPLEMENTATION OF THIS SECTION WITH RESPECT TO UNITS OF**  
8 **STATE GOVERNMENT.**

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

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

13 **3.5-2A-04.**

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

15 **(1) THE DIRECTION, COORDINATION, AND IMPLEMENTATION OF THE**  
16 **OVERALL CYBERSECURITY STRATEGY AND POLICY FOR UNITS OF STATE**  
17 **GOVERNMENT; AND**

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

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

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

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

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

1           **(4) ESTABLISH SECURITY REQUIREMENTS FOR INFORMATION AND**  
2 **INFORMATION SYSTEMS IN EACH CATEGORY;**

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

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

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

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

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

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

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

28           **(12) REVIEW AND CERTIFY LOCAL CYBERSECURITY PREPAREDNESS**  
29 **AND RESPONSE PLANS;**

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

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

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

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

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

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

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

12           **(3) DEVELOP APPROPRIATE REPORTS ON LOCAL CYBERSECURITY**  
13 **PREPAREDNESS.**

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

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

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

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

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

1           **(2) A COMPILATION AND ANALYSIS OF THE DATA FROM THE**  
2 **INFORMATION CONTAINED IN THE REPORTS RECEIVED BY THE OFFICE UNDER §**  
3 **3.5-405 OF THIS TITLE, INCLUDING:**

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

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

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

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

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

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

22           **(VII) ANY ADDITIONAL RECOMMENDATIONS FOR IMPROVING**  
23 **STATE AND LOCAL CYBERSECURITY PREPAREDNESS.**

24 **3.5-2A-05.**

25           **(A) THERE IS A MARYLAND CYBERSECURITY COORDINATING COUNCIL.**

26           **(B) THE COUNCIL CONSISTS OF THE FOLLOWING MEMBERS:**

27           **(1) THE SECRETARY OF BUDGET AND MANAGEMENT, OR THE**  
28 **SECRETARY'S DESIGNEE;**

29           **(2) THE SECRETARY OF GENERAL SERVICES, OR THE SECRETARY'S**  
30 **DESIGNEE;**

31           **(3) THE SECRETARY OF HEALTH, OR THE SECRETARY'S DESIGNEE;**

1           (4) THE SECRETARY OF HUMAN SERVICES, OR THE SECRETARY'S  
2 DESIGNEE;

3           (5) THE SECRETARY OF PUBLIC SAFETY AND CORRECTIONAL  
4 SERVICES, OR THE SECRETARY'S DESIGNEE;

5           (6) THE SECRETARY OF TRANSPORTATION, OR THE SECRETARY'S  
6 DESIGNEE;

7           (7) THE SECRETARY OF DISABILITIES, OR THE SECRETARY'S  
8 DESIGNEE;

9           (8) THE STATE CHIEF INFORMATION SECURITY OFFICER;

10           (9) THE ADJUTANT GENERAL OF THE MARYLAND NATIONAL GUARD,  
11 OR THE ADJUTANT GENERAL'S DESIGNEE;

12           (10) THE SECRETARY OF EMERGENCY MANAGEMENT, OR THE  
13 SECRETARY'S DESIGNEE;

14           (11) THE SUPERINTENDENT OF STATE POLICE, OR THE  
15 SUPERINTENDENT'S DESIGNEE;

16           (12) THE DIRECTOR OF THE GOVERNOR'S OFFICE OF HOMELAND  
17 SECURITY, OR THE DIRECTOR'S DESIGNEE;

18           (13) THE EXECUTIVE DIRECTOR OF THE DEPARTMENT OF  
19 LEGISLATIVE SERVICES, OR THE EXECUTIVE DIRECTOR'S DESIGNEE;

20           (14) ONE REPRESENTATIVE OF THE ADMINISTRATIVE OFFICE OF THE  
21 COURTS;

22           (15) THE CHANCELLOR OF THE UNIVERSITY SYSTEM OF MARYLAND,  
23 OR THE CHANCELLOR'S DESIGNEE; AND

24           (16) ANY OTHER STAKEHOLDER THAT THE STATE CHIEF  
25 INFORMATION SECURITY OFFICER DEEMS APPROPRIATE.

