

# SENATE BILL 868

S2

3lr2724

---

By: **Senator Hester**

Introduced and read first time: February 6, 2023

Assigned to: Education, Energy, and the Environment

---

## 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 State Chief  
7 Information Security Officer in the Office of Security Management reports to the  
8 Governor; altering certain qualifications and duties of the State Chief Information  
9 Security Officer; altering certain duties of the Office; altering certain duties of the  
10 Secretary of Information Technology; altering the membership of the Modernize  
11 Maryland Oversight Commission and providing for the appointment of the chair and  
12 vice chair of the Commission; altering the duties of certain independent contractors  
13 hired by the Department of Information Technology; establishing that certain  
14 information related to cybersecurity incidents reported by local governments may  
15 not be used in a certain manner; authorizing the Office to ensure compliance of an  
16 agency's cybersecurity with cybersecurity standards in a certain manner; requiring  
17 a certain independent contractor hired by the Department of Information Technology  
18 to provide certain quarterly updates on its work; requiring a certain report by the  
19 Commission to include a certain evaluation; requiring the Department of  
20 Information Technology to hire an independent contractor to conduct a certain  
21 review; and generally relating to State and local cybersecurity.

22 BY repealing and reenacting, with amendments,  
23 Article – Public Safety  
24 Section 14–104.1  
25 Annotated Code of Maryland  
26 (2022 Replacement Volume)

27 BY repealing and reenacting, without amendments,  
28 Article – State Finance and Procurement  
29 Section 3.5–2A–02 and 3.5–301(a)

---

EXPLANATION: CAPITALS INDICATE MATTER ADDED TO EXISTING LAW.

[Brackets] indicate matter deleted from existing law.



1 Annotated Code of Maryland  
2 (2021 Replacement Volume and 2022 Supplement)

3 BY repealing and reenacting, with amendments,  
4 Article – State Finance and Procurement  
5 Section 3.5–2A–03, 3.5–2A–04(b)(11), 3.5–301(i), 3.5–303(a) and (d), 3.5–316,  
6 3.5–317(b)(1), and 3.5–407(d)  
7 Annotated Code of Maryland  
8 (2021 Replacement Volume and 2022 Supplement)

9 BY adding to  
10 Article – State Finance and Procurement  
11 Section 3.5–318  
12 Annotated Code of Maryland  
13 (2021 Replacement Volume and 2022 Supplement)

14 BY repealing and reenacting, with amendments,  
15 Chapter 242 of the Acts of the General Assembly of 2022  
16 Section 5 and 6

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

19 **Article – Public Safety**

20 14–104.1.

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

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

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

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

26 **(2) (I) THE HEAD OF THE UNIT IS THE DIRECTOR OF**  
27 **CYBERSECURITY PREPAREDNESS.**

28 **(II) THE DIRECTOR SHALL WORK IN COORDINATION WITH THE**  
29 **DIRECTOR OF LOCAL CYBERSECURITY IN THE OFFICE OF SECURITY MANAGEMENT**  
30 **TO PROVIDE TECHNICAL ASSISTANCE, COORDINATE RESOURCES, AND IMPROVE**  
31 **CYBERSECURITY PREPAREDNESS FOR UNITS OF LOCAL GOVERNMENT.**

32 **[(2)] (3)** In coordination with the State Chief Information Security  
33 Officer, the Unit shall:

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

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

8 (iii) assist local governments in:

9 1. the development of cybersecurity preparedness and  
10 response plans;

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

13 3. identifying and acquiring resources to complete  
14 appropriate cybersecurity vulnerability assessments;

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

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

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

22 **[(3)] (4)** The Unit shall support the Office of Security Management in the  
23 Department of Information Technology during emergency response efforts.

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

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

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

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

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

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

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

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

10 (i) \$220,335 for 3 PINs for Administrator III positions; and

11 (ii) \$137,643 for 2 PINs for Administrator II positions] **SUFFICIENT**  
12 **FOR THE POSITIONS CREATED UNDER PARAGRAPH (1) OF THIS SUBSECTION.**

13 **Article – State Finance and Procurement**

14 3.5–2A–02.

15 There is an Office of Security Management within the Department.

16 3.5–2A–03.

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

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

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

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

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

22 (4) serve as the chief information security officer of the Department]

23 **GOVERNOR.**

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

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

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

1            **[(3)] (2)**        have experience:

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

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

4                            (iii)      managing highly technical security, security operations centers,  
5 and incident response teams in a complex cloud environment and supporting multiple sites;  
6 and

7                            (iv)      working with common information security management  
8 frameworks;

9            **[(4)] (3)**        have extensive knowledge of information technology and  
10 cybersecurity field concepts, best practices, and procedures, with an understanding of  
11 existing enterprise capabilities and limitations to ensure the secure integration and  
12 operation of security networks and systems; and

13            **[(5)] (4)**        have knowledge of current security regulations.

