SENATE BILL 882

P2 8lr1687

By: **Senator Lee**
Introduced and read first time: February 5, 2018
Assigned to: Education, Health, and Environmental Affairs

A BILL ENTITLED

AN ACT concerning

Procurement – Telecommunication and Computer Network Access – Security Requirements

FOR the purpose of requiring a unit to require a certain bidder or offeror to submit a certain certification or application before the unit is authorized to award a procurement contract for a certain Internet–connected device; requiring a certain bidder or offeror to certify certain information regarding a certain security vulnerability of a certain Internet–connected device; authorizing a certain bidder or offeror to submit a certain application for a waiver from certain certification requirements; requiring a certain application for a waiver to identify or include certain information; authorizing a certain unit to petition the Department of Information Technology for a certain waiver if the unit determines that a certain procurement is unfeasible or economically impractical; requiring a certain petition to include certain waivers; requiring the Department to establish a certain process for submitting and reviewing certain petitions; prohibiting a unit from awarding a certain procurement before the Department grants a certain petition; requiring the head of a certain unit to sign a certain statement accepting certain responsibility if the Department grants a certain petition; requiring the Department to adopt regulations to define a certain set of conditions for security standards for certain noncompliant devices; requiring certain conditions to be met before a unit is authorized to award a certain procurement for a certain noncompliant device; authorizing the Department to coordinate with certain partners and experts and consider certain factors in establishing certain conditions; authorizing the Department to coordinate with certain partners and experts to adopt certain regulations regarding management and use of certain noncompliant devices; authorizing a certain unit to use certain third–party security standards under certain circumstances; requiring a certain unit to require a certain bidder or offeror to submit a certain certification regarding compliance with a certain third–party security standard; requiring the Department to coordinate with certain units to determine requirements for certain third–party security standards and whether certain standards align with certain regulations; authorizing a unit to use a certain security evaluation process or criteria for certain Internet–connected

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

devices under certain circumstances; requiring the Department, in coordination with certain units, to determine if a certain process or criteria align with certain regulations; requiring a certain contract to include certain clauses; authorizing a unit to alter certain contract clauses after consultation with the Department; providing that a unit is authorized to enter into a certain contract or accept a certain bid or proposal only from an Internet service provider that does not engage in certain action; requiring the Board of Public Works to establish a certain process to authorize a unit to obtain a certain waiver; requiring a waiver process to include a certain hearing and vote; requiring the Board to publish certain notice on its website within a certain period of time; requiring the Board to submit a certain report to the General Assembly on or before a certain date each year; requiring the Department to adopt certain regulations in accordance with certain requirements on or before a certain date; providing for the construction of this Act; and generally relating to procurement and security requirements for telecommunication and computer network access.

BY adding to
Article – State Finance and Procurement
Section 13–401 through 13–409 to be under the new subtitle "Subtitle 4. Requirements for Telecommunication and Computer Network Access Security"
Annotated Code of Maryland
(2015 Replacement Volume and 2017 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

SUBTITLE 4. REQUIREMENTS FOR TELECOMMUNICATION AND COMPUTER NETWORK ACCESS SECURITY.

13–401.

THIS SUBTITLE APPLIES TO ALL PROCUREMENTS BY THE STATE.

13–402.

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

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

(C) (1) "FIRMWARE" MEANS A COMPUTER PROGRAM AND THE DATA STORED IN HARDWARE SUCH THAT THE PROGRAM AND DATA CANNOT BE

DYNAMICALLY WRITTEN OR MODIFIED DURING THE EXECUTION OF THE PROGRAM.

(2) "FIRMWARE" INCLUDES A COMPUTER PROGRAM AND THE DATA STORED IN HARDWARE IN READ–ONLY MEMORY OR PROGRAMMABLE READ–ONLY MEMORY.

(D) (1) "FIXED OR HARD–CODED CREDENTIAL" MEANS A VALUE USED AS PART OF AN AUTHENTICATION MECHANISM FOR GRANTING REMOTE ACCESS TO AN INFORMATION SYSTEM OR ITS INFORMATION, THAT:

(I) IS ESTABLISHED BY A PRODUCT VENDOR OR SERVICE PROVIDER; AND

(II) EXCEPT THROUGH A FIRMWARE UPDATE, IS INCAPABLE OF BEING MODIFIED OR REVOKED BY THE USER OR MANUFACTURER LAWFULLY OPERATING THE INFORMATION SYSTEM.

