

SENATE BILL 553

C2, P2

9lr0608
CF 9lr2416

By: **Senators Lee, Elfreth, Guzzone, Nathan–Pulliam, Smith, Waldstreicher, Washington, and Young**

Introduced and read first time: February 4, 2019

Assigned to: Finance and Education, Health, and Environmental Affairs

A BILL ENTITLED

1 AN ACT concerning

2 **Security Feature for Connected Devices – Requirements, Procurement**
3 **Preferences, and Reports**

4 FOR the purpose of requiring the manufacturer of a connected device to equip the device
5 with a certain reasonable security feature; providing that a security feature for a
6 connected device is reasonable if the connected device is equipped with a certain
7 means for authentication; authorizing the Attorney General to seek relief against a
8 manufacturer that violates certain provisions of this Act; establishing a certain
9 penalty for certain violations; prohibiting a manufacturer from being fined more
10 than a certain amount for violations arising from a single model of a connected
11 device; providing that certain provisions of law do not create or authorize a private
12 right of action; requiring the Department of Labor, Licensing, and Regulation to
13 report certain information to the Maryland Cybersecurity Council and to the
14 Secretary of General Services; requiring the Secretary of General Services to report
15 the make and model of a certain connected device that violates certain provisions of
16 this Act to certain units that procure supplies on receiving a certain report; altering
17 State procurement law to grant a preference for secure connected devices in State
18 contracting; requiring a public body to require that certain contractors and
19 subcontractors use a secure connected device in the performance of a contract;
20 requiring the Maryland Cybersecurity Council to take reports of violations of certain
21 provisions of this Act into account when performing certain work; providing for the
22 construction of certain provisions of this Act; defining certain terms; providing for a
23 delayed effective date; and generally relating to security features for connected
24 devices.

25 BY adding to
26 Article – Business Regulation
27 Section 19–1001 through 19–1005 to be under the new subtitle “Subtitle 10. Security
28 Feature for Connected Devices”
29 Annotated Code of Maryland

EXPLANATION: CAPITALS INDICATE MATTER ADDED TO EXISTING LAW.

[Brackets] indicate matter deleted from existing law.



1 (2015 Replacement Volume and 2018 Supplement)

2 BY adding to

3 Article – State Finance and Procurement

4 Section 4–317 and 14–417

5 Annotated Code of Maryland

6 (2015 Replacement Volume and 2018 Supplement)

7 BY repealing and reenacting, without amendments,

8 Article – State Government

9 Section 9–2901(b) and (j)

10 Annotated Code of Maryland

11 (2014 Replacement Volume and 2018 Supplement)

12 BY adding to

13 Article – State Government

14 Section 9–2901(k)

15 Annotated Code of Maryland

16 (2014 Replacement Volume and 2018 Supplement)

17 BY repealing and reenacting, with amendments,

18 Article – State Government

19 Section 9–2901(k)

20 Annotated Code of Maryland

21 (2014 Replacement Volume and 2018 Supplement)

22 SECTION 1. BE IT ENACTED BY THE GENERAL ASSEMBLY OF MARYLAND,

23 That the Laws of Maryland read as follows:

24 **Article – Business Regulation**

25 **SUBTITLE 10. SECURITY FEATURE FOR CONNECTED DEVICES.**

26 **19–1001.**

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

29 **(B) “AUTHENTICATION” MEANS A METHOD OF VERIFYING THE AUTHORITY**
30 **OF A USER, PROCESS, OR CONNECTED DEVICE TO ACCESS RESOURCES THROUGH AN**
31 **INFORMATION SYSTEM.**