26           (C) THE CHAIR OF THE COUNCIL IS THE STATE CHIEF INFORMATION  
27 SECURITY OFFICER.

28           (D) (1) THE COUNCIL SHALL MEET AT LEAST QUARTERLY AT THE  
29 REQUEST OF THE CHAIR.

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

3           **(E) THE COUNCIL SHALL:**

4           **(1) PROVIDE ADVICE AND RECOMMENDATIONS TO THE STATE CHIEF**  
5 **INFORMATION SECURITY OFFICER REGARDING:**

6                   **(I) THE STRATEGY AND IMPLEMENTATION OF CYBERSECURITY**  
7 **INITIATIVES AND RECOMMENDATIONS; AND**

8                   **(II) BUILDING AND SUSTAINING THE CAPABILITY OF THE STATE**  
9 **TO IDENTIFY AND MITIGATE CYBERSECURITY RISK AND RESPOND TO AND RECOVER**  
10 **FROM CYBERSECURITY-RELATED INCIDENTS.**

11           **(2) USE THE ANALYSIS COMPILED BY THE OFFICE UNDER §**  
12 **3.5-2A-04(E)(2) OF THIS SUBTITLE TO PRIORITIZE CYBERSECURITY RISK ACROSS**  
13 **THE EXECUTIVE BRANCH OF STATE GOVERNMENT AND MAKE CORRESPONDING**  
14 **RECOMMENDATIONS FOR SECURITY INVESTMENTS IN THE GOVERNOR'S ANNUAL**  
15 **BUDGET.**

16           **(F) IN CARRYING OUT THE DUTIES OF THE COUNCIL, THE COUNCIL MAY**  
17 **CONSULT WITH OUTSIDE EXPERTS, INCLUDING EXPERTS IN THE PRIVATE SECTOR,**  
18 **GOVERNMENT AGENCIES, AND INSTITUTIONS OF HIGHER EDUCATION.**

19 **3.5-2A-06.**

20           **THE COUNCIL SHALL STUDY THE SECURITY AND FINANCIAL IMPLICATIONS OF**  
21 **EXECUTING PARTNERSHIPS WITH OTHER STATES TO PROCURE INFORMATION**  
22 **TECHNOLOGY AND CYBERSECURITY PRODUCTS AND SERVICES, INCLUDING THE**  
23 **IMPLICATIONS FOR POLITICAL SUBDIVISIONS OF THE STATE.**

24 **3.5-2A-07.**

25           **THE COUNCIL SHALL:**

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

29           **(2) UTILIZE RELATIONSHIPS WITH INSTITUTIONS OF HIGHER**  
30 **EDUCATION TO ADVERTISE CYBERSECURITY CAREERS AND JOB POSITIONS**  
31 **AVAILABLE IN STATE OR LOCAL GOVERNMENT; AND**

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

3 3.5–301.

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

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

9 3.5–302.

10           (c) Notwithstanding any other provision of law, except as provided in subsection  
11 (a) of this section and **[§§ 3A–307(a)(2), 3A–308, and 3A–309] §§ 3.5–306(A)(2), 3.5–307,**  
12 **AND 3.5–308** of this subtitle, this subtitle applies to all units of the Executive Branch of  
13 State government including public institutions of higher education other than Morgan  
14 State University, the University System of Maryland, St. Mary’s College of Maryland, and  
15 Baltimore City Community College.

16 3.5–303.

