SENATE BILL 107

By: Senator Jackson
Requested: October 12, 2021
Introduced and read first time: January 12, 2022
Assigned to: Education, Health, and Environmental Affairs

A BILL ENTITLED

AN ACT concerning

State Government – State and Local Government Employees and Contractors – Cybersecurity Training

FOR the purpose of making certain provisions of law governing the protection of information by government agencies applicable to the Legislative and Judicial branches of State government; requiring the Maryland Cybersecurity Coordinating Council to develop a Cybersecurity Awareness and Training Program; establishing certain criteria for the Program; requiring the State Chief Information Security Officer to coordinate with the Council to certify certain cybersecurity trainings; establishing certain criteria for the cybersecurity trainings; requiring, on or after a certain date, certain unit employees and certain contractors to complete cybersecurity trainings under certain circumstances; authorizing chief executives of local units to select certain cybersecurity trainings; requiring chief executives of local units to follow certain verification and reporting procedures for cybersecurity trainings; requiring chief executives of State units to follow certain verification procedures for cybersecurity trainings; requiring the Secretary of Information Technology to conduct certain periodic assessments; requiring certain contracts to include a cybersecurity training mandate on or after a certain date; and generally relating to cybersecurity training for State and local government employees and contractors.

BY repealing and reenacting, without amendments,

Article – State Government
Section 10–1301(a) and (d)
Annotated Code of Maryland
(2021 Replacement Volume)

BY repealing and reenacting, with amendments,

Article – State Government
Section 10–1301(f) and 10–1302

EXPLANATION: CAPITALS INDICATE MATTER ADDED TO EXISTING LAW.
[Brackets] indicate matter deleted from existing law.
SENATE BILL 107

Annotated Code of Maryland
(2021 Replacement Volume)

BY adding to
Article – State Government
Section 10–13B–01 through 10–13B–04 to be under the new subtitle “Subtitle 13B. Cybersecurity Training”
Annotated Code of Maryland
(2021 Replacement Volume)

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

Article – State Government

10–1301.

(a) In this subtitle the following words have the meanings indicated.

(d) “Reasonable security procedures and practices” means data security procedures and practices developed, in good faith, and set forth in a written information security policy.

(f) “Unit” means:

(1) an executive agency, or a department, a board, a commission, an authority, a public institution of higher education, a unit or an instrumentality of the State;

(2) AN AGENCY, A DEPARTMENT, OR A UNIT OF THE LEGISLATIVE BRANCH OF STATE GOVERNMENT;

(3) AN AGENCY, A DEPARTMENT, OR A UNIT OF THE JUDICIAL BRANCH OF STATE GOVERNMENT; OR

(4) a county, municipality, bi-county, regional, or multicounty agency, county board of education, public corporation or authority, or any other political subdivision of the State.

10–1302.

[(a)] This subtitle does not apply to personal information that:

(1) is publicly available information that is lawfully made available to the general public from federal, State, or local government records;
(2) an individual has consented to have publicly disseminated or listed;

(3) except for a medical record that a person is prohibited from redisclosing under § 4–302(d) of the Health – General Article, is disclosed in accordance with the federal Health Insurance Portability and Accountability Act; or

(4) is disclosed in accordance with the federal Family Educational Rights and Privacy Act.

(b) This subtitle does not apply to the Legislative or Judicial Branch of State government.]

SUBTITLE 13B. CYBERSECURITY TRAINING.

10–13B–01.

(A) In this subtitle the following words have the meanings indicated.

(B) “COUNCIL” means the MARYLAND CYBERSECURITY COORDINATING COUNCIL.

(C) “CYBERSECURITY AWARENESS” means organizational and individual attention to cybersecurity concerns and appropriate responses.

(D) “CYBERSECURITY TRAINING” means a formal course of activities focused on:

(1) informing personnel of their roles and responsibilities within a particular information technology plan; and

(2) building the knowledge and skills to effectively perform those roles and responsibilities.

(E) “CYBERSECURITY TRAINING ASSESSMENT” means an audit of cybersecurity trainings under the Program.

(F) “DEPARTMENT” means the DEPARTMENT OF INFORMATION TECHNOLOGY.

(G) “PROGRAM” means the CYBERSECURITY AWARENESS AND TRAINING PROGRAM.
(H) “Reasonable security procedures and practices” has the meaning stated in § 10–1301 of this title.

(I) “Unit” has the meaning stated in § 10–1301 of this title.

10–13B–02.

(A) (1) The Council shall develop a Cybersecurity Awareness and Training Program.

