SENATE BILL 734

P2 1lr2393

By: **Senator Lee**
Introduced and read first time: February 5, 2021
Assigned to: Education, Health, and Environmental Affairs

A BILL ENTITLED

AN ACT concerning

State Procurement – Internet of Things Devices – Guidelines, Standards, and Purchasing Restrictions

FOR the purpose of requiring the Department of Information Technology to issue certain standards and guidelines for units of State government for the appropriate use and management of certain Internet of Things devices under certain circumstances; requiring the Department to review and revise its standards and guidelines at certain intervals for a certain purpose; requiring the Department to issue certain standards and guidelines for certain information systems owned or controlled by a unit, provided by a contractor to a unit, or provided by a subcontractor to a contractor regarding certain security vulnerabilities; requiring certain requirements for certain standards and guidelines; requiring the head of each unit, within a certain time frame, to implement policy changes to ensure compliance with certain standards and guidelines; requiring the Department to provide certain assistance to certain units to implement certain standards and guidelines established to guide the response to a security vulnerability in an information system; prohibiting a unit from procuring, executing a renewal option for a contract for the purchase of, or continuing to use an Internet of Things device if the unit makes a certain determination; authorizing the head of a unit to waive a certain prohibition if the unit makes certain determinations; requiring the Department to establish a certain process for a unit to follow to determine whether a certain waiver may be granted; authorizing a unit to request the assistance of the Department when making a decision to grant a certain waiver; requiring a unit to report certain information to the Department within a certain period of time after the unit grants a certain waiver; authorizing the Department, in consultation with the Board of Public Works and the Office of the Attorney General, to adopt certain regulations; requiring the Department to submit a certain report to certain persons at certain times; applying certain provisions of law to certain universities; providing for the application of this Act; providing for the construction of this Act; defining certain terms; and generally relating to the procurement and use of Internet of Things devices by units of State government.

EXPLANATION: **CAPITALS INDICATE MATTER ADDED TO EXISTING LAW**.
[Brackets**]** indicate matter deleted from existing law.

BY repealing and reenacting, without amendments,
Article – State Finance and Procurement
Section 11–203(e)(1) and (2)
Annotated Code of Maryland
(2015 Replacement Volume and 2020 Supplement)

BY repealing and reenacting, with amendments,
Article – State Finance and Procurement
Section 11–203(e)(5)
Annotated Code of Maryland
(2015 Replacement Volume and 2020 Supplement)

BY adding to
Article – State Finance and Procurement
Section 12–601 through 12–605 to be under the new subtitle "Subtitle 6. Use and Management of Internet of Things Devices"
Annotated Code of Maryland
(2015 Replacement Volume and 2020 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

11–203.

(e) (1) In this subsection, "University" means the University System of Maryland, Morgan State University, or St. Mary's College of Maryland.

(2) Except as otherwise provided in this subsection, this Division II does not apply to the University System of Maryland, Morgan State University, or St. Mary's College of Maryland.

(5) (i) Except as provided in paragraph (7) of this subsection, the following provisions of Division II of this article apply to a University:

1. § 11–205 of this subtitle ("Collusion");

2. § 11–205.1 of this subtitle ("Falsification, concealment, etc., of material facts");

3. § 13–219 of this article ("Required clauses – Nondiscrimination clause");

4. § 13–225 of this article ("Retainage");

5. TITLE 13, SUBTITLE 3 OF THIS ARTICLE ("USE AND

MANAGEMENT OF INTERNET OF THINGS DEVICES");

[5.**] 6.** Title 14, Subtitle 3 of this article ("Minority Business Participation");

[6.**] 7.** Title 15, Subtitle 1 of this article ("Procurement Contract Administration");

[7.**] 8.** § 15–226 of this article ("Policy established; timing of payments; notice upon nonpayment; disputes; appeals"); and

[8.**] 9.** Title 16 of this article ("Suspension and Debarment of Contractors").

(ii) If a procurement violates the provisions of this subsection or policies adopted in accordance with this subsection, the procurement contract is void or voidable in accordance with the provisions of § 11–204 of this subtitle.