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

15                            (1)        provide cybersecurity advice and recommendations to the Governor on  
16 request; AND

17                            (2)        **DEVELOP AND MAINTAIN A STATEWIDE CYBERSECURITY**  
18 **STRATEGY THAT WILL:**

19                            (I)        **CENTRALIZE THE MANAGEMENT AND DIRECTION OF**  
20 **CYBERSECURITY STRATEGY WITHIN THE EXECUTIVE BRANCH OF STATE**  
21 **GOVERNMENT UNDER THE CONTROL OF THE DEPARTMENT; AND**

22                            (II)       **SERVE AS THE BASIS FOR BUDGET ALLOCATIONS FOR**  
23 **CYBERSECURITY PREPAREDNESS FOR THE EXECUTIVE BRANCH OF STATE**  
24 **GOVERNMENT.**

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

27                            (ii)       The Director of Local Cybersecurity shall:

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

1                                   **2. IN CONSULTATION WITH THE MARYLAND**  
2 **CYBERSECURITY COORDINATING COUNCIL, DEVELOP GUIDANCE ON CONSISTENT**  
3 **CYBERSECURITY STRATEGIES FOR COUNTIES, MUNICIPAL CORPORATIONS, SCHOOL**  
4 **SYSTEMS, AND ALL OTHER POLITICAL SUBDIVISIONS OF THE STATE.**

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

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

9                                   **(III) IN CONSULTATION WITH THE MARYLAND CYBERSECURITY**  
10 **COORDINATING COUNCIL, THE DIRECTOR OF STATE CYBERSECURITY SHALL**  
11 **ADVISE AND OVERSEE A CONSISTENT CYBERSECURITY STRATEGY FOR UNITS OF**  
12 **STATE GOVERNMENT, INCLUDING INSTITUTIONS UNDER THE CONTROL OF THE**  
13 **GOVERNING BOARDS OF THE PUBLIC INSTITUTIONS OF HIGHER EDUCATION.**

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

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

22 3.5-2A-04.

23                   (b) The Office shall:

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

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

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

33 3.5-301.

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

2 (i) “Master plan” means the statewide information technology master plan [and  
3 statewide cybersecurity strategy].

4 3.5–303.

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

6 (1) developing, maintaining, revising, and enforcing information  
7 technology policies, procedures, and standards;

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

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

12 (4) developing and maintaining a statewide information technology master  
13 plan that will:

14 (i) centralize the management and direction of information  
15 technology policy within the Executive Branch of State government under the control of the  
16 Department;

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

19 (iii) consider interstate transfers as a result of federal legislation and  
20 regulation;

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

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

27 (vi) allows a State agency to maintain the agency’s own information  
28 technology unit that provides for information technology services to support the mission of  
29 the agency;

30 (5) [developing and maintaining a statewide cybersecurity strategy that  
31 will:

1 (i) centralize the management and direction of cybersecurity  
2 strategy within the Executive Branch of State government under the control of the  
3 Department; and

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

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

9 **[(7)** in consultation with the Maryland Cybersecurity Coordinating Council,  
10 advising and overseeing a consistent cybersecurity strategy for units of State government,  
11 including institutions under the control of the governing boards of the public institutions  
12 of higher education;

13 **(8)] (6)** advising and consulting with the Legislative and Judicial  
14 branches of State government regarding a cybersecurity strategy;

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

18 **(10)] (7)** upgrading information technology and cybersecurity-related  
19 State government infrastructure; and

20 **[(11)] (8)** annually evaluating:

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

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

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

31 **(2)]** On or before January 31 each year, in a separate report or included  
32 within a general budget report, the Governor shall submit a report in accordance with §  
33 2-1257 of the State Government Article to the Senate Budget and Taxation Committee and  
34 the House Appropriations Committee that includes:



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

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

8 3.5–316.

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

10                    (2)    “Commission” means the Modernize Maryland Oversight Commission.

11                    (3)    “Critical system” means an information technology or cybersecurity  
12 system that is severely outdated, as determined by the Department.

