

HOUSE BILL 1065

S2

3lr2778

By: **Delegates Kaiser, Bartlett, Feldmark, Kerr, and Kipke**

Introduced and read first time: February 10, 2023

Assigned to: Health and Government Operations

A BILL ENTITLED

1 AN ACT concerning

2 **State and Local Cybersecurity – Revisions**

3 FOR the purpose of establishing the Director of Cybersecurity Preparedness in the Cyber
4 Preparedness Unit of the Maryland Department of Emergency Management;
5 establishing certain duties of the Director; specifying the amount of a certain annual
6 appropriation made by the Governor to the Unit; establishing that the Deputy
7 Secretary of Information Technology is the State Chief Information Officer; requiring
8 a certain number of Position Identification Numbers to be created to assist the
9 Deputy Secretary; making the Office of Security Management an independent office
10 that functions in the Department of Information Technology and establishing that
11 the State Chief Information Security Officer in the Office reports to the Governor;
12 altering certain qualifications and duties of the State Chief Information Security
13 Officer; altering certain duties of the Office; establishing a certain exemption from
14 certain provisions of law for the State Board of Elections; altering certain duties of
15 the Secretary of Information Technology; altering the membership of the Modernize
16 Maryland Oversight Commission and providing for the appointment of cochairs of
17 the Commission; altering the duties of certain independent contractors hired by the
18 Department of Information Technology; establishing that certain information
19 related to cybersecurity incidents reported by local governments may not be used in
20 a certain manner; authorizing the Office to ensure compliance of an agency's
21 cybersecurity with cybersecurity standards in a certain manner; requiring a certain
22 independent contractor hired by the Department of Information Technology to
23 provide certain quarterly updates on its work; requiring a certain report by the
24 Commission to include a certain evaluation; requiring the Department of
25 Information Technology to hire an independent contractor to conduct a certain
26 review; and generally relating to State and local cybersecurity.

27 BY repealing and reenacting, with amendments,

28 Article – Public Safety

29 Section 14–104.1

30 Annotated Code of Maryland

EXPLANATION: CAPITALS INDICATE MATTER ADDED TO EXISTING LAW.

[Brackets] indicate matter deleted from existing law.



1 (2022 Replacement Volume)

2 BY repealing and reenacting, with amendments,
3 Article – State Finance and Procurement
4 Section 3.5–203(a), 3.5–2A–02, 3.5–2A–03, 3.5–2A–04(b)(11), 3.5–301(i), 3.5–302(a),
5 3.5–303(a) and (d), 3.5–316, 3.5–317(b)(1), and 3.5–407(d)
6 Annotated Code of Maryland
7 (2021 Replacement Volume and 2022 Supplement)

8 BY repealing and reenacting, without amendments,
9 Article – State Finance and Procurement
10 Section 3.5–301(a)
11 Annotated Code of Maryland
12 (2021 Replacement Volume and 2022 Supplement)

13 BY adding to
14 Article – State Finance and Procurement
15 Section 3.5–318
16 Annotated Code of Maryland
17 (2021 Replacement Volume and 2022 Supplement)

18 BY repealing and reenacting, with amendments,
19 Chapter 242 of the Acts of the General Assembly of 2022
20 Section 5 and 6

21 SECTION 1. BE IT ENACTED BY THE GENERAL ASSEMBLY OF MARYLAND,
22 That the Laws of Maryland read as follows:

23 **Article – Public Safety**

24 14–104.1.

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

26 (2) “Local government” includes local school systems, local school boards,
27 and local health departments.

28 (3) “Unit” means the Cyber Preparedness Unit.

29 (b) (1) There is a Cyber Preparedness Unit in the Department.