SUBTITLE 6. USE AND MANAGEMENT OF INTERNET OF THINGS DEVICES.

12–601.

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

(B) "DEPARTMENT" MEANS THE DEPARTMENT OF INFORMATION TECHNOLOGY.

(C) "INFORMATION RESOURCES" MEANS INFORMATION AND RELATED RESOURCES, INCLUDING PERSONNEL, EQUIPMENT, FUNDS, AND INFORMATION TECHNOLOGY.

(D) "INFORMATION SYSTEM" MEANS A DISCRETE SET OF INFORMATION RESOURCES ORGANIZED FOR THE COLLECTION, PROCESSING, MAINTENANCE, USE, SHARING, DISSEMINATION, OR DISPOSITION OF INFORMATION.

(E) (1) "INFORMATION TECHNOLOGY" MEANS ANY EQUIPMENT OR INTERCONNECTED SYSTEM OR SUBSYSTEM OF EQUIPMENT USED IN THE AUTOMATIC ACQUISITION, STORAGE, ANALYSIS, EVALUATION, MANIPULATION, MANAGEMENT, MOVEMENT, CONTROL, DISPLAY, SWITCHING, INTERCHANGE, TRANSMISSION, OR RECEPTION OF DATA OR INFORMATION BY A UNIT, IF THE EQUIPMENT IS USED BY THE UNIT DIRECTLY OR USED BY A CONTRACTOR UNDER A CONTRACT WITH THE UNIT.

(2) "INFORMATION TECHNOLOGY" INCLUDES COMPUTERS, ANCILLARY EQUIPMENT, PERIPHERAL EQUIPMENT DESIGNED TO BE CONTROLLED BY THE CENTRAL PROCESSING UNIT OF A COMPUTER, SOFTWARE, FIRMWARE, AND SIMILAR PROCEDURES, SERVICES, AND SUPPORT SERVICES.

(3) "INFORMATION TECHNOLOGY" DOES NOT INCLUDE ANY EQUIPMENT ACQUIRED BY A FEDERAL CONTRACTOR INCIDENTAL TO A FEDERAL CONTRACT.

(F) "INTERNET OF THINGS DEVICES" MEANS DEVICES THAT CAN FUNCTION INDEPENDENTLY OF ANOTHER DEVICE AND THAT:

(1) HAVE AT LEAST ONE SENSOR OR ACTUATOR FOR INTERACTING DIRECTLY WITH THE PHYSICAL WORLD;

(2) HAVE AT LEAST ONE NETWORK INTERFACE; AND

(3) ARE NOT CONVENTIONAL INFORMATION TECHNOLOGY DEVICES, INCLUDING SMARTPHONES AND LAPTOPS, FOR WHICH THERE EXIST GENERALLY ACCEPTED, UNDERSTOOD, AND UTILIZED CYBERSECURITY FEATURES.

(G) "NIST" MEANS THE NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY.

(H) "SECURITY CONTROL" MEANS THE MANAGEMENT, OPERATIONAL, AND TECHNICAL CONTROLS USED TO PROTECT AGAINST AN UNAUTHORIZED EFFORT TO ADVERSELY AFFECT THE CONFIDENTIALITY, INTEGRITY, AND AVAILABILITY OF AN INFORMATION SYSTEM OR ITS INFORMATION.

(I) "SECURITY VULNERABILITY" MEANS AN ATTRIBUTE OF HARDWARE, SOFTWARE, PROCESS, PROCEDURE, OR A COMBINATION OF THESE FACTORS THAT COULD ENABLE OR FACILITATE THE DEFEAT OR COMPROMISE OF A SECURITY CONTROL.

12–602.

THIS SUBTITLE APPLIES TO ALL PROCUREMENTS BY THE STATE.

12–603.

(A) (1) THE DEPARTMENT SHALL ISSUE STANDARDS AND GUIDELINES TO UNITS FOR THE APPROPRIATE USE AND MANAGEMENT OF INTERNET OF THINGS DEVICES:

(I) OWNED OR CONTROLLED BY A UNIT; AND

(II) CONNECTED TO INFORMATION SYSTEMS OWNED OR CONTROLLED BY A UNIT.