(2) "FIXED OR HARD–CODED CREDENTIAL" INCLUDES A PASSWORD, TOKEN, CRYPTOGRAPHIC KEY, OR OTHER DATA ELEMENT.

(E) "HARDWARE" MEANS THE PHYSICAL COMPONENTS OF AN INFORMATION SYSTEM.

(F) "INTERNET–CONNECTED DEVICE" MEANS A PHYSICAL OBJECT THAT:

(1) IS CAPABLE OF CONNECTING TO AND IS IN REGULAR CONNECTION WITH THE INTERNET; AND

(2) HAS COMPUTER PROCESSING CAPABILITIES THAT CAN COLLECT, SEND, OR RECEIVE DATA.

(G) (1) "INTERNET SERVICE PROVIDER" MEANS A PERSON, A BUSINESS, OR AN ORGANIZATION QUALIFIED TO DO BUSINESS IN THE STATE THAT PROVIDES INDIVIDUALS, CORPORATIONS, OR OTHER ENTITIES WITH THE ABILITY TO CONNECT TO THE INTERNET.

(2) "INTERNET SERVICE PROVIDER" INCLUDES A MUNICIPAL BROADBAND PROVIDER.

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

(I) "PROPERLY AUTHENTICATED UPDATE" MEANS AN UPDATE, A

REMEDIATION, OR A TECHNICAL FIX TO A HARDWARE, FIRMWARE, OR SOFTWARE COMPONENT THAT:

(1) IS ISSUED BY A PRODUCT VENDOR OR SERVICE PROVIDER TO CORRECT A PARTICULAR PROBLEM WITH THE COMPONENT; AND

(2) FOR A SOFTWARE OR FIRMWARE COMPONENT, CONTAINS A METHOD OF AUTHENTICITY PROTECTION, SUCH AS A DIGITAL SIGNATURE, THAT AUTOMATICALLY DETECTS AND REJECTS UNAUTHORIZED UPDATES.

(J) (1) "REASONABLE NETWORK MANAGEMENT" MEANS A NETWORK MANAGEMENT PRACTICE THAT HAS A PRIMARILY TECHNICAL NETWORK MANAGEMENT JUSTIFICATION.

(2) "REASONABLE NETWORK MANAGEMENT" INCLUDES A PRACTICE THAT:

(I) IS PRIMARILY USED FOR AND TAILORED TO ACHIEVING A LEGITIMATE NETWORK MANAGEMENT PURPOSE; AND

(II) TAKES INTO ACCOUNT THE PARTICULAR NETWORK ARCHITECTURE AND TECHNOLOGY OF THE BROADBAND INTERNET ACCESS SERVICE.

(3) "REASONABLE NETWORK MANAGEMENT" DOES NOT INCLUDE OTHER BUSINESS PRACTICES THAT ARE NOT RELATED TO NETWORK MANAGEMENT.

(K) "SECURITY VULNERABILITY" MEANS AN ATTRIBUTE OF HARDWARE, FIRMWARE, SOFTWARE, PROCESS, PROCEDURE, OR A COMBINATION OF THESE FACTORS THAT COULD ENABLE OR FACILITATE THE DEFEAT OR COMPROMISE OF THE CONFIDENTIALITY, INTEGRITY, OR AVAILABILITY OF AN INFORMATION SYSTEM, INFORMATION WITHIN THE INFORMATION SYSTEM, OR THE PHYSICAL DEVICES TO WHICH THE INFORMATION SYSTEM IS CONNECTED.

(L) "SOFTWARE" MEANS A COMPUTER PROGRAM AND ASSOCIATED DATA THAT MAY BE DYNAMICALLY WRITTEN OR MODIFIED.

13–403.