30 **(2) (I) THE HEAD OF THE UNIT IS THE DIRECTOR OF**
31 **CYBERSECURITY PREPAREDNESS.**

32 **(II) THE DIRECTOR SHALL WORK IN COORDINATION WITH THE**
33 **DIRECTOR OF LOCAL CYBERSECURITY IN THE OFFICE OF SECURITY MANAGEMENT**

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

3 **[(2)] (3)** In coordination with the State Chief Information Security
4 Officer, the Unit shall:

5 (i) support local governments in developing a vulnerability
6 assessment and cyber assessment, including providing local governments with the
7 resources and information on best practices to complete the assessments;

8 (ii) develop and regularly update an online database of cybersecurity
9 training resources for local government personnel, including technical training resources,
10 cybersecurity continuity of operations templates, consequence management plans, and
11 trainings on malware and ransomware detection;

12 (iii) assist local governments in:

13 1. the development of cybersecurity preparedness and
14 response plans;

15 2. implementing best practices and guidance developed by
16 the State Chief Information Security Officer; and

17 3. identifying and acquiring resources to complete
18 appropriate cybersecurity vulnerability assessments;

19 (iv) connect local governments to appropriate resources for any other
20 purpose related to cybersecurity preparedness and response;

21 (v) as necessary and in coordination with the National Guard, local
22 emergency managers, and other State and local entities, conduct regional cybersecurity
23 preparedness exercises; and

24 (vi) establish regional assistance groups to deliver and coordinate
25 support services to local governments, agencies, or regions.

26 **[(3)] (4)** The Unit shall support the Office of Security Management in the
27 Department of Information Technology during emergency response efforts.

28 (c) (1) Each local government shall report a cybersecurity incident, including
29 an attack on a State system being used by the local government, to the appropriate local
30 emergency manager and the State Security Operations Center in the Department of
31 Information Technology [and to the Maryland Joint Operations Center in the Department]
32 in accordance with paragraph (2) of this subsection.

33 (2) For the reporting of cybersecurity incidents under paragraph (1) of this
34 subsection, the State Chief Information Security Officer shall determine:

- 1 (i) the criteria for determining when an incident must be reported;
- 2 (ii) the manner in which to report; and
- 3 (iii) the time period within which a report must be made.

4 (3) The State Security Operations Center shall immediately notify
5 appropriate agencies of a cybersecurity incident reported under this subsection through the
6 State Security Operations Center.

7 (d) (1) Five Position Identification Numbers (PINs) shall be created for the
8 purpose of hiring staff to conduct the duties of the Maryland Department of Emergency
9 Management Cybersecurity Preparedness Unit.

10 (2) For fiscal year 2024 and each fiscal year thereafter, the Governor shall
11 include in the annual budget bill an appropriation [of at least:

- 12 (i) \$220,335 for 3 PINs for Administrator III positions; and
- 13 (ii) \$137,643 for 2 PINs for Administrator II positions] **SUFFICIENT**
14 **FOR THE POSITIONS CREATED UNDER PARAGRAPH (1) OF THIS SUBSECTION.**

15 **Article – State Finance and Procurement**

16 3.5–203.

17 (a) (1) With the approval of the Governor, the Secretary shall appoint a
18 Deputy Secretary.

19 (2) The Deputy Secretary:

- 20 (i) serves at the pleasure of the Secretary;
- 21 (ii) is entitled to the salary provided in the State budget; and
- 22 (iii) has the duties provided by law or delegated by the Secretary.

23 **(3) THE DEPUTY SECRETARY SHALL SERVE AS THE STATE CHIEF**
24 **INFORMATION OFFICER.**

25 **(4) SIX POSITION IDENTIFICATION NUMBERS SHALL BE CREATED**
26 **FOR THE PURPOSE OF HIRING STAFF TO ASSIST THE DEPUTY SECRETARY AND TO**
27 **CONDUCT BUSINESS RELATIONSHIP MANAGEMENT FOR AGENCIES AND LOCAL**
28 **GOVERNMENTS.**

1 3.5-2A-02.

2 (A) There is an Office of Security Management [within the Department].

3 (B) **THE OFFICE IS AN INDEPENDENT OFFICE THAT FUNCTIONS IN THE**
4 **DEPARTMENT.**

5 3.5-2A-03.

6 (a) The head of the Office is the State Chief Information Security Officer.