(2) THE STANDARDS AND GUIDELINES ISSUED IN ACCORDANCE WITH PARAGRAPH (1) OF THIS SUBSECTION SHALL:

(I) INCLUDE MINIMUM INFORMATION SECURITY REQUIREMENTS FOR MANAGING CYBERSECURITY RISKS ASSOCIATED WITH INTERNET OF THINGS DEVICES; AND

(II) AT A MINIMUM, ALIGN WITH THE STANDARDS AND GUIDELINES ADOPTED BY THE DIRECTOR OF NIST FOR THE USE AND MANAGEMENT OF INTERNET OF THINGS DEVICES BY AGENCIES OF THE FEDERAL GOVERNMENT.

(3) AT LEAST ONCE EVERY 5 YEARS, THE DEPARTMENT SHALL REVIEW AND REVISE THE STANDARDS AND GUIDELINES TO ENSURE THAT THEY ARE AT LEAST AS COMPREHENSIVE AS THE STANDARDS AND GUIDELINES ADOPTED BY THE DIRECTOR OF NIST FOR THE USE AND MANAGEMENT OF INTERNET OF THINGS DEVICES BY AGENCIES OF THE FEDERAL GOVERNMENT.

(B) WITHIN 180 DAYS AFTER THE DEPARTMENT ISSUES NEW OR REVISED STANDARDS AND GUIDELINES UNDER THIS SECTION, THE HEAD OF EACH UNIT SHALL IMPLEMENT POLICY CHANGES TO ENSURE COMPLIANCE WITH THE STANDARDS AND GUIDELINES.

12–604.

(A) (1) THE DEPARTMENT SHALL ISSUE STANDARDS AND GUIDELINES:

(I) FOR INFORMATION SYSTEMS OWNED OR CONTROLLED BY A UNIT, INCLUDING INTERNET OF THINGS DEVICES FOR:

1. REPORTING, COORDINATING, PUBLISHING, AND RECEIVING INFORMATION ABOUT A SECURITY VULNERABILITY; AND

2. RESOLVING A SECURITY VULNERABILITY; AND

(II) FOR A CONTRACTOR THAT PROVIDES AN INFORMATION SYSTEM TO A UNIT, INCLUDING INTERNET OF THINGS DEVICES, AND A SUBCONTRACTOR THAT PROVIDES AN INFORMATION SYSTEM TO A CONTRACTOR

FOR:

1. RECEIVING INFORMATION ABOUT A POTENTIAL SECURITY VULNERABILITY RELATING TO THE INFORMATION SYSTEM; AND

2. DISSEMINATING INFORMATION ABOUT THE RESOLUTION OF A SECURITY VULNERABILITY RELATING TO THE INFORMATION SYSTEM.

(2) THE STANDARDS AND GUIDELINES ISSUED IN ACCORDANCE WITH PARAGRAPH (1) OF THIS SUBSECTION SHALL, AT A MINIMUM, ALIGN WITH THE GUIDELINES ADOPTED BY THE DIRECTOR OF NIST FOR THE RECEIPT AND DISSEMINATION OF INFORMATION ABOUT A POTENTIAL SECURITY VULNERABILITY RELATING TO AN INFORMATION SYSTEM, INCLUDING INTERNET OF THINGS DEVICES, OWNED OR CONTROLLED BY AGENCIES OF THE FEDERAL GOVERNMENT.

(B) THE HEAD OF EACH UNIT SHALL IMPLEMENT, AND THE DEPARTMENT SHALL PROVIDE, OPERATIONAL AND TECHNICAL ASSISTANCE TO EACH UNIT IN IMPLEMENTING THE STANDARDS AND GUIDELINES ISSUED UNDER SUBSECTION (A) OF THIS SECTION.

12–605.