(A) BEFORE A UNIT MAY AWARD A PROCUREMENT CONTRACT FOR AN INTERNET–CONNECTED DEVICE, THE UNIT SHALL REQUIRE A BIDDER OR AN OFFEROR TO SUBMIT:

(1) A WRITTEN CERTIFICATION IN ACCORDANCE WITH SUBSECTION (B) OF THIS SECTION; OR

(2) AN APPLICATION FOR A WAIVER IN ACCORDANCE WITH SUBSECTION (C) OF THIS SECTION.

(B) EXCEPT AS PROVIDED IN SUBSECTION (C) OF THIS SECTION, A BIDDER OR AN OFFEROR SHALL CERTIFY THAT THE INTERNET–CONNECTED DEVICE:

(1) AT THE TIME OF SUBMITTING THE BID OR PROPOSAL, DOES NOT CONTAIN A HARDWARE, SOFTWARE, OR FIRMWARE COMPONENT WITH A KNOWN SECURITY VULNERABILITY OR DEFECT LISTED IN:

(I) THE NATIONAL VULNERABILITY DATABASE OF NIST; OR

(II) ANY ADDITIONAL DATABASE SELECTED BY THE SECRETARY OF INFORMATION TECHNOLOGY;

(2) RELIES ON SOFTWARE OR FIRMWARE COMPONENTS CAPABLE OF ACCEPTING PROPERLY AUTHENTICATED AND TRUSTED UPDATES FROM THE BIDDER OR OFFEROR;

(3) USES ONLY NONDEPRECATED INDUSTRY–STANDARD PROTOCOLS AND TECHNOLOGIES FOR FUNCTIONS, INCLUDING:

(I) COMMUNICATIONS, SUCH AS STANDARD PORTS FOR NETWORK TRAFFIC;

(II) ENCRYPTION; AND

(III) INTERCONNECTION WITH OTHER DEVICES OR PERIPHERALS; AND

(4) DOES NOT INCLUDE ANY FIXED OR HARD–CODED CREDENTIALS USED FOR REMOTE ADMINISTRATION, THE DELIVERY OF UPDATES, OR COMMUNICATION.

(C) (1) A BIDDER OR AN OFFEROR MAY SUBMIT A WRITTEN APPLICATION FOR A WAIVER FROM THE CERTIFICATION REQUIREMENTS UNDER SUBSECTION (B) OF THIS SECTION FOR THE PURPOSE OF DISCLOSING A KNOWN VULNERABILITY TO THE UNIT.

(2) AN APPLICATION FOR A WAIVER SHALL:

(I) IDENTIFY THE SPECIFIC VULNERABILITY;

(II) IDENTIFY ANY MITIGATION ACTIONS THAT MAY LIMIT OR ELIMINATE THE ABILITY FOR AN ADVERSARY TO EXPLOIT THE VULNERABILITY; AND

(III) INCLUDE A JUSTIFICATION FOR SECURE USE OF THE DEVICE NOTWITHSTANDING THE VULNERABILITY.

13–404.

(A) (1) IF A UNIT REASONABLY DETERMINES THAT PROCUREMENT OF AN INTERNET–CONNECTED DEVICE THAT MEETS THE CERTIFICATION REQUIREMENTS UNDER § 13–403(B) OF THIS SUBTITLE WOULD BE UNFEASIBLE OR ECONOMICALLY IMPRACTICAL, THE UNIT SHALL PETITION THE DEPARTMENT FOR A WAIVER TO PURCHASE A NONCOMPLIANT INTERNET–CONNECTED DEVICE.

(2) A PETITION SUBMITTED UNDER PARAGRAPH (1) OF THIS SUBSECTION SHALL INCLUDE ANY WAIVERS SUBMITTED TO THE UNIT UNDER § 13–403(C) OF THIS SUBTITLE.

(B) THE DEPARTMENT SHALL ESTABLISH A PROCESS FOR SUBMITTING AND REVIEWING PETITIONS UNDER THIS SECTION.

(C) A UNIT MAY NOT AWARD A PROCUREMENT TO A BIDDER OR AN OFFEROR THAT DOES NOT MEET THE CERTIFICATION REQUIREMENTS OF § 13–403(B) OF THIS SUBTITLE BEFORE THE DEPARTMENT GRANTS THE PETITION FOR WAIVER.

