Chapter 467

(Senate Bill 553)

AN ACT concerning

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

FOR the purpose of altering the aspects of State information technology that are to be included in the statewide information technology master plan developed and maintained by the Secretary of Information Technology; ~~requiring the Secretary to develop, maintain, and revise certain security training material;~~ requiring each unit of State government to develop a plan to identify unit personnel who handle security–sensitive data and establish certain security training for each employee who handles security–sensitive data as part of the employee's duties; defining a certain term; requiring each unit of State government to submit a certain plan to ~~the Governor and~~ the Department of Information Technology on or before a certain date; requiring the Department to develop a certain plan and report certain information to the Governor and certain committees of the General Assembly on or before a certain date; and generally relating to security training for employees of units of State government.

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

BY adding to
Article – State Finance and Procurement
Section 3A–314
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 3. Information Processing **AND SECURITY**.

3A–303.

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~~; AND~~

~~(6) DEVELOPING, MAINTAINING, AND REVISING SECURITY TRAINING MATERIAL THAT:~~

~~(I) FOCUSES ON ENSURING DATA PROTECTION AND INTEGRITY; AND~~

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

3A–314.

(A) IN THIS SECTION, "SECURITY–SENSITIVE DATA" MEANS INFORMATION THAT IS PROTECTED AGAINST UNWARRANTED DISCLOSURE.

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

(1) IDENTIFY UNIT PERSONNEL WHO HANDLE SECURITY–SENSITIVE DATA; AND

(2) ESTABLISH ANNUAL SECURITY OVERVIEW TRAINING OR REFRESHER SECURITY TRAINING FOR EACH EMPLOYEE WHO HANDLES SECURITY–SENSITIVE DATA AS PART OF THE EMPLOYEE'S DUTIES.

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

SECTION 3. AND BE IT FURTHER ENACTED, That, on or before January 31, 2019, the Department of Information Technology shall:

(1) develop a plan to develop, maintain, and revise security training material that:

(i) focuses on ensuring data protection and integrity; and

(ii) can be used by the Governor and any unit of State government; and

(2) report to the Governor and, in accordance with § 2–1246 of the State Government Article, the Senate Education, Health, and Environmental Affairs Committee and the House Health and Government Operations Committee on:

(i) the number of personnel who handle security–sensitive data identified by each unit of State government; and

(ii) the total additional number of identified training licenses required to implement the plan developed under item (1) of this section beyond the Department's existing training license growth projections.

SECTION ~~3.~~ 4. AND BE IT FURTHER ENACTED, That this Act shall take effect June 1, 2018.

Approved by the Governor, May 8, 2018.