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

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

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

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

18                            (i)    the appropriate information technology and cybersecurity  
19 investments and upgrades;

20                            (ii)   the funding sources for the appropriate information technology  
21 and cybersecurity upgrades; and

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

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

26                    (1)    the Secretary;

27                    (2)    the State Chief Information Security Officer;

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

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

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

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

8 **[(6)] (7)** two individuals who are end users of State information  
9 technology systems **AND WHO ARE NOT STATE EMPLOYEES**, appointed by the Governor;

10 **[(7)] (8)** one representative from the Cybersecurity Association of  
11 Maryland; [and]

12 **[(8)] (9)** one individual who is either an instructor or a professional in the  
13 academic field of cybersecurity **OR INFORMATION TECHNOLOGY MODERNIZATION** at a  
14 college or university in the State, appointed by the Governor; **AND**

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

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

21 **(F) THE CHAIR OF THE COMMISSION MAY APPOINT THREE ADDITIONAL**  
22 **MEMBERS, AS NECESSARY.**

23 **(G) THE CHAIR AND VICE CHAIR OF THE COMMISSION SHALL BE ELECTED**  
24 **FROM AMONG THE MEMBERS OF THE COMMISSION WHO ARE NOT EMPLOYED BY**  
25 **STATE OR LOCAL GOVERNMENT.**

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

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

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

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

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

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

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

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

16 3.5–317.

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

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

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

24 **3.5–318.**

25 **(A) FOR FISCAL YEAR 2025 AND EACH FISCAL YEAR THEREAFTER, THE**  
26 **GOVERNOR SHALL INCLUDE IN THE ANNUAL BUDGET BILL AN APPROPRIATION IN**  
27 **AN AMOUNT THAT IS NOT LESS THAN 20% OF THE AGGREGATED AMOUNT**  
28 **APPROPRIATED FOR INFORMATION TECHNOLOGY RESOURCES IN THE ANNUAL**  
29 **BUDGET BILL FOR THE PRIOR FISCAL YEAR FOR THE DEDICATED PURPOSE**  
30 **ACCOUNT FOR CYBERSECURITY.**

31 **(B) THE APPROPRIATIONS FOR EACH FISCAL YEAR UNDER SUBSECTION (A)**  
32 **OF THIS SECTION SHALL BE USED TO SUPPLEMENT, NOT SUPPLANT, ANY EXISTING**  
33 **FUNDS IN THE DEDICATED PURPOSE ACCOUNT FOR CYBERSECURITY THAT MAY**  
34 **HAVE ACCRUED FROM A PRIOR FISCAL YEAR.**

1 3.5–407.

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

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

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

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

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

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

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

## 18 Chapter 242 of the Acts of 2022

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

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

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

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

29 (b) Except as provided in subsection (c) of this section, if an agency has not  
30 remediated [any] **THE** findings pertaining to State cybersecurity standards found by the  
31 independent audit required under subsection (a) of this section **TO BECOME COMPLIANT**  
32 **WITH STATE MINIMUM CYBERSECURITY STANDARDS** by July 1, 2024, the Office of

1 Security Management shall ensure compliance of an agency's cybersecurity with  
2 cybersecurity standards through a shared service agreement[, administrative privileges, or  
3 access to Network Maryland] **TO ONBOARD THE AGENCY TO DEPARTMENT OF**  
4 **INFORMATION TECHNOLOGY CYBERSECURITY SERVICES AND PROVIDE OFFICE OF**  
5 **SECURITY MANAGEMENT STAFF ADMINISTRATIVE PRIVILEGES TO THE AGENCY'S**  
6 **INFORMATION TECHNOLOGY ASSETS.**

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

9 SECTION 6. AND BE IT FURTHER ENACTED, That:

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

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

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

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

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

22 **[(1)] (2)** on or before December 1, 2023, submit an interim report of its  
23 findings and recommendations to the Governor and, in accordance with § 2-1257 of the  
24 State Government Article, the General Assembly; and

25 **[(2)] (3)** on or before December 1, 2024, submit a final report of its  
26 findings and recommendations to the Governor and, in accordance with § 2-1257 of the  
27 State Government Article, the General Assembly.

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

33 SECTION 3. AND BE IT FURTHER ENACTED, That, on or before November 1,  
34 2023, the Modernize Maryland Oversight Commission shall report to the General  
35 Assembly, in accordance with § 2-1257 of the State Government Article, recommendations

1 to improve the format for the Secretary of Information Technology to report on major  
2 information technology development projects under § 3.5–309 of the State Finance and  
3 Procurement Article to meet the needs for strategic planning and investment.

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

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

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

13 SECTION 5. AND BE IT FURTHER ENACTED, That this Act shall take effect June  
14 1, 2023.