(D) IF THE DEPARTMENT GRANTS A PETITION FOR A WAIVER, THE HEAD OF THE UNIT AWARDING THE PROCUREMENT SHALL SUBMIT A WRITTEN AND SIGNED STATEMENT THAT THE UNIT ACCEPTS THE RISKS RESULTING FROM USE OF THE DEVICE WITH THE KNOWN VULNERABILITY AS REPRESENTED BY THE BIDDER OR OFFEROR.

13–405.

(A) THE DEPARTMENT SHALL ADOPT REGULATIONS THAT DEFINE A SET OF CONDITIONS THAT:

(1) ENSURE AN INTERNET–CONNECTED DEVICE THAT DOES NOT COMPLY WITH THE CERTIFICATION REQUIREMENTS UNDER § 13–403(B) OF THIS SUBTITLE CAN BE USED WITH A LEVEL OF SECURITY THAT IS EQUIVALENT TO THE LEVEL OF SECURITY DESCRIBED IN THE CERTIFICATION REQUIREMENTS; AND

(2) SHALL BE MET BEFORE A UNIT MAY AWARD A PROCUREMENT FOR A NONCOMPLIANT DEVICE.

(B) IN ESTABLISHING THE SET OF CONDITIONS REQUIRED UNDER SUBSECTION (A) OF THIS SECTION, THE DEPARTMENT, IN COORDINATION WITH RELEVANT PARTNERS AND EXPERTS, MAY CONSIDER:

(1) THE USE OF NETWORK SEGMENTATION OR MICRO–SEGMENTATION;

(2) THE ADOPTION OF SYSTEM–LEVEL SECURITY CONTROLS, INCLUDING OPERATING SYSTEM CONTAINERS AND MICROSERVICES;

(3) THE USE OF MULTIFACTOR AUTHENTICATION; AND

(4) THE USE OF INTELLIGENT NETWORK SOLUTIONS AND EDGE SYSTEMS, INCLUDING GATEWAYS, THAT CAN ISOLATE, DISABLE, OR REMEDIATE CONNECTED DEVICES.

(C) THE DEPARTMENT, IN COORDINATION WITH RELEVANT PARTNERS AND EXPERTS, MAY ADOPT ADDITIONAL REGULATIONS FOR MANAGEMENT AND USE OF NONCOMPLIANT DEVICES DESIGNED TO ADDRESS THE LONG–TERM RISK OF USING A NONCOMPLIANT INTERNET–CONNECTED DEVICE, INCLUDING:

(1) DEADLINES FOR REMOVAL, REPLACEMENT, OR DISABLING OF NONCOMPLIANT DEVICES OR THE INTERNET CONNECTIVITY OF THE DEVICE; AND

(2) MINIMAL REQUIREMENTS FOR GATEWAY PRODUCTS TO ENSURE THE INTEGRITY AND SECURITY OF THE NONCOMPLIANT DEVICES.

13–406.

(A) IF A UNIT USES A THIRD–PARTY SECURITY STANDARD FOR INTERNET–CONNECTED DEVICES THAT PROVIDES AN EQUIVALENT OR GREATER LEVEL OF SECURITY THAN THE STANDARDS PROVIDED BY THE CERTIFICATION REQUIREMENTS UNDER § 13–403(B) OF THIS SUBTITLE, AS DETERMINED BY THE DEPARTMENT IN ACCORDANCE WITH SUBSECTION (C) OF THIS SECTION, THE UNIT MAY ALLOW A BIDDER OR AN OFFEROR TO DEMONSTRATE COMPLIANCE WITH THAT STANDARD IN LIEU OF THE CERTIFICATION REQUIREMENTS.

(B) A UNIT THAT USES A THIRD–PARTY SECURITY STANDARD SHALL REQUIRE A BIDDER OR AN OFFEROR FOR A PROCUREMENT TO PROVIDE AN

INTERNET–CONNECTED DEVICE TO SUBMIT A WRITTEN CERTIFICATION THAT THE DEVICE COMPLIES WITH THE SECURITY STANDARDS OF THE THIRD PARTY.