7 (b) The State Chief Information Security Officer shall:

8 (1) be appointed by the Governor with the advice and consent of the Senate;

9 (2) serve at the pleasure of the Governor; **AND**

10 (3) be supervised by the [Secretary; and

11 (4) serve as the chief information security officer of the Department]
12 **GOVERNOR.**

13 (c) An individual appointed as the State Chief Information Security Officer under
14 subsection (b) of this section shall:

15 (1) [at a minimum, hold a bachelor's degree;

16 (2)] hold appropriate information technology or cybersecurity certifications;

17 [(3)] **(2)** have experience:

18 (i) identifying, implementing, or assessing security controls;

19 (ii) in infrastructure, systems engineering, or cybersecurity;

20 (iii) managing highly technical security, security operations centers,
21 and incident response teams in a complex cloud environment and supporting multiple sites;
22 and

23 (iv) working with common information security management
24 frameworks;

25 [(4)] **(3)** have extensive knowledge of information technology and
26 cybersecurity field concepts, best practices, and procedures, with an understanding of
27 existing enterprise capabilities and limitations to ensure the secure integration and
28 operation of security networks and systems; and

1 ~~[(5)] (4)~~ have knowledge of current security regulations.

2 (d) The State Chief Information Security Officer shall:

3 (1) provide cybersecurity advice and recommendations to the Governor on
4 request; AND

5 (2) **DEVELOP AND MAINTAIN A STATEWIDE CYBERSECURITY**
6 **STRATEGY THAT WILL:**

7 (I) **CENTRALIZE THE MANAGEMENT AND DIRECTION OF**
8 **CYBERSECURITY STRATEGY WITHIN THE EXECUTIVE BRANCH OF STATE**
9 **GOVERNMENT UNDER THE CONTROL OF THE DEPARTMENT; AND**

10 (II) **SERVE AS THE BASIS FOR BUDGET ALLOCATIONS FOR**
11 **CYBERSECURITY PREPAREDNESS FOR THE EXECUTIVE BRANCH OF STATE**
12 **GOVERNMENT.**

13 (e) (1) (i) There is a Director of Local Cybersecurity, who shall be
14 appointed by the State Chief Information Security Officer.

15 (ii) The Director of Local Cybersecurity shall:

16 1. work in coordination with the Maryland Department of
17 Emergency Management to provide technical assistance, coordinate resources, and improve
18 cybersecurity preparedness for units of local government; AND

19 2. **IN CONSULTATION WITH THE MARYLAND**
20 **CYBERSECURITY COUNCIL, DEVELOP GUIDANCE ON CONSISTENT CYBERSECURITY**
21 **STRATEGIES FOR COUNTIES, MUNICIPAL CORPORATIONS, SCHOOL SYSTEMS, AND**
22 **ALL OTHER POLITICAL SUBDIVISIONS OF THE STATE.**

23 (2) (i) There is a Director of State Cybersecurity, who shall be
24 appointed by the State Chief Information Security Officer.

25 (ii) The Director of State Cybersecurity is responsible for
26 implementation of this section with respect to units of State government.

27 (iii) **IN CONSULTATION WITH THE MARYLAND CYBERSECURITY**
28 **COUNCIL, THE DIRECTOR OF STATE CYBERSECURITY SHALL ADVISE AND OVERSEE**
29 **A CONSISTENT CYBERSECURITY STRATEGY FOR UNITS OF STATE GOVERNMENT,**
30 **INCLUDING INSTITUTIONS UNDER THE CONTROL OF THE GOVERNING BOARDS OF**
31 **THE PUBLIC INSTITUTIONS OF HIGHER EDUCATION.**

1 (f) The Department shall provide the Office with sufficient staff to perform the
2 functions of this subtitle.

3 (G) **THE GOVERNOR SHALL INCLUDE AN APPROPRIATION IN THE ANNUAL**
4 **BUDGET BILL IN AN AMOUNT NECESSARY TO COVER THE COSTS OF IMPLEMENTING**
5 **THE STATEWIDE CYBERSECURITY STRATEGY DEVELOPED UNDER SUBSECTION (D)**
6 **OF THIS SECTION WITHOUT THE NEED FOR THE OFFICE TO OPERATE A**
7 **CHARGE-BACK MODEL FOR CYBERSECURITY SERVICES PROVIDED TO OTHER UNITS**
8 **OF STATE GOVERNMENT OR UNITS OF LOCAL GOVERNMENT.**

9 3.5-2A-04.