32 **(C) “CONNECTED DEVICE” MEANS A PHYSICAL OBJECT THAT IS:**

33 **(1) CAPABLE OF CONNECTING TO THE INTERNET, DIRECTLY OR**
34 **INDIRECTLY; AND**

1 **(2) ASSIGNED AN INTERNET PROTOCOL ADDRESS OR BLUETOOTH**
2 **ADDRESS.**

3 **(D) (1) “MANUFACTURER” MEANS A PERSON WHO:**

4 **(I) MANUFACTURES OR ASSEMBLES A NEW CONNECTED**
5 **DEVICE FOR SALE OR DISTRIBUTION; OR**

6 **(II) CONTRACTS WITH ANOTHER PERSON TO MANUFACTURE OR**
7 **ASSEMBLE A CONNECTED DEVICE ON THAT PERSON’S BEHALF.**

8 **(2) “MANUFACTURER” DOES NOT INCLUDE A PERSON WHO**
9 **CONTRACTS WITH ANOTHER PERSON TO PURCHASE AND BRAND A CONNECTED**
10 **DEVICE.**

11 **(E) “SECURITY FEATURE” MEANS AN ATTRIBUTE OF HARDWARE,**
12 **FIRMWARE, SOFTWARE, PROCESS, PROCEDURE, OR A COMBINATION OF THESE**
13 **FACTORS THAT COULD PREVENT OR LESSEN THE FAILURE OR COMPROMISE OF THE**
14 **CONFIDENTIALITY, INTEGRITY, OR ACCESSIBILITY OF A CONNECTED DEVICE OR**
15 **INFORMATION STORED WITHIN A CONNECTED DEVICE.**

16 **(F) “UNAUTHORIZED ACCESS” MEANS ANY USE, MODIFICATION,**
17 **DISCLOSURE, OR DESTRUCTION OF ANY INFORMATION STORED WITHIN A**
18 **CONNECTED DEVICE THAT IS NOT AUTHORIZED BY THE OWNER OF THE CONNECTED**
19 **DEVICE.**

20 **19-1002.**

21 **THIS SUBTITLE MAY NOT BE CONSTRUED TO IMPOSE ANY DUTY ON:**

22 **(1) A MANUFACTURER OF A CONNECTED DEVICE FOR AN**
23 **UNAUTHORIZED ACCESS THAT ARISES FROM AN UNAFFILIATED THIRD-PARTY**
24 **SOFTWARE OR APPLICATION THAT A USER ADDS TO A CONNECTED DEVICE;**

25 **(2) A MANUFACTURER TO PREVENT A USER FROM HAVING FULL**
26 **CONTROL OVER A CONNECTED DEVICE, INCLUDING BY ALLOWING A USER TO**
27 **MODIFY THE SOFTWARE OR FIRMWARE RUNNING ON THE CONNECTED DEVICE; OR**

28 **(3) THE OPERATOR OF AN ELECTRONIC STORE, AN ELECTRONIC**
29 **MARKETPLACE, OR ANY OTHER MEANS OF PURCHASING OR DOWNLOADING**
30 **SOFTWARE OR APPLICATIONS TO ENFORCE COMPLIANCE WITH THIS SUBTITLE.**

1 **19-1003.**

2 (A) A MANUFACTURER OF A CONNECTED DEVICE SHALL EQUIP THE DEVICE
3 WITH A REASONABLE SECURITY FEATURE THAT IS:

4 (1) APPROPRIATE TO THE NATURE AND FUNCTION OF THE
5 CONNECTED DEVICE;

6 (2) APPROPRIATE TO THE INFORMATION THE CONNECTED DEVICE
7 COLLECTS, CONTAINS, OR TRANSMITS; AND

8 (3) DESIGNED TO PROTECT THE CONNECTED DEVICE FROM
9 UNAUTHORIZED ACCESS, DESTRUCTION, OR MODIFICATION.

