

# HOUSE BILL 5

P1, S2

(PRE-FILED)

2lr0735  
CF 2lr0736

---

By: **Delegate Krimm**

Requested: October 12, 2021

Introduced and read first time: January 12, 2022

Assigned to: Health and Government Operations

---

## A BILL ENTITLED

1 AN ACT concerning

2 **State Government – State and Local Government Employees and Contractors –**  
3 **Cybersecurity Training**

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

21 BY repealing and reenacting, without amendments,  
22 Article – State Government  
23 Section 10–1301(a) and (d)  
24 Annotated Code of Maryland  
25 (2021 Replacement Volume)

26 BY repealing and reenacting, with amendments,  
27 Article – State Government  
28 Section 10–1301(f) and 10–1302

---

EXPLANATION: CAPITALS INDICATE MATTER ADDED TO EXISTING LAW.

[Brackets] indicate matter deleted from existing law.



1 Annotated Code of Maryland  
2 (2021 Replacement Volume)

3 BY adding to  
4 Article – State Government  
5 Section 10–13B–01 through 10–13B–04 to be under the new subtitle “Subtitle 13B.  
6 Cybersecurity Training”  
7 Annotated Code of Maryland  
8 (2021 Replacement Volume)

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

11 **Article – State Government**

12 10–1301.

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

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

17 (f) “Unit” means:

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

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

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

25 **[(2)] (4)** a county, municipality, bi–county, regional, or multicounty  
26 agency, county board of education, public corporation or authority, or any other political  
27 subdivision of the State.

28 10–1302.

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

30 (1) is publicly available information that is lawfully made available to the  
31 general public from federal, State, or local government records;

1 (2) an individual has consented to have publicly disseminated or listed;

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

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

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

9 **SUBTITLE 13B. CYBERSECURITY TRAINING.**

10 **10-13B-01.**

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

13 (B) “COUNCIL” MEANS THE MARYLAND CYBERSECURITY COORDINATING  
14 COUNCIL.

15 (C) “CYBERSECURITY AWARENESS” MEANS ORGANIZATIONAL AND  
16 INDIVIDUAL ATTENTION TO CYBERSECURITY CONCERNS AND APPROPRIATE  
17 RESPONSES.

18 (D) “CYBERSECURITY TRAINING” MEANS A FORMAL COURSE OF ACTIVITIES  
19 FOCUSED ON:

20 (1) INFORMING PERSONNEL OF THEIR ROLES AND RESPONSIBILITIES  
21 WITHIN A PARTICULAR INFORMATION TECHNOLOGY PLAN; AND

22 (2) BUILDING THE KNOWLEDGE AND SKILLS TO EFFECTIVELY  
23 PERFORM THOSE ROLES AND RESPONSIBILITIES.

24 (E) “CYBERSECURITY TRAINING ASSESSMENT” MEANS AN AUDIT OF  
25 CYBERSECURITY TRAININGS UNDER THE PROGRAM.

26 (F) “DEPARTMENT” MEANS THE DEPARTMENT OF INFORMATION  
27 TECHNOLOGY.

28 (G) “PROGRAM” MEANS THE CYBERSECURITY AWARENESS AND TRAINING  
29 PROGRAM.

1           **(H) “REASONABLE SECURITY PROCEDURES AND PRACTICES” HAS THE**  
2 **MEANING STATED IN § 10–1301 OF THIS TITLE.**

3           **(I) “UNIT” HAS THE MEANING STATED IN § 10–1301 OF THIS TITLE.**

4 **10–13B–02.**

5           **(A) (1) THE COUNCIL SHALL DEVELOP A CYBERSECURITY AWARENESS**  
6 **AND TRAINING PROGRAM.**

7                   **(2) THE PROGRAM SHALL INCLUDE A COURSE OF PERIODIC**  
8 **CYBERSECURITY AWARENESS AND CYBERSECURITY TRAINING ACTIVITIES, EACH OF**  
9 **WHICH INCLUDES CYBERSECURITY TRAINING ASSESSMENTS.**

