

# SENATE BILL 553

P1

8lr1162

---

By: **Senator Simonaire**

Introduced and read first time: January 31, 2018

Assigned to: Education, Health, and Environmental Affairs

---

## A BILL ENTITLED

1 AN ACT concerning

2 **State Government – Security Training – Protection of Security–Sensitive Data**

3 FOR the purpose of altering the aspects of State information technology that are to be  
4 included in the statewide information technology master plan developed and  
5 maintained by the Secretary of Information Technology; requiring the Secretary to  
6 develop, maintain, and revise certain security training material; requiring each unit  
7 of State government to develop a plan to identify unit personnel who handle  
8 security–sensitive data and establish certain security training for each employee  
9 who handles security–sensitive data as part of the employee’s duties; defining a  
10 certain term; requiring each unit of State government to submit a certain plan to the  
11 Governor and the Department of Information Technology on or before a certain date;  
12 and generally relating to security training for employees of units of State  
13 government.

14 BY repealing and reenacting, with amendments,  
15 Article – State Finance and Procurement  
16 Section 3A–303 to be under the amended subtitle “Subtitle 3. Information Processing  
17 and Security”  
18 Annotated Code of Maryland  
19 (2015 Replacement Volume and 2017 Supplement)

20 BY adding to  
21 Article – State Finance and Procurement  
22 Section 3A–314  
23 Annotated Code of Maryland  
24 (2015 Replacement Volume and 2017 Supplement)

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

27 **Article – State Finance and Procurement**

---

EXPLANATION: CAPITALS INDICATE MATTER ADDED TO EXISTING LAW.

[Brackets] indicate matter deleted from existing law.



1 Subtitle 3. Information Processing **AND SECURITY.**

2 3A-303.

3 The Secretary is responsible for carrying out the following duties:

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

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

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

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

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

14 (ii) include all aspects of State information technology including  
15 telecommunications, **SECURITY**, data processing, and information management;

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

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

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

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

26 (5) adopting by regulation and enforcing nonvisual access standards to be  
27 used in the procurement of information technology services by or on behalf of units of State  
28 government; **AND**

29 **(6) DEVELOPING, MAINTAINING, AND REVISING SECURITY TRAINING**  
30 **MATERIAL THAT:**

1                   **(I)    FOCUSES ON ENSURING DATA PROTECTION AND INTEGRITY;**  
2 **AND**

3                   **(II)   CAN BE USED BY THE GOVERNOR AND ANY UNIT OF STATE**  
4 **GOVERNMENT.**

5 **3A-314.**

6           **(A)    IN THIS SECTION, “SECURITY-SENSITIVE DATA” MEANS INFORMATION**  
7 **THAT IS PROTECTED AGAINST UNWARRANTED DISCLOSURE.**

8           **(B)    IN ACCORDANCE WITH GUIDELINES ESTABLISHED BY THE SECRETARY,**  
9 **EACH UNIT OF STATE GOVERNMENT SHALL DEVELOP A PLAN TO:**

10                   **(1)    IDENTIFY UNIT PERSONNEL WHO HANDLE SECURITY-SENSITIVE**  
11 **DATA; AND**

12                   **(2)    ESTABLISH ANNUAL SECURITY OVERVIEW TRAINING OR**  
13 **REFRESHER SECURITY TRAINING FOR EACH EMPLOYEE WHO HANDLES**  
14 **SECURITY-SENSITIVE DATA AS PART OF THE EMPLOYEE’S DUTIES.**

15           SECTION 2. AND BE IT FURTHER ENACTED, That, on or before December 31,  
16 2018, each unit of State government shall submit the plan developed under § 3A-314 of the  
17 State Finance and Procurement Article, as enacted by Section 1 of this Act, to the Governor  
18 and the Department of Information Technology.

19           SECTION 3. AND BE IT FURTHER ENACTED, That this Act shall take effect June  
20 1, 2018.