10 (b) The Office shall:

11 (11) develop and maintain information technology security policy,
12 standards, and guidance documents, consistent with [best practices developed by the] A
13 **WIDELY RECOGNIZED SECURITY STANDARD, INCLUDING:**

14 (I) National Institute of Standards and Technology (NIST)
15 **CYBERSECURITY FRAMEWORK, NIST 800-53, OR INTERNATIONAL ORGANIZATION**
16 **FOR STANDARDIZATION (ISO) ISO 27001; OR**

17 (II) **IN THE CASE OF ORGANIZATIONS HANDLING CONTROLLED**
18 **UNCLASSIFIED INFORMATION, NIST SP 800-171 OR THE CYBERSECURITY**
19 **MATURITY MODEL CERTIFICATION FROM THE U.S. DEPARTMENT OF DEFENSE;**

20 3.5-301.

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

22 (i) "Master plan" means the statewide information technology master plan [and
23 statewide cybersecurity strategy].

24 3.5-302.

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

27 (1) public institutions of higher education solely for academic or research
28 purposes;

29 (2) the Maryland Port Administration;

30 (3) the University System of Maryland;

1 (4) St. Mary's College of Maryland;

2 (5) Morgan State University;

3 (6) the Maryland Stadium Authority;

4 (7) Baltimore City Community College;

5 **(8) THE STATE BOARD OF ELECTIONS;**

6 **[(8)] (9)** the Legislative Branch of State government;

7 **[(9)] (10)** the Judicial Branch of State government;

8 **[(10)] (11)** the Office of the Attorney General;

9 **[(11)] (12)** the Comptroller; or

10 **[(12)] (13)** the State Treasurer.

11 3.5-303.

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

13 (1) developing, maintaining, revising, and enforcing information
14 technology policies, procedures, and standards;

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

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

19 (4) developing and maintaining a statewide information technology master
20 plan that will:

21 (i) centralize the management and direction of information
22 technology policy within the Executive Branch of State government under the control of the
23 Department;

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

26 (iii) consider interstate transfers as a result of federal legislation and
27 regulation;

1 (iv) ensure that the State information technology plan and related
2 policies and standards are consistent with State goals, objectives, and resources, and
3 represent a long-range vision for using information technology to improve the overall
4 effectiveness of State government;

5 (v) include standards to assure nonvisual access to the information
6 and services made available to the public over the Internet; and

7 (vi) allows a State agency to maintain the agency's own information
8 technology unit that provides for information technology services to support the mission of
9 the agency;

10 (5) [developing and maintaining a statewide cybersecurity strategy that
11 will:

12 (i) centralize the management and direction of cybersecurity
13 strategy within the Executive Branch of State government under the control of the
14 Department; and

15 (ii) serve as the basis for budget allocations for cybersecurity
16 preparedness for the Executive Branch of State government;

17 (6)] adopting by regulation and enforcing nonvisual access standards to be
18 used in the procurement of information technology services by or on behalf of units of State
19 government in accordance with subsection (b) of this section;

20 [(7) in consultation with the Maryland Cybersecurity Coordinating Council,
21 advising and overseeing a consistent cybersecurity strategy for units of State government,
22 including institutions under the control of the governing boards of the public institutions
23 of higher education;

24 (8)] (6) advising and consulting with the Legislative and Judicial
25 branches of State government regarding a cybersecurity strategy;

26 [(9) in consultation with the Maryland Cybersecurity Coordinating Council,
27 developing guidance on consistent cybersecurity strategies for counties, municipal
28 corporations, school systems, and all other political subdivisions of the State;

29 (10)] (7) upgrading information technology and cybersecurity-related
30 State government infrastructure; and

31 [(11)] (8) annually evaluating:

1 (i) the feasibility of units of State government providing public
2 services using artificial intelligence, machine learning, commercial cloud computer
3 services, device-as-a-service procurement models, and other emerging technologies; and

4 (ii) the development of data analytics capabilities to enable
5 data-driven policymaking by units of State government.