10           **(B) (1) THE STATE CHIEF INFORMATION SECURITY OFFICER, IN**  
11 **COORDINATION WITH THE COUNCIL, SHALL ANNUALLY:**

12                           **(I) CERTIFY CYBERSECURITY TRAININGS FOR USE UNDER THE**  
13 **PROGRAM; AND**

14                           **(II) UPDATE STANDARDS FOR THE MAINTENANCE OF**  
15 **CYBERSECURITY TRAININGS UNDER THIS SECTION.**

16                   **(2) THE COUNCIL SHALL DETERMINE THE NUMBER OF**  
17 **CYBERSECURITY TRAININGS TO BE CERTIFIED UNDER PARAGRAPH (1)(I) OF THIS**  
18 **SUBSECTION.**

19                   **(3) THE COUNCIL SHALL PROVIDE MINIMUM STANDARDS FOR**  
20 **CYBERSECURITY TRAINING CONTENT.**

21           **(C) THE CRITERIA USED TO CERTIFY A CYBERSECURITY TRAINING UNDER**  
22 **SUBSECTION (B)(1)(I) OF THIS SECTION SHALL INCLUDE REQUIREMENTS THAT**  
23 **EACH CYBERSECURITY TRAINING INCLUDE ACTIVITIES, HYPOTHETICAL**  
24 **SITUATIONS, AND OTHER METHODS THAT:**

25                           **(1) AIM TO INCREASE THE PARTICIPANT’S CYBERSECURITY**  
26 **AWARENESS;**

27                           **(2) FOCUS ON FORMING INFORMATION SECURITY HABITS AND**  
28 **REASONABLE SECURITY PROCEDURES AND PRACTICES THAT PROTECT**  
29 **INFORMATION RESOURCES, PERSONAL INFORMATION, AND RECORDS; AND**

30                           **(3) TEACH BEST PRACTICES FOR DETECTING, ASSESSING,**

1 REPORTING, AND ADDRESSING INFORMATION SECURITY THREATS.

2 (D) THE STATE CHIEF INFORMATION SECURITY OFFICER MAY CONTRACT  
3 WITH A THIRD PARTY TO CERTIFY CYBERSECURITY TRAININGS UNDER THIS  
4 SECTION.

5 (E) BEGINNING OCTOBER 1, 2023, THE COUNCIL SHALL ANNUALLY  
6 PUBLISH ON THE DEPARTMENT'S WEBSITE A LIST OF CYBERSECURITY TRAININGS  
7 CERTIFIED UNDER THIS SECTION.

8 10-13B-03.

9 (A) THIS SECTION AND § 10-13B-04 OF THIS SUBTITLE APPLY ON OR AFTER  
10 OCTOBER 1, 2023.

11 (B) (1) EACH EMPLOYEE OF A UNIT SHALL COMPLETE A CERTIFIED  
12 CYBERSECURITY TRAINING IF THAT EMPLOYEE'S JOB DUTIES INCLUDE ACCESSING  
13 A STATE OR LOCAL GOVERNMENT COMPUTER SYSTEM OR DATABASE.

14 (2) THE COUNCIL SHALL ENSURE THAT EACH EMPLOYEE COMPLETES  
15 A CYBERSECURITY TRAINING UNDER THE PROGRAM AT LEAST FOUR TIMES EACH  
16 YEAR.

17 (C) (1) THE CHIEF EXECUTIVE OF A LOCAL UNIT MAY SELECT THE MOST  
18 APPROPRIATE CERTIFIED CYBERSECURITY TRAINING FOR EMPLOYEES OF THE  
19 LOCAL UNIT.

20 (2) THE CHIEF EXECUTIVE OF A LOCAL UNIT SHALL:

21 (I) VERIFY THE COMPLETION OF A CYBERSECURITY TRAINING  
22 BY EMPLOYEES OF THE LOCAL UNIT AND REPORT THE COMPLETION TO THE STATE  
23 CHIEF INFORMATION SECURITY OFFICER OR THE STATE CHIEF INFORMATION  
24 SECURITY OFFICER'S DESIGNEE; AND

25 (II) REQUIRE PERIODIC CYBERSECURITY TRAINING  
26 ASSESSMENTS TO ENSURE COMPLIANCE WITH THIS SECTION.