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

18                   (1) developing, maintaining, revising, and enforcing information  
19 technology policies, procedures, and standards;

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

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

24                   (4) developing and maintaining a statewide information technology master  
25 plan that will:

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

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

1 (iii) consider interstate transfers as a result of federal legislation and  
2 regulation;

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

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

9 [(vi)] (v) include standards to assure nonvisual access to the  
10 information and services made available to the public over the Internet;

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

14 **(6) DEVELOPING AND MAINTAINING A STATEWIDE CYBERSECURITY  
15 MASTER PLAN THAT WILL:**

16 **(I) CENTRALIZE THE MANAGEMENT AND DIRECTION OF  
17 CYBERSECURITY STRATEGY WITHIN THE EXECUTIVE BRANCH OF STATE  
18 GOVERNMENT UNDER THE CONTROL OF THE DEPARTMENT; AND**

19 **(II) SERVE AS THE BASIS FOR BUDGET ALLOCATIONS FOR  
20 CYBERSECURITY PREPAREDNESS FOR THE EXECUTIVE BRANCH OF STATE  
21 GOVERNMENT;**

22 [(5)] (7) adopting by regulation and enforcing nonvisual access standards  
23 to be used in the procurement of information technology services by or on behalf of units of  
24 State government in accordance with subsection (b) of this section;

25 [(6)] (8) in consultation with the [Attorney General,] **MARYLAND  
26 CYBERSECURITY COORDINATING COUNCIL**, advising and overseeing a consistent  
27 cybersecurity strategy for units of State government, including institutions under the  
28 control of the governing boards of the public institutions of higher education;

29 [(7)] (9) advising and consulting with the Legislative and Judicial  
30 branches of State government regarding a cybersecurity strategy; and

31 [(8)] (10) in consultation with the [Attorney General,] **MARYLAND  
32 CYBERSECURITY COORDINATING COUNCIL**, developing guidance on consistent  
33 cybersecurity strategies for counties, municipal corporations, school systems, and all other  
34 political subdivisions of the State.

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

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

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

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

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

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

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

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

19 2. for information technology procured by a State unit on or  
20 after January 1, 2020, enforce the nonvisual access clause developed under [§ 3A-311] §  
21 **3.5-310** of this subtitle, including the enforcement of the civil penalty described in [§  
22 3A-311(a)(2)(iii)1] **§ 3.5-310(A)(2)(III)1** of this subtitle.

23 **(D) (1) THE GOVERNOR SHALL INCLUDE AN APPROPRIATION IN THE**  
24 **ANNUAL BUDGET BILL IN AN AMOUNT NECESSARY TO COVER THE COSTS OF**  
25 **IMPLEMENTING THE STATEWIDE CYBERSECURITY MASTER PLAN DEVELOPED**  
26 **UNDER SUBSECTION (A) OF THIS SECTION WITHOUT THE NEED FOR THE**  
27 **DEPARTMENT TO OPERATE A CHARGE-BACK MODEL FOR CYBERSECURITY**  
28 **SERVICES PROVIDED TO OTHER UNITS OF STATE GOVERNMENT OR UNITS OF LOCAL**  
29 **GOVERNMENT.**

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

1                   **(I) SPECIFIC INFORMATION ON THE INFORMATION**  
2 **TECHNOLOGY BUDGET AND CYBERSECURITY BUDGET THAT THE GOVERNOR HAS**  
3 **SUBMITTED TO THE GENERAL ASSEMBLY FOR THE UPCOMING FISCAL YEAR; AND**

4                   **(II) HOW THE BUDGETS LISTED UNDER ITEM (I) OF THIS**  
5 **PARAGRAPH COMPARE TO THE ANNUAL OVERVIEW OF THE U.S. PRESIDENT'S**  
6 **BUDGET SUBMISSION ON INFORMATION TECHNOLOGY AND CYBERSECURITY TO**  
7 **CONGRESS CONDUCTED BY THE U.S. OFFICE OF MANAGEMENT AND BUDGET.**

8 3.5–305.

9           (a) [Except as provided in subsection (b) of this section, in accordance with  
10 guidelines established by the Secretary, each unit of State government shall develop and  
11 submit to the Secretary:

12                   (1) information technology policies and standards;

13                   (2) an information technology plan; and

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

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

19                   **[(2)] (B)** If the Secretary finds that the submissions required under this  
20 **[subsection] SECTION** are consistent with the master plan, the Secretary shall incorporate  
21 those submissions into the master plan.