(C) THE DEPARTMENT, IN COORDINATION WITH OTHER APPROPRIATE UNITS, SHALL DETERMINE:

(1) REQUIREMENTS FOR THIRD–PARTY SECURITY STANDARDS THAT ARE EQUIVALENT TO THE CERTIFICATION REQUIREMENTS UNDER § 13–403(B) OF THIS SUBTITLE; AND

(2) WHETHER THE THIRD–PARTY SECURITY STANDARDS PROVIDE APPROPRIATE SECURITY AND ARE ALIGNED WITH REGULATIONS ISSUED BY THE DEPARTMENT AS REQUIRED UNDER § 13–405 OF THIS SUBTITLE.

13–407.

(A) IF A UNIT USES A SECURITY EVALUATION PROCESS OR CRITERIA FOR INTERNET–CONNECTED DEVICES THAT PROVIDE AN EQUIVALENT OR GREATER LEVEL OF SECURITY THAN THE CERTIFICATION REQUIREMENTS UNDER § 13–403(B) OF THIS SUBTITLE, AS DETERMINED BY THE DEPARTMENT UNDER SUBSECTION (B) OF THIS SECTION, AN AGENCY MAY CONTINUE TO USE THAT PROCESS OR THOSE CRITERIA IN LIEU OF THE CERTIFICATION REQUIREMENTS.

(B) THE DEPARTMENT, IN COORDINATION WITH OTHER APPROPRIATE UNITS, SHALL DETERMINE WHETHER THE PROCESS OR CRITERIA USED BY THE UNIT PROVIDE APPROPRIATE SECURITY AND ARE ALIGNED WITH THE REGULATIONS ADOPTED BY THE DEPARTMENT AS REQUIRED UNDER § 13–405 OF THIS SUBTITLE.

13–408.

(A) EXCEPT AS PROVIDED IN SUBSECTION (B) OF THIS SECTION, A CONTRACT BETWEEN A UNIT AND A CONTRACTOR FOR THE PROCUREMENT OF AN INTERNET–CONNECTED DEVICE SHALL INCLUDE:

(1) A CLAUSE THAT REQUIRES THE CONTRACTOR PROVIDING THE SOFTWARE OR FIRMWARE COMPONENT OF THE INTERNET–CONNECTED DEVICE TO NOTIFY THE UNIT OF ANY KNOWN SECURITY VULNERABILITIES OR DEFECTS SUBSEQUENTLY DISCLOSED TO THE CONTRACTOR BY A SECURITY RESEARCHER OR THAT THE CONTRACTOR OTHERWISE BECOMES AWARE OF DURING THE DURATION OF THE CONTRACT;

(2) A CLAUSE THAT REQUIRES THE INTERNET–CONNECTED DEVICE SOFTWARE OR FIRMWARE TO BE UPDATED OR REPLACED, CONSISTENT WITH OTHER

PROVISIONS IN THE CONTRACT GOVERNING THE TERM OF SUPPORT, IN A MANNER THAT ALLOWS FOR ANY FUTURE SECURITY VULNERABILITY OR DEFECT IN ANY PART OF THE SOFTWARE OR FIRMWARE TO BE PATCHED IN ORDER TO FIX OR REMOVE A VULNERABILITY OR DEFECT IN THE SOFTWARE OR FIRMWARE COMPONENT IN A PROPERLY AUTHENTICATED MANNER;

(3) A CLAUSE THAT REQUIRES THE CONTRACTOR TO PROVIDE A REPAIR OR REPLACEMENT IN A TIMELY MANNER FOR ANY NEW SECURITY VULNERABILITY DISCOVERED THROUGH ANY OF THE DATABASES DESCRIBED IN § 13–403(B)(1) OF THIS SUBTITLE IN THE EVENT THE VULNERABILITY CANNOT BE REMEDIATED THROUGH AN UPDATE DESCRIBED IN ITEM (2) OF THIS SUBSECTION; AND

(4) A CLAUSE THAT REQUIRES THE CONTRACTOR TO PROVIDE THE PURCHASING AGENCY WITH GENERAL INFORMATION ON THE ABILITY OF THE DEVICE TO BE UPDATED, INCLUDING:

(I) THE MANNER IN WHICH THE DEVICE RECEIVES SECURITY UPDATES;

(II) THE ANTICIPATED TIMELINE FOR ENDING SECURITY SUPPORT ASSOCIATED WITH THE INTERNET–CONNECTED DEVICE;

(III) FORMAL NOTIFICATION WHEN SECURITY SUPPORT HAS CEASED; AND

(IV) ANY ADDITIONAL INFORMATION RECOMMENDED BY THE SECRETARY OF INFORMATION TECHNOLOGY.