10 (B) A CONNECTED DEVICE HAS A REASONABLE SECURITY FEATURE FOR
11 THE PURPOSE OF THIS SUBTITLE IF:

12 (1) THE SECURITY FEATURE MEETS THE REQUIREMENTS UNDER
13 SUBSECTION (A) OF THIS SECTION; AND

14 (2) THE CONNECTED DEVICE IS EQUIPPED WITH A MEANS FOR
15 AUTHENTICATION OUTSIDE OF A LOCAL AREA NETWORK THAT INCLUDES:

16 (I) A PREPROGRAMMED PASSWORD THAT IS UNIQUE TO EACH
17 MANUFACTURED CONNECTED DEVICE; OR

18 (II) A PROCESS THAT REQUIRES THE USER TO GENERATE A NEW
19 MEANS OF AUTHENTICATION BEFORE THE USER IS GRANTED ACCESS TO THE
20 CONNECTED DEVICE FOR THE FIRST TIME.

21 **19-1004.**

22 (A) THE ATTORNEY GENERAL MAY SEEK RELIEF AGAINST A
23 MANUFACTURER THAT VIOLATES THIS SUBTITLE IN ACCORDANCE WITH THIS
24 SECTION.

25 (B) (1) SUBJECT TO PARAGRAPH (2) OF THIS SUBSECTION, FOR EACH
26 CONNECTED DEVICE THAT DOES NOT HAVE A REASONABLE SECURITY FEATURE AS
27 REQUIRED BY § 19-1003 OF THIS SUBTITLE, THE MANUFACTURER OF A CONNECTED
28 DEVICE IS SUBJECT TO A SEPARATE CIVIL PENALTY OF \$1,000.

29 (2) A MANUFACTURER MAY NOT BE FINED MORE THAN \$100,000 FOR
30 VIOLATIONS ARISING FROM A SINGLE MODEL OF A CONNECTED DEVICE.

1 (C) THIS SUBTITLE DOES NOT CREATE OR AUTHORIZE A PRIVATE RIGHT OF
2 ACTION.

3 19-1005.

4 (A) THE DEPARTMENT SHALL SEND TO THE MARYLAND CYBERSECURITY
5 COUNCIL A REPORT ON ANY VIOLATION OF THIS SUBTITLE THAT INCLUDES:

6 (1) THE NAME OF THE MANUFACTURER RESPONSIBLE; AND

7 (2) THE NATURE OF THE VIOLATION.

8 (B) THE DEPARTMENT SHALL REPORT THE MAKE AND MODEL OF A
9 CONNECTED DEVICE THAT VIOLATES THIS SUBTITLE TO THE SECRETARY OF
10 GENERAL SERVICES.

11 Article – State Finance and Procurement

12 4-317.

13 ON RECEIVING A REPORT FROM THE DEPARTMENT OF LABOR, LICENSING,
14 AND REGULATION UNDER § 19-1005 OF THE BUSINESS REGULATION ARTICLE, THE
15 SECRETARY SHALL REPORT THE MAKE AND MODEL OF A CONNECTED DEVICE THAT
16 VIOLATES TITLE 19, SUBTITLE 10 OF THE BUSINESS REGULATION ARTICLE TO
17 EACH UNIT THAT PROCURES SUPPLIES UNDER DIVISION II OF THIS ARTICLE.

18 14-417.

19 (A) (1) IN THIS SECTION THE FOLLOWING WORDS HAVE THE MEANINGS
20 INDICATED.

21 (2) “INSECURE CONNECTED DEVICE” MEANS A CONNECTED DEVICE
22 THAT THE DEPARTMENT OF LABOR, LICENSING, AND REGULATION HAS
23 DETERMINED VIOLATES TITLE 19, SUBTITLE 10 OF THE BUSINESS REGULATION
24 ARTICLE UNDER § 4-317 OF THIS ARTICLE.

25 (2) “PUBLIC BODY” MEANS:

26 (I) A UNIT;

27 (II) A COUNTY;

1 (III) A MUNICIPALITY IN THE STATE;

2 (IV) A SCHOOL DISTRICT IN THE STATE; OR

3 (V) A SPECIAL DISTRICT IN THE STATE.