6 (d) [(1) The Governor shall include an appropriation in the annual budget bill
7 in an amount necessary to cover the costs of implementing the statewide cybersecurity
8 master plan developed under subsection (a) of this section without the need for the
9 Department to operate a charge-back model for cybersecurity services provided to other
10 units of State government or units of local government.

11 (2)] On or before January 31 each year, in a separate report or included
12 within a general budget report, the Governor shall submit a report in accordance with §
13 2-1257 of the State Government Article to the Senate Budget and Taxation Committee and
14 the House Appropriations Committee that includes:

15 [(i) (1) specific information on the information technology budget
16 and cybersecurity budget that the Governor has submitted to the General Assembly for the
17 upcoming fiscal year; and

18 [(ii) (2) how the budgets listed under item [(i) (1) of this
19 [paragraph] SUBSECTION compare to the annual overview of the U.S. President's budget
20 submission on information technology and cybersecurity to Congress conducted by the U.S.
21 Office of Management and Budget.

22 3.5-316.

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

24 (2) "Commission" means the Modernize Maryland Oversight Commission.

25 (3) "Critical system" means an information technology or cybersecurity
26 system that is severely outdated, as determined by the Department.

27 (b) There is an independent Modernize Maryland Oversight Commission.

28 (c) The purpose of the Commission is to:

29 (1) ensure the confidentiality, integrity, and availability of information
30 held by the State concerning State residents; and

31 (2) advise the Secretary and State Chief Information Security Officer on:

32 (i) the appropriate information technology and cybersecurity
33 investments and upgrades;

1 (ii) the funding sources for the appropriate information technology
2 and cybersecurity upgrades; and

3 (iii) future mechanisms for the procurement of appropriate
4 information technology and cybersecurity upgrades, including ways to increase the
5 efficiency of procurements made for information technology and cybersecurity upgrades.

6 (d) The Commission consists of the following members:

7 (1) the Secretary;

8 (2) the State Chief Information Security Officer;

9 (3) three chief information security officers representing different units of
10 State government, appointed by the Governor;

11 (4) one information technology modernization expert with experience in
12 the private sector, appointed by the Governor;

13 (5) one representative from the Maryland Chamber of Commerce with
14 knowledge of cybersecurity issues;

15 **(6) ONE REPRESENTATIVE FROM THE MARYLAND CHAMBER OF**
16 **COMMERCE WITH EXPERTISE IN INFORMATION TECHNOLOGY MODERNIZATION IN**
17 **THE PRIVATE SECTOR;**

18 **[(6)] (7) [two] THREE** individuals who are end users of State information
19 technology systems, appointed by the Governor;

20 **[(7)] (8) [one representative] TWO REPRESENTATIVES** from the
21 Cybersecurity Association of Maryland; **[and]**

22 **[(8)] (9)** one individual who is either an instructor or a professional in the
23 academic field of cybersecurity **OR INFORMATION TECHNOLOGY MODERNIZATION** at a
24 college or university in the State, appointed by the Governor; **AND**

25 **(10) ONE INDIVIDUAL WITH EXPERIENCE WORKING WITH THE STATE**
26 **BUDGET AND APPROPRIATIONS, APPOINTED JOINTLY BY THE PRESIDENT OF THE**
27 **SENATE AND THE SPEAKER OF THE HOUSE.**

28 (e) The cochairs of the Joint Committee on Cybersecurity, Information
29 Technology, and Biotechnology shall serve as advisory, nonvoting members of the
30 Commission.

1 **(F) THE COCHAIRS OF THE COMMISSION MAY APPOINT THREE ADDITIONAL**
2 **MEMBERS, AS NECESSARY, REPRESENTING THE PRIVATE SECTOR.**

3 **(G) (1) THE PRESIDENT OF THE SENATE AND THE SPEAKER OF THE**
4 **HOUSE SHALL JOINTLY APPOINT TWO COCHAIRS OF THE COMMISSION.**

5 **(2) UNTIL THE COCHAIRS ARE APPOINTED UNDER PARAGRAPH (1) OF**
6 **THIS SUBSECTION, THE COCHAIRS SHALL BE ELECTED FROM AMONG THE MEMBERS**
7 **OF THE COMMISSION WHO ARE NOT EMPLOYED BY STATE OR LOCAL GOVERNMENT.**