(A) EXCEPT AS PROVIDED IN SUBSECTION (B) OF THIS SECTION, A UNIT MAY NOT PROCURE, EXECUTE A RENEWAL OPTION FOR A CONTRACT FOR THE PURCHASE OF, OR CONTINUE TO USE AN INTERNET OF THINGS DEVICE IF THE UNIT DETERMINES THAT THE USE OF THE DEVICE PREVENTS COMPLIANCE WITH THE STANDARDS AND GUIDELINES ESTABLISHED UNDER §§ 12–603 OR 12–604 OF THIS SUBTITLE.

(B) (1) THE HEAD OF A UNIT MAY WAIVE THE PROHIBITION IN SUBSECTION (A) IF THE HEAD OF THE UNIT DETERMINES THAT:

(I) THE WAIVER IS REQUIRED TO COMPLY WITH A PROVISION OF FEDERAL LAW;

(II) PROCURING OR USING THE INTERNET OF THINGS DEVICE IS NECESSARY FOR RESEARCH PURPOSES; OR

(III) THE DEVICE IS SECURED USING ALTERNATIVE AND EFFECTIVE METHODS APPROPRIATE TO THE FUNCTION OF THE DEVICE.

(2) THE DEPARTMENT SHALL ESTABLISH A PROCESS FOR A UNIT TO

FOLLOW TO DETERMINE WHETHER THE WAIVER UNDER PARAGRAPH (1) OF THIS SUBSECTION MAY BE GRANTED.

(3) A UNIT MAY REQUEST THE ASSISTANCE OF THE DEPARTMENT WHEN MAKING A DECISION TO WAIVE THE PROHIBITION IN SUBSECTION (A) OF THIS SECTION.

(4) WITHIN 15 DAYS AFTER THE HEAD OF A UNIT GRANTS A WAIVER, THE UNIT SHALL REPORT TO THE DEPARTMENT THE FOLLOWING INFORMATION:

(I) THE TYPE OF THE INTERNET OF THINGS DEVICE FOR WHICH THE WAIVER WAS GRANTED;

(II) THE TOTAL NUMBER OF INTERNET OF THINGS DEVICES PROCURED OR OBTAINED UNDER THE WAIVER;

(III) THE REASON FOR GRANTING THE WAIVER; AND

(IV) IF THE HEAD OF A UNIT GRANTED THE WAIVER IN ACCORDANCE WITH PARAGRAPH (1)(III) OF THIS SUBSECTION, A DESCRIPTION OF THE ALTERNATIVE AND EFFECTIVE METHODS USED TO SECURE THE INTERNET OF THINGS DEVICE.

(C) THE DEPARTMENT, IN CONSULTATION WITH THE BOARD AND THE OFFICE OF THE ATTORNEY GENERAL, MAY ADOPT REGULATIONS TO CARRY OUT THE PROVISIONS OF THIS SECTION, INCLUDING REGULATIONS FOR MANAGEMENT AND USE OF NONCOMPLIANT DEVICES DESIGNED TO ADDRESS THE LONG–TERM RISK OF USING A NONCOMPLIANT INTERNET OF THINGS DEVICE.

(D) WITHIN 60 DAYS AFTER THE END OF EACH FISCAL YEAR, THE DEPARTMENT SHALL SUBMIT A REPORT TO THE BOARD AND, IN ACCORDANCE WITH § 2–1257 OF THE STATE GOVERNMENT ARTICLE, THE GENERAL ASSEMBLY THAT PROVIDES, BY UNIT AND FOR THE PRECEDING FISCAL YEAR:

(1) THE TOTAL NUMBER OF WAIVERS GRANTED UNDER SUBSECTION (B) OF THIS SUBSECTION; AND

(2) THE NUMBER, TYPE, AND BASIS FOR GRANTING THE WAIVER FOR EACH INTERNET OF THINGS DEVICE FOR WHICH A WAIVER WAS GRANTED.

SECTION 2. AND BE IT FURTHER ENACTED, That nothing in this Act shall be construed to establish additional obligations or criminal penalties for individuals engaged in researching the cybersecurity of Internet of Things devices, as defined in § 12–601 of the State Finance and Procurement Article, as enacted by Section 1 of this Act.

SECTION 3. AND BE IT FURTHER ENACTED, That this Act shall take effect October 1, 2021.