27 (D) (1) THE CHIEF EXECUTIVE OF A STATE UNIT SHALL VERIFY  
28 COMPLETION OF A CYBERSECURITY TRAINING UNDER THE PROGRAM BY  
29 EMPLOYEES OF THE UNIT.

30 (2) THE STATE CHIEF INFORMATION SECURITY OFFICER SHALL  
31 DETERMINE THE METHOD BY WHICH A CHIEF EXECUTIVE SHALL VERIFY

1 COMPLETION OF A CYBERSECURITY TRAINING UNDER PARAGRAPH (1) OF THIS  
2 SUBSECTION.

3 (E) (1) A UNIT MAY REQUIRE EMPLOYEES WHOSE JOB DUTIES DO NOT  
4 INCLUDE ACCESSING A STATE OR LOCAL GOVERNMENT COMPUTER SYSTEM OR  
5 DATABASE TO COMPLETE A CYBERSECURITY TRAINING UNDER § 10-13B-02 OF THIS  
6 SUBTITLE.

7 (2) IF A UNIT REQUIRES EMPLOYEES TO COMPLETE A  
8 CYBERSECURITY TRAINING, THE UNIT SHALL SELECT A TRAINING BASED ON ITS  
9 RELEVANCE TO THE WORK OR RESPONSIBILITIES OF ITS EMPLOYEES.

10 (3) A UNIT MAY SET DIFFERENT CYBERSECURITY TRAINING  
11 REQUIREMENTS FOR ITS EMPLOYEES BASED ON THE POSITION OR TITLE OF THE  
12 EMPLOYEE.

13 (F) THE SECRETARY OF INFORMATION TECHNOLOGY SHALL CONDUCT  
14 PERIODIC CYBERSECURITY TRAINING ASSESSMENTS OF STATE UNITS TO ENSURE  
15 COMPLIANCE WITH THIS SECTION.

16 10-13B-04.

17 (A) IN THIS SECTION, "CONTRACTOR" INCLUDES A CONTRACTOR, A  
18 SUBCONTRACTOR, AN OFFICER OF A CONTRACTOR OR SUBCONTRACTOR, OR AN  
19 EMPLOYEE OF A CONTRACTOR OR SUBCONTRACTOR.

20 (B) THE STATE CHIEF INFORMATION SECURITY OFFICER SHALL APPROVE  
21 A CYBERSECURITY TRAINING CERTIFIED UNDER § 10-13B-02 OF THIS SUBTITLE  
22 FOR CONTRACTORS WHOSE JOB DUTIES INCLUDE ACCESSING A STATE OR LOCAL  
23 GOVERNMENT COMPUTER SYSTEM OR DATABASE.

24 (C) (1) A CONTRACTOR WHO ACCESSES A STATE OR LOCAL GOVERNMENT  
25 COMPUTER SYSTEM OR DATABASE THAT IS AWARDED A CONTRACT BY A UNIT SHALL  
26 COMPLETE A CYBERSECURITY TRAINING APPROVED FOR CONTRACTORS UNDER  
27 THIS SECTION.

28 (2) A CONTRACTOR SHALL COMPLETE AN APPROVED  
29 CYBERSECURITY TRAINING BEFORE BEGINNING WORK UNDER A CONTRACT AND  
30 BEFORE ANY CONTRACT RENEWAL TERM.

31 (3) A CONTRACTOR SHALL VERIFY COMPLETION OF THE  
32 CYBERSECURITY TRAINING TO THE APPROPRIATE UNIT.

1           **(4) AN EMPLOYEE OF A UNIT WHO OVERSEES A CONTRACTOR SHALL:**

2                   **(I) REPORT THE CONTRACTOR'S COMPLETION OF THE**  
3 **CYBERSECURITY TRAINING TO THE STATE CHIEF INFORMATION SECURITY**  
4 **OFFICER OR THE STATE CHIEF INFORMATION SECURITY OFFICER'S DESIGNEE;**  
5 **AND**

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

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

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

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