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

24                           (i) the Secretary shall return the submissions to the governing  
25 boards; and

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

28 **[3.5–306.**

29 Information technology of each unit of State government shall be consistent with the  
30 master plan.]

31 **[3.5–307.] 3.5–306.**

1 (a) (1) [A unit of State government] **THE DEPARTMENT** may not purchase,  
2 lease, or rent information technology **ON BEHALF OF A UNIT OF STATE GOVERNMENT**  
3 unless consistent with the master plan.

4 (2) A unit of State government other than a public institution of higher  
5 education [may not make] **SHALL SUBMIT REQUESTS FOR** expenditures for major  
6 information technology development projects except as provided in [**§ 3A-308**] **§ 3.5-307**  
7 of this subtitle.

8 (b) [(1)] The Secretary may review any information technology project for  
9 consistency with the master plan.

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

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

15 (2) The Secretary shall determine if the value of the resources, services,  
16 and property to be obtained by the State under the terms of any proposal submitted in  
17 accordance with the provisions of paragraph (1) of this subsection equals or exceeds  
18 \$100,000.

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

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

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

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

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

34 [**3.5-308.**] **3.5-307.**

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

2 (b) In submitting its information technology project requests, a unit of State  
3 government shall designate projects which are major information technology development  
4 projects.

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

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

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

13 (f) With the advice of the Secretary of Budget and Management, expenditures for  
14 major information technology development projects shall be subject to the approval of the  
15 Secretary who shall approve expenditures only when those projects are consistent with  
16 statewide plans, policies, and standards.

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

20 (2) An approved systems development life cycle plan shall include  
21 submission of:

22 (i) a project planning request that details initial planning for the  
23 project, including:

24 1. the project title, appropriation code, and summary;

25 2. a description of:

26 A. the needs addressed by the project;

27 B. the potential risks associated with the project;

28 C. possible alternatives; and

29 D. the scope and complexity of the project; and

30 3. an estimate of:

- 1                   A.     the total costs required to complete through planning; and
- 2                   B.     the fund sources available to support planning costs; and
- 3                   (ii)    a project implementation request to begin full design,
- 4 development, and implementation of the project after the completion of planning, including:
- 5                   1.     the project title, appropriation code, and summary;
- 6                   2.     a description of:
- 7                   A.     the needs addressed by the project;
- 8                   B.     the potential risks associated with the project;
- 9                   C.     possible alternatives;
- 10                  D.     the scope and complexity of the project; and
- 11                  E.     how the project meets the goals of the statewide master
- 12 plan; and
- 13                  3.     an estimate of:
- 14                  A.     the total project cost; and
- 15                  B.     the fund sources available.

16                  (3)    The Secretary may approve funding incrementally, consistent with the

17 systems development life cycle plan.

18 **[3.5–309.] 3.5–308.**

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

20                  (b)    The purpose of the Fund is to support major information technology

21 development projects.

22                  (c)    The Secretary:

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

24                   (2)    subject to the provisions of § 2–201 of this article and **[§ 3A–307] §**

25 **3.5–306** of this subtitle, may receive and accept contributions, grants, or gifts of money or

26 property.

1 (d) (1) The Fund is a special, nonlapsing fund that is not subject to § 7–302 of  
2 this article.

3 (2) The State Treasurer shall hold the Fund separately and the  
4 Comptroller shall account for the Fund.