8 **[(f)] (H)** The Commission shall:

9 (1) advise the Secretary **AND THE STATE CHIEF INFORMATION**
10 **SECURITY OFFICER** on a strategic roadmap with a timeline and budget that will:

11 (i) require the updates and investments of critical information
12 technology and cybersecurity systems identified by the Commission in the first
13 recommendations reported under paragraph (2) of this subsection to be completed on or
14 before December 31, 2025; and

15 (ii) require all updates and investments of information technology
16 and cybersecurity to be made on or before December 31, 2030;

17 (2) make periodic recommendations on investments in State information
18 technology structures based on the assessments completed in accordance with the
19 framework developed in § 3.5–317 of this subtitle;

20 (3) review and provide recommendations on the Department's basic
21 security standards for use of the network established under § 3.5–404(b) of this title; and

22 (4) each year, in accordance with § 2–1257 of the State Government Article,
23 report its findings and recommendations to the Senate Budget and Taxation Committee,
24 the Senate **[Education, Health, and Environmental Affairs] EDUCATION, ENERGY, AND**
25 **THE ENVIRONMENT** Committee, the House Appropriations Committee, the House Health
26 and Government Operations Committee, and the Joint Committee on Cybersecurity,
27 Information Technology, and Biotechnology.

28 **[(g)] (I)** The report submitted under subsection **[(f)(4)] (H)(4)** of this section
29 may not contain information about the security of an information system.

30 3.5–317.

31 (b) (1) The Department shall hire independent contractors to:

1 (i) develop a framework for investments in technology, **INCLUDING**
2 **FOUNDATIONAL INFORMATION TECHNOLOGY PROJECTS THAT IMPACT MULTIPLE**
3 **UNITS OF STATE GOVERNMENT**; and

4 (ii) at least once every 2 years, in accordance with the framework,
5 assess the cybersecurity and information technology systems in each unit of State
6 government.

7 **3.5–318.**

8 **FOR FISCAL YEAR 2025 AND EACH FISCAL YEAR THEREAFTER, THE**
9 **GOVERNOR SHALL INCLUDE IN THE ANNUAL BUDGET BILL AN APPROPRIATION IN**
10 **AN AMOUNT THAT IS NOT LESS THAN 120% OF THE AGGREGATED AMOUNT**
11 **APPROPRIATED FOR INFORMATION TECHNOLOGY AND CYBERSECURITY**
12 **RESOURCES IN THE ANNUAL BUDGET BILL FOR THE PRIOR FISCAL YEAR FOR THE**
13 **DEDICATED PURPOSE ACCOUNT FOR CYBERSECURITY.**

14 **3.5–407.**

15 (d) (1) Each local government shall report a cybersecurity incident, including
16 an attack on a State system being used by the local government, to the appropriate local
17 emergency manager and the State Security Operations Center in the Department in
18 accordance with paragraph (2) of this subsection.

19 (2) For the reporting of cybersecurity incidents to local emergency
20 managers under subparagraph (i) of this paragraph, the State Chief Information Security
21 Officer shall determine:

22 (i) the criteria for determining when an incident must be reported;

23 (ii) the manner in which to report; and

24 (iii) the time period within which a report must be made.

25 (3) The State Security Operations Center shall immediately notify the
26 appropriate agencies of a cybersecurity incident reported under this subsection through the
27 State Security Operations Center.

28 **(4) INFORMATION REPORTED BY A LOCAL GOVERNMENT UNDER THIS**
29 **SUBSECTION MAY NOT BE USED BY THE STATE AS A BASIS FOR IMPOSING A FINE,**
30 **RESTRICTING FUNDING, OR OTHERWISE PENALIZING THE LOCAL GOVERNMENT.**

31 **Chapter 242 of the Acts of 2022**

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

1 (a) (1) On or before June 30, 2023, each agency in the Executive Branch of
2 State government shall certify to the Office of Security Management compliance with State
3 minimum cybersecurity standards established by the Department of Information
4 Technology.

