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

AN ACT concerning

State Government – Department of Information Technology – Cybersecurity

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

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

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

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

Article – State Finance and Procurement

3A–101.

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

(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

Fund.

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

(1) maintenance;

(2) telecommunications; and

(3) associated consulting services.

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

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

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

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

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

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

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

(iii) the public visibility of the project; or

(iv) other reasons as determined by the Secretary.

[(g)**] (I)** "Master plan" means the statewide information technology master plan.

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

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

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

3A–303.

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

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

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

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

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

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

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

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

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

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

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

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

(6) IN CONSULTATION WITH THE ATTORNEY GENERAL, ADVISING

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

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

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