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

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

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

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

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

11 (i) the sale, lease, or exchange of communication sites,  
12 communication facilities, or communication frequencies for information technology  
13 purposes; or

14 (ii) an information technology agreement involving resource  
15 sharing;

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

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

20 (5) general funds appropriated for major information technology  
21 development projects of any unit of State government other than a public institution of  
22 higher education that:

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

24 (ii) have been abandoned; or

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

26 (6) any investment earnings; and

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

28 (f) The Fund does not include any money:

1 (1) received by the Department of Transportation, the Maryland  
2 Transportation Authority, Baltimore City Community College, or the Maryland Public  
3 Broadcasting Commission;

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

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

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

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

11 (2) an estimate of projected revenue from each of the sources specified in  
12 subsection (e) of this section for the fiscal year for which the State budget is submitted; and

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

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

16 (1) in accordance with an appropriation approved by the General Assembly  
17 in the annual State budget; or

18 (2) through an approved State budget amendment under Title 7, Subtitle  
19 2, Part II of this article, provided that a State budget amendment for any project not  
20 requested as part of the State budget submission or for any project for which the scope or  
21 cost has increased by more than 5% or \$250,000 shall be submitted to the budget  
22 committees allowing a 30-day period for their review and comment.

23 (i) The Fund may be used:

24 (1) for major information technology development projects;

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

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

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

31 (1) educationally related information technology projects;

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

3           (3) information technology projects, including:

4                   (i) pilots; and

5                   (ii) prototypes.

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

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

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

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

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

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

24           (2) The report shall include:

25                   (i) the financial status of the Fund and a summary of its operations  
26 for the preceding fiscal year;

27                   (ii) an accounting for the preceding fiscal year of all money from each  
28 of the revenue sources specified in subsection (e) of this section, including any expenditures  
29 made from the Fund; and

30                   (iii) for each project receiving money from the Fund in the preceding  
31 fiscal year and for each major information technology development project receiving  
32 funding from any source other than the Fund in the preceding fiscal year:

33                           1. the status of the project;



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

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

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

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

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

13 (ii) if the information technology does not meet the nonvisual access  
14 standards, the Secretary, or the Secretary's designee, will notify the vendor in writing that  
15 the vendor, at the vendor's own expense, has 12 months after the date of the notification to  
16 modify the information technology in order to meet the nonvisual access standards; and

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

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

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

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

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

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

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

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

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

7 **[3.5–312.] 3.5–311.**

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

10 **[3.5–313.] 3.5–312.**

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

12 (2) “Agency” includes a unit of State government that receives funds that  
13 are not appropriated in the annual budget bill.

14 (3) (i) “Payee” means any party who receives from the State an  
15 aggregate payment of \$25,000 in a fiscal year.

16 (ii) “Payee” does not include:

17 1. a State employee with respect to the employee’s  
18 compensation; or

19 2. a State retiree with respect to the retiree’s retirement  
20 allowance.

21 (4) “Searchable website” means a website created in accordance with this  
22 section that displays and searches State payment data.

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

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

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

29 (1) the name of a payee receiving a payment;

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

1 (3) the amount of a payment; and

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

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

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

5 (2) search by the following data fields:

6 (i) a payee receiving a payment;

7 (ii) an agency making a payment; and

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

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

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

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

15 **[3.5–314.] 3.5–313.**

16 (a) In this section, “security–sensitive data” means information that is protected  
17 against unwarranted disclosure.

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

20 (1) identify unit personnel who handle security–sensitive data; and

21 (2) establish annual security overview training or refresher security  
22 training for each employee who handles security–sensitive data as part of the employee’s  
23 duties.

24 3.5–401.

25 (a) The Department shall:

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

1           **(2) TO ADDRESS PREPAREDNESS AND RESPONSE CAPABILITIES OF**  
2 **LOCAL JURISDICTIONS, COORDINATE THE PROCUREMENT OF MANAGED**  
3 **CYBERSECURITY SERVICES PROCURED BY LOCAL GOVERNMENTS WITH STATE**  
4 **FUNDING;**

5           **[(2)] (3)** acquire and manage common user telecommunication  
6 equipment, systems, or services and charge units of State government for their  
7 proportionate share of the costs of installation, maintenance, and operation of the common  
8 user telecommunication equipment, systems, or services;

9           **[(3)] (4)** promote compatibility of telecommunication systems by  
10 developing policies, procedures, and standards for the [acquisition and] use of  
11 telecommunication equipment, systems, and services by units of State government;