5 (2) Except as provided in paragraph (3) of this subsection, certification
6 shall be reviewed by independent auditors, and any findings must be remediated.

7 (3) Certification for the Department of Public Safety and Correctional
8 Services and any State criminal justice agency shall be reviewed by the Office of Legislative
9 Audits, and any findings must be remediated.

10 (b) Except as provided in subsection (c) of this section, if an agency has not
11 remediated [any] **THE** findings pertaining to State cybersecurity standards found by the
12 independent audit required under subsection (a) of this section **TO BECOME COMPLIANT**
13 **WITH STATE MINIMUM CYBERSECURITY STANDARDS** by July 1, 2024, the Office of
14 Security Management shall ensure compliance of an agency's cybersecurity with
15 cybersecurity standards through a shared service agreement[, administrative privileges, or
16 access to Network Maryland] **TO ONBOARD THE AGENCY TO DEPARTMENT OF**
17 **INFORMATION TECHNOLOGY CYBERSECURITY SERVICES AND PROVIDE OFFICE OF**
18 **SECURITY MANAGEMENT STAFF ADMINISTRATIVE PRIVILEGES TO THE AGENCY'S**
19 **INFORMATION TECHNOLOGY ASSETS.**

20 (c) Subsection (b) of this section does not apply if a federal law or regulation
21 forbids the Office of Security Management from managing a specific system.

22 **SECTION 6. AND BE IT FURTHER ENACTED, That:**

23 (a) The Department of Information Technology shall hire a contractor to conduct
24 a performance and capacity assessment of the Department to:

25 (1) evaluate the Department's capacity to implement provisions of this Act;
26 and

27 (2) recommend additional resources necessary for the Department to
28 implement provisions of this title and meet future needs, including additional budget
29 appropriations, additional staff, altered contracting authority, and pay increases for staff.

30 (b) The contractor hired by the Department to complete the assessment and
31 report required by this section shall:

32 **(1) PROVIDE QUARTERLY UPDATES ON ITS WORK UNDER THIS**
33 **SECTION TO THE COCHAIRS OF THE JOINT COMMITTEE ON CYBERSECURITY,**
34 **INFORMATION TECHNOLOGY, AND BIOTECHNOLOGY;**

1 ~~[(1)] (2)~~ on or before December 1, 2023, submit an interim report of its
2 findings and recommendations to the Governor and, in accordance with § 2–1257 of the
3 State Government Article, the General Assembly; and

4 ~~[(2)] (3)~~ on or before December 1, 2024, submit a final report of its
5 findings and recommendations to the Governor and, in accordance with § 2–1257 of the
6 State Government Article, the General Assembly.

7 SECTION 2. AND BE IT FURTHER ENACTED, That the report submitted by the
8 Modernize Maryland Oversight Commission under § 3.5–316(h) of the State Finance and
9 Procurement Article, as enacted by Section 1 of this Act, in calendar year 2024 shall include
10 an evaluation of services provided by the Department of Information Technology and an
11 assessment of whether those services meet the needs of the agencies being served.

12 SECTION 3. AND BE IT FURTHER ENACTED, That, on or before November 1,
13 2023, the Modernize Maryland Oversight Commission shall report to the General
14 Assembly, in accordance with § 2–1257 of the State Government Article, recommendations
15 to improve the format for the Secretary of Information Technology to report on major
16 information technology development projects under § 3.5–309 of the State Finance and
17 Procurement Article to meet the needs for strategic planning and investment.

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

19 (1) the Department of Information Technology shall hire an independent
20 contractor to review the efficiency and effectiveness of foundational information technology
21 projects that impact multiple units of State government, including MDThink and OneStop,
22 according to the framework developed under § 3.5–317(b) of the State Finance and
23 Procurement Article, as enacted by Section 1 of this Act; and

24 (2) on or before November 1, 2023, the independent contractor hired under
25 item (1) of this section shall report its findings and recommendations to the General
26 Assembly, in accordance with § 2–1257 of the State Government Article.

27 SECTION 5. AND BE IT FURTHER ENACTED, That this Act shall take effect June
28 1, 2023.