(2) The Program shall include a course of periodic cybersecurity awareness and cybersecurity training activities, each of which includes cybersecurity training assessments.

(B) (1) The State Chief Information Security Officer, in coordination with the Council, shall annually:

(i) certify cybersecurity trainings for use under the Program; and

(ii) update standards for the maintenance of cybersecurity trainings under this section.

(2) The Council shall determine the number of cybersecurity trainings to be certified under paragraph (1)(i) of this subsection.

(3) The Council shall provide minimum standards for cybersecurity training content.

(C) The criteria used to certify a cybersecurity training under subsection (b)(1)(i) of this section shall include requirements that each cybersecurity training include activities, hypothetical situations, and other methods that:

(1) aim to increase the participant’s cybersecurity awareness;

(2) focus on forming information security habits and reasonable security procedures and practices that protect information resources, personal information, and records; and

(3) teach best practices for detecting, assessing,
REPORTING, AND ADDRESSING INFORMATION SECURITY THREATS.

(d) The State Chief Information Security Officer may contract with a third party to certify cybersecurity trainings under this section.

(e) Beginning October 1, 2023, the Council shall annually publish on the Department’s website a list of cybersecurity trainings certified under this section.

10–13B–03.

(a) This section and §10–13B–04 of this subtitle apply on or after October 1, 2023.

(b)(1) Each employee of a unit shall complete a certified cybersecurity training if that employee’s job duties include accessing a State or local government computer system or database.

(2) The Council shall ensure that each employee completes a cybersecurity training under the Program at least four times each year.

(c)(1) The chief executive of a local unit may select the most appropriate certified cybersecurity training for employees of the local unit.

(2) The chief executive of a local unit shall:

(i) Verify the completion of a cybersecurity training by employees of the local unit and report the completion to the State Chief Information Security Officer or the State Chief Information Security Officer’s designee; and

(ii) Require periodic cybersecurity training assessments to ensure compliance with this section.

(d)(1) The chief executive of a State unit shall verify completion of a cybersecurity training under the Program by employees of the unit.

(2) The State Chief Information Security Officer shall determine the method by which a chief executive shall verify
COMPLETION OF A CYBERSECURITY TRAINING UNDER PARAGRAPH (1) OF THIS SUBSECTION.

(E) (1) A unit may require employees whose job duties do not include accessing a State or local government computer system or database to complete a cybersecurity training under § 10–13B–02 of this subtitle.

(2) If a unit requires employees to complete a cybersecurity training, the unit shall select a training based on its relevance to the work or responsibilities of its employees.

(3) A unit may set different cybersecurity training requirements for its employees based on the position or title of the employee.

(F) The Secretary of Information Technology shall conduct periodic cybersecurity training assessments of State units to ensure compliance with this section.

10–13B–04.

(A) In this section, “contractor” includes a contractor, a subcontractor, an officer of a contractor or subcontractor, or an employee of a contractor or subcontractor.

(B) The State Chief Information Security Officer shall approve a cybersecurity training certified under § 10–13B–02 of this subtitle for contractors whose job duties include accessing a State or local government computer system or database.

(C) (1) A contractor who accesses a State or local government computer system or database that is awarded a contract by a unit shall complete a cybersecurity training approved for contractors under this section.

(2) A contractor shall complete an approved cybersecurity training before beginning work under a contract and before any contract renewal term.

(3) A contractor shall verify completion of the cybersecurity training to the appropriate unit.
(4) AN EMPLOYEE OF A UNIT WHO OVERSEES A CONTRACTOR SHALL:

(I) REPORT THE CONTRACTOR’S COMPLETION OF THE CYBERSECURITY TRAINING TO THE STATE CHIEF INFORMATION SECURITY OFFICER OR THE STATE CHIEF INFORMATION SECURITY OFFICER’S DESIGNEE;

AND

(II) CONDUCT PERIODIC CYBERSECURITY TRAINING ASSESSMENTS TO ENSURE COMPLIANCE WITH THIS SECTION.

SECTION 2. AND BE IT FURTHER ENACTED, That on or before April 1, 2023, the Maryland Cybersecurity Coordinating Council shall develop standards that the Cybersecurity Awareness and Training Program and the cybersecurity trainings developed under § 10–13B–02 of the State Government Article, as enacted under Section 1 of this Act, shall meet to receive certification.

SECTION 3. AND BE IT FURTHER ENACTED, That this Act shall be construed to apply only prospectively and may not be applied or interpreted to have any effect on or application to any contract executed before the effective date of this Act.

SECTION 4. AND BE IT FURTHER ENACTED, That this Act shall take effect October 1, 2022.