12           **[(4)] (5)** coordinate State government telecommunication systems and  
13 services by reviewing requests by units of State government for, **AND ACQUIRING ON**  
14 **BEHALF OF UNITS OF STATE GOVERNMENT,** telecommunication equipment, systems, or  
15 services;

16           **[(5)] (6)** advise units of State government about [planning, acquisition,]  
17 **PLANNING** and operation of telecommunication equipment, systems, or services; and

18           **[(6)] (7)** provide radio frequency coordination for State and local  
19 governments in accordance with regulations of the Federal Communications Commission.

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

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

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

29                   **(II) BY A UNIT OF STATE GOVERNMENT THAT IS LESS THAN**  
30 **\$50,000 FOR SYSTEMS OR DEVICES THAT WILL CONNECT TO STATE**  
31 **TELECOMMUNICATION EQUIPMENT, SYSTEMS, OR SERVICES.**

32           **(2) THE SECURITY REQUIREMENTS DEVELOPED UNDER PARAGRAPH**  
33 **(1) OF THIS SUBSECTION SHALL BE CONSISTENT WITH A WIDELY RECOGNIZED**  
34 **SECURITY STANDARD, INCLUDING NATIONAL INSTITUTE OF STANDARDS AND**

1 **TECHNOLOGY SP 800–171, ISO27001, OR CYBERSECURITY MATURITY MODEL**  
2 **CERTIFICATION.**

3 3.5–404.

4 (a) The General Assembly declares that:

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

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

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

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

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

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

22 (2) The network shall consist of:

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

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

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

30 **(D) ON OR BEFORE DECEMBER 1 EACH YEAR, EACH UNIT OF THE**  
31 **LEGISLATIVE OR JUDICIAL BRANCH OF STATE GOVERNMENT AND ANY DIVISION OF**  
32 **THE UNIVERSITY SYSTEM OF MARYLAND THAT USE THE NETWORK ESTABLISHED**  
33 **UNDER SUBSECTION (B) OF THIS SECTION SHALL CERTIFY TO THE DEPARTMENT**

1 THAT THE UNIT OR DIVISION IS IN COMPLIANCE WITH THE DEPARTMENT'S MINIMUM  
2 SECURITY STANDARDS.

3 **3.5-405.**

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

6 (1) COMPLETE A CYBERSECURITY PREPAREDNESS ASSESSMENT AND  
7 REPORT THE RESULTS TO THE OFFICE OF SECURITY MANAGEMENT IN  
8 ACCORDANCE WITH GUIDELINES DEVELOPED BY THE OFFICE; AND

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

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

13 (II) A FULL DATA INVENTORY OF THE UNIT;

14 (III) A LIST OF ALL CLOUD OR STATISTICAL ANALYSIS SYSTEM  
15 SOLUTIONS USED BY THE UNIT;

16 (IV) A LIST OF ALL PERMANENT AND TRANSIENT VENDOR  
17 INTERCONNECTIONS THAT ARE IN PLACE;

18 (V) THE NUMBER OF UNIT EMPLOYEES WHO HAVE RECEIVED  
19 CYBERSECURITY TRAINING;

20 (VI) THE TOTAL NUMBER OF UNIT EMPLOYEES WHO USE THE  
21 NETWORK;

22 (VII) THE NUMBER OF INFORMATION TECHNOLOGY STAFF  
23 POSITIONS, INCLUDING VACANCIES;

24 (VIII) THE NUMBER OF NONINFORMATION TECHNOLOGY STAFF  
25 POSITIONS, INCLUDING VACANCIES;

26 (IX) THE UNIT'S INFORMATION TECHNOLOGY BUDGET,  
27 ITEMIZED TO INCLUDE THE FOLLOWING CATEGORIES:

28 1. SERVICES;

29 2. EQUIPMENT;