4 (3) "SECURE CONNECTED DEVICE" MEANS A PHYSICAL OBJECT THAT
5 IS:

6 (I) NOT AN INSECURE CONNECTED DEVICE;

7 (II) CAPABLE OF CONNECTING TO THE INTERNET, DIRECTLY OR
8 INDIRECTLY; AND

9 (III) ASSIGNED AN INTERNET PROTOCOL ADDRESS OR
10 BLUETOOTH ADDRESS.

11 (B) EXCEPT AS PROVIDED IN SUBSECTION (C) OF THIS SECTION, A PUBLIC
12 BODY SHALL REQUIRE A CONTRACTOR OR SUBCONTRACTOR TO USE A SECURE
13 CONNECTED DEVICE IN THE PERFORMANCE OF A CONTRACT.

14 (C) THIS SECTION DOES NOT APPLY IF THE HEAD OF A PUBLIC BODY
15 DETERMINES THAT:

16 (1) THE PRICE OF A SECURE CONNECTED DEVICE EXCEEDS THE
17 PRICE OF A SIMILAR INSECURE CONNECTED DEVICE BY AN UNREASONABLE
18 AMOUNT;

19 (2) A SECURE CONNECTED DEVICE IS NOT AVAILABLE FOR PURCHASE
20 IN REASONABLY AVAILABLE QUANTITIES;

21 (3) THE QUALITY OF A SECURE CONNECTED DEVICE IS
22 SUBSTANTIALLY LESS THAN THE QUALITY OF A COMPARABLY PRICED, SIMILAR, AND
23 AVAILABLE INSECURE CONNECTED DEVICE; OR

24 (4) THE PROCUREMENT OF A SECURE CONNECTED DEVICE WOULD BE
25 INCONSISTENT WITH THE PUBLIC INTEREST.

26 Article – State Government

27 9–2901.

28 (b) There is a Maryland Cybersecurity Council.

1 (j) The Council shall work with the National Institute of Standards and
2 Technology and other federal agencies, private sector businesses, and private cybersecurity
3 experts to:

4 (1) for critical infrastructure not covered by federal law or the Executive
5 Order, review and conduct risk assessments to determine which local infrastructure sectors
6 are at the greatest risk of cyber attacks and need the most enhanced cybersecurity
7 measures;

8 (2) use federal guidance to identify categories of critical infrastructure as
9 critical cyber infrastructure if cyber damage or unauthorized cyber access to the
10 infrastructure could reasonably result in catastrophic consequences, including:

11 (i) interruption in the provision of energy, water, transportation,
12 emergency services, food, or other life-sustaining services sufficient to cause a mass
13 casualty event or mass evacuations;

14 (ii) catastrophic economic damage; or

15 (iii) severe degradation of State or national security;

16 (3) assist infrastructure entities that are not covered by the Executive
17 Order in complying with federal cybersecurity guidance;

18 (4) assist private sector cybersecurity businesses in adopting, adapting,
19 and implementing the National Institute of Standards and Technology cybersecurity
20 framework of standards and practices;

21 (5) examine inconsistencies between State and federal laws regarding
22 cybersecurity;

23 (6) recommend a comprehensive State strategic plan to ensure a
24 coordinated and adaptable response to and recovery from cybersecurity attacks; and

25 (7) recommend any legislative changes considered necessary by the
26 Council to address cybersecurity issues.

27 **(K) THE COUNCIL SHALL TAKE REPORTS OF ANY VIOLATIONS OF TITLE 19,**
28 **SUBTITLE 10 OF THE BUSINESS REGULATION ARTICLE INTO ACCOUNT WHEN**
29 **PERFORMING ITS WORK UNDER SUBSECTION (J) OF THIS SECTION.**

30 **[(k)] (L)** Beginning July 1, 2017, and every 2 years thereafter, the Council shall
31 submit a report of its activities to the General Assembly in accordance with § 2-1246 of this
32 article.

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