(B) AFTER CONSULTATION WITH THE DEPARTMENT, A UNIT MAY ALTER THE REQUIREMENTS OF SUBSECTION (A) OF THIS SECTION.

13–409.

(A) EXCEPT AS PROVIDED IN SUBSECTION (B) OF THIS SECTION, A UNIT MAY ENTER INTO A CONTRACT OR ACCEPT A BID OR PROPOSAL ONLY FROM AN INTERNET SERVICE PROVIDER THAT DOES NOT:

(1) BLOCK LAWFUL CONTENT, APPLICATIONS, SERVICES, OR NONHARMFUL DEVICES, SUBJECT TO REASONABLE NETWORK MANAGEMENT;

(2) IMPAIR OR DEGRADE LAWFUL INTERNET TRAFFIC ON THE BASIS OF INTERNET CONTENT, APPLICATION, OR SERVICE, OR USE OF A NONHARMFUL

DEVICE, SUBJECT TO REASONABLE NETWORK MANAGEMENT; AND

(3) ENGAGE IN COMMERCIAL TRAFFIC PREFERENCING, INCLUDING TRAFFIC SHAPING, PRIORITIZATION, RESOURCE RESERVATION, OR OTHER FORMS OF PREFERENTIAL TRAFFIC MANAGEMENT, EITHER:

(I) IN EXCHANGE FOR CONSIDERATION FROM A THIRD PARTY; OR

(II) TO BENEFIT AN AFFILIATED ENTITY.

(B) (1) THE BOARD MAY ESTABLISH A PROCESS TO ALLOW A UNIT TO OBTAIN A WAIVER FROM COMPLYING WITH THE REQUIREMENTS OF SUBSECTION (A) OF THIS SECTION.

(2) THE WAIVER PROCESS SHALL:

(I) INCLUDE A PUBLIC HEARING BEFORE THE BOARD; AND

(II) REQUIRE A MAJORITY VOTE OF THE MEMBERS OF THE BOARD.

(3) THE BOARD SHALL PUBLISH PUBLIC NOTICE OF THE WAIVER ON ITS WEBSITE WITHIN 48 HOURS OF ISSUANCE OF A WAIVER UNDER THIS SUBSECTION.

(4) ON OR BEFORE NOVEMBER 1 EACH YEAR, THE BOARD SHALL REPORT ON ALL WAIVERS ISSUED UNDER THIS SUBSECTION TO THE GENERAL ASSEMBLY, IN ACCORDANCE WITH § 2–1246 OF THE STATE GOVERNMENT ARTICLE.

SECTION 2. AND BE IT FURTHER ENACTED, That:

(a) The Department of Information Technology shall adopt regulations in accordance with Section 1 of this Act on or before October 1, 2019.

(b) In adopting regulations, the Department shall:

(1) include policies and procedures for conducting research on the cybersecurity of an Internet–connected device, which shall be based, in part, on Standard 29147 of the International Standards Organization, or any successor standard, relating to the processing and resolving of potential vulnerability information in a product or online service, including procedures for a contractor or vendor providing an Internet–connected device to the State on how to:

(i) receive information about potential vulnerabilities in the product

or online service of the contractor or vendor; and

(ii) disseminate resolution information about vulnerabilities in the product or online service of the contractor or vendor; and

(2) include a requirement that research on the cybersecurity of an Internet–connected device provided by a contractor to the State shall be conducted on the same class, model, or type of device provided to the State and not on the actual device provided to the State.

SECTION 3. 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–connected devices.

SECTION 4. AND BE IT FURTHER ENACTED, That this Act shall take effect October 1, 2018.