- 1                           **3. APPLICATIONS;**
- 2                           **4. PERSONNEL;**
- 3                           **5. SOFTWARE LICENSING;**
- 4                           **6. DEVELOPMENT;**
- 5                           **7. NETWORK PROJECTS;**
- 6                           **8. MAINTENANCE; AND**
- 7                           **9. CYBERSECURITY;**

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

11                           **(XI) THE UNIT'S PLANS FOR FUTURE FISCAL YEARS TO**  
12 **IMPLEMENT THE UNIT'S INFORMATION TECHNOLOGY GOALS;**

13                           **(XII) COMPLIANCE WITH TIMELINES AND METRICS PROVIDED IN**  
14 **THE DEPARTMENT'S MASTER PLAN; AND**

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

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

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

24                           **(I) THE CRITERIA FOR DETERMINING WHEN AN INCIDENT MUST**  
25 **BE REPORTED;**

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

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

1           **(C) (1) THIS SUBSECTION DOES NOT APPLY TO MUNICIPAL**  
2 **GOVERNMENTS.**

3           **(2) ON OR BEFORE DECEMBER 1 EACH YEAR, EACH COUNTY**  
4 **GOVERNMENT, LOCAL SCHOOL SYSTEM, AND LOCAL HEALTH DEPARTMENT SHALL:**

5                   **(I) IN CONSULTATION WITH THE LOCAL EMERGENCY**  
6 **MANAGER, CREATE OR UPDATE A CYBERSECURITY PREPAREDNESS AND RESPONSE**  
7 **PLAN AND SUBMIT THE PLAN TO THE OFFICE OF SECURITY MANAGEMENT FOR**  
8 **APPROVAL;**

9                   **(II) COMPLETE A CYBERSECURITY PREPAREDNESS**  
10 **ASSESSMENT AND REPORT THE RESULTS TO THE OFFICE OF SECURITY**  
11 **MANAGEMENT IN ACCORDANCE WITH GUIDELINES DEVELOPED BY THE OFFICE;**  
12 **AND**

13                   **(III) REPORT TO THE OFFICE OF SECURITY MANAGEMENT:**

14                   **1. THE NUMBER OF INFORMATION TECHNOLOGY STAFF**  
15 **POSITIONS, INCLUDING VACANCIES;**

16                   **2. THE ENTITY'S CYBERSECURITY BUDGET AND**  
17 **OVERALL INFORMATION TECHNOLOGY BUDGET;**

18                   **3. THE NUMBER OF EMPLOYEES WHO HAVE RECEIVED**  
19 **CYBERSECURITY TRAINING; AND**

20                   **4. THE TOTAL NUMBER OF EMPLOYEES WITH ACCESS TO**  
21 **THE ENTITY'S COMPUTER SYSTEMS AND DATABASES.**

22           **(3) (I) EACH COUNTY GOVERNMENT, LOCAL SCHOOL SYSTEM, AND**  
23 **LOCAL HEALTH DEPARTMENT SHALL REPORT A CYBERSECURITY INCIDENT IN**  
24 **ACCORDANCE WITH SUBPARAGRAPH (II) OF THIS PARAGRAPH TO THE APPROPRIATE**  
25 **LOCAL EMERGENCY MANAGER.**

26                   **(II) FOR THE REPORTING OF CYBERSECURITY INCIDENTS TO**  
27 **LOCAL EMERGENCY MANAGERS UNDER SUBPARAGRAPH (I) OF THIS PARAGRAPH,**  
28 **THE STATE CHIEF INFORMATION SECURITY OFFICER SHALL DETERMINE:**

29                   **1. THE CRITERIA FOR DETERMINING WHEN AN INCIDENT**  
30 **MUST BE REPORTED;**

31                   **2. THE MANNER IN WHICH TO REPORT; AND**

1                                   **3. THE TIME PERIOD WITHIN WHICH A REPORT MUST BE**  
2 **MADE.**

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. AND BE IT FURTHER ENACTED, That this Act shall take effect  
21 October 1, 2022.