

HOUSE BILL 235

P1

0lr0398
CF SB 120

By: **Delegates Carey, Charkoudian, Crosby, and C. Watson**

Introduced and read first time: January 17, 2020

Assigned to: Health and Government Operations

A BILL ENTITLED

1 AN ACT concerning

2 **State Government – Department of Information Technology – Cybersecurity**

3 FOR the purpose of requiring the Secretary of Information Technology, in consultation with
4 the Attorney General, to advise and oversee a consistent cybersecurity strategy for
5 units of State government and political subdivisions of the State; requiring the
6 Secretary to advise and consult with the Legislative and Judicial branches of State
7 government regarding a cybersecurity strategy; defining certain terms; and
8 generally relating to cybersecurity.

9 BY repealing and reenacting, without amendments,
10 Article – State Finance and Procurement
11 Section 3A–101
12 Annotated Code of Maryland
13 (2015 Replacement Volume and 2019 Supplement)

14 BY repealing and reenacting, with amendments,
15 Article – State Finance and Procurement
16 Section 3A–301 and 3A–303(a)
17 Annotated Code of Maryland
18 (2015 Replacement Volume and 2019 Supplement)

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

21 **Article – State Finance and Procurement**

22 3A–101.

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

24 (b) “Department” means the Department of Information Technology.

EXPLANATION: CAPITALS INDICATE MATTER ADDED TO EXISTING LAW.

[Brackets] indicate matter deleted from existing law.



(c) “Secretary” means the Secretary of Information Technology.

(d) “Telecommunication” means the transmission of information, images, pictures, voice, or data by radio, video, or other electronic or impulse means.

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

3A-301.

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

(B) “CYBERSECURITY” MEANS PROCESSES OR CAPABILITIES WHEREIN SYSTEMS, COMMUNICATIONS, AND INFORMATION ARE PROTECTED AND DEFENDED AGAINST DAMAGE, UNAUTHORIZED USE OR MODIFICATION, AND EXPLOITATION.

(C) “CYBERSECURITY STRATEGY” MEANS A VISION, A PLAN OF ACTION, OR GUIDING PRINCIPLES.

[(b)] (D) (1) “Development” means all expenditures for a new information technology system or an enhancement to an existing system including system:

(i) planning;

(ii) procurement;

(iii) creation;

(iv) installation;

(v) testing; and

(vi) initial training.

(2) “Development” does not include:

(i) ongoing operating costs, software or hardware maintenance, routine upgrades, or modifications that merely allow for a continuation of the existing level of functionality; or

(ii) expenditures made after a new or enhanced system has been legally accepted by the user and is being used for the business process for which it was intended.

[(c)] (E) “Fund” means the Major Information Technology Development Project

1 Fund.

2 **[(d)] (F)** “Information technology” means all electronic information processing
3 hardware and software, including:

4 (1) maintenance;

5 (2) telecommunications; and

6 (3) associated consulting services.

7 **[(e)] (G)** “Information technology services” means information provided by
8 electronic means by or on behalf of a unit of State government.

9 **[(f)] (H)** “Major information technology development project” means any
10 information technology development project that meets one or more of the following
11 criteria:

12 (1) the estimated total cost of development equals or exceeds \$1,000,000;

13 (2) the project is undertaken to support a critical business function
14 associated with the public health, education, safety, or financial well-being of the citizens
15 of Maryland; or

16 (3) the Secretary determines that the project requires the special attention
17 and consideration given to a major information technology development project due to:

18 (i) the significance of the project’s potential benefits or risks;

19 (ii) the impact of the project on the public or local governments;

20 (iii) the public visibility of the project; or

21 (iv) other reasons as determined by the Secretary.

22 **[(g)] (I)** “Master plan” means the statewide information technology master
23 plan.

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

28 **[(i)] (K)** “Resource sharing” means the utilization of a State resource by private
29 industry in exchange for the provision to the State of a communication service or other
30 consideration.

1 **[(j)] (L)** “Systems development life cycle plan” means a plan that defines all
2 actions, functions, or activities to be performed by a unit of State government in the
3 definition, planning, acquisition, development, testing, implementation, operation,
4 enhancement, and modification of information technology systems.

5 3A-303.

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

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

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

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

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

15 (i) be the basis for the management and direction of information
16 technology within the Executive Branch of State government;

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) work jointly with the Secretary of Budget and Management to
22 ensure that information technology plans and budgets are consistent;

23 (v) ensure that State information technology plans, policies, and
24 standards are consistent with State goals, objectives, and resources, and represent a
25 long-range vision for using information technology to improve the overall effectiveness of
26 State government; and

27 (vi) include standards to assure nonvisual access to the information
28 and services made available to the public over the Internet; **[and]**

29 (5) adopting by regulation and enforcing nonvisual access standards to be
30 used in the procurement of information technology services by or on behalf of units of State
31 government in accordance with subsection (b) of this section;

32 **(6) IN CONSULTATION WITH THE ATTORNEY GENERAL, ADVISING**

1 AND OVERSEEING A CONSISTENT CYBERSECURITY STRATEGY FOR UNITS OF STATE
2 GOVERNMENT, INCLUDING INSTITUTIONS UNDER THE CONTROL OF THE
3 GOVERNING BOARDS OF THE PUBLIC INSTITUTIONS OF HIGHER EDUCATION, AND
4 COUNTIES, MUNICIPAL CORPORATIONS, SCHOOL DISTRICTS, AND ALL OTHER
5 POLITICAL SUBDIVISIONS OF THE STATE; AND

6 (7) ADVISING AND CONSULTING WITH THE LEGISLATIVE AND
7 JUDICIAL BRANCHES OF STATE GOVERNMENT REGARDING A CYBERSECURITY
8 STRATEGY.

9 SECTION 2. AND BE IT FURTHER ENACTED, That this Act shall take effect
10 October 1, 2020.