



General Assembly

January Session, 2021

Raised Bill No. 6607

LCO No. 4480



Referred to Committee on COMMERCE

Introduced by:

(CE)

AN ACT INCENTIVIZING THE ADOPTION OF CYBERSECURITY STANDARDS FOR BUSINESSES.

Be it enacted by the Senate and House of Representatives in General Assembly convened:

1 Section 1. (NEW) (*Effective October 1, 2021*) (a) As used in this section:

2 (1) "Business" means any individual or sole proprietorship,
3 partnership, firm, corporation, trust, limited liability company, limited
4 liability partnership, joint stock company, joint venture, association or
5 other legal entity through which business for profit or not-for-profit is
6 conducted;

7 (2) "Covered entity" means a business that accesses, maintains,
8 communicates or processes personal information or restricted
9 information in or through one or more systems, networks or services
10 located in or outside this state;

11 (3) "Data breach" means unauthorized access to and acquisition of
12 computerized data that compromises the security or confidentiality of
13 personal information or restricted information owned by or licensed to

14 a covered entity and that causes, reasonably is believed to have caused
15 or reasonably is believed will cause a material risk of identity theft or
16 other fraud to a person or property. "Data breach" does not include (A)
17 good faith acquisition of personal information or restricted information
18 by the covered entity's employee or agent for the purposes of the
19 covered entity, provided the personal information or restricted
20 information is not used for an unlawful purpose or subject to further
21 unauthorized disclosure, or (B) acquisition of personal information or
22 restricted information pursuant to a search warrant, subpoena or other
23 court order, or pursuant to a subpoena, order or duty of a regulatory
24 state agency;

25 (4) "Personal information" means an individual's name, consisting of
26 the individual's first name or first initial and last name, in combination
27 with and linked to any one or more of the following data elements, when
28 the data elements are not encrypted, redacted or altered by any method
29 or technology in such a manner that the data elements are unreadable:
30 (A) Social security number; (B) driver's license number or state
31 identification number; or (C) account number or credit or debit card
32 number, in combination with and linked to any required security code,
33 access code or password that would permit access to an individual's
34 financial account; and

35 (5) "Restricted information" means any information about an
36 individual, other than personal information, that, alone or in
37 combination with other information, including personal information,
38 can be used to distinguish or trace the individual's identity or that is
39 linked or linkable to an individual, if the information is not encrypted,
40 redacted or altered by any method or technology in such a manner that
41 the information is unreadable, and the breach of which is likely to result
42 in a material risk of identity theft or other fraud to a person or property.

43 (b) In any cause of action founded in tort that is brought under the
44 laws of this state or in the courts of this state and that alleges that the
45 failure to implement reasonable cybersecurity controls resulted in a data
46 breach concerning personal information or restricted information, it

47 shall be an affirmative defense that a covered entity created, maintained
48 and complied with a written cybersecurity program that contains
49 administrative, technical and physical safeguards for the protection of
50 personal or restricted information and that reasonably conforms to an
51 industry recognized cybersecurity framework, as described in
52 subsection (c) of this section and that such covered entity designed its
53 cybersecurity program in accordance with the provisions of subsection
54 (d) of this section.

55 (c) A covered entity's cybersecurity program, as described in
56 subsection (b) of this section, reasonably conforms to an industry
57 recognized cybersecurity framework if:

58 (1) (A) The cybersecurity program reasonably conforms to the current
59 version of or any combination of the current versions of:

60 (i) The "Framework for Improving Critical Infrastructure
61 Cybersecurity" published by the National Institute of Standards and
62 Technology;

63 (ii) The National Institute of Standards and Technology's special
64 publication 800-171;

65 (iii) The National Institute of Standards and Technology's special
66 publications 800-53 and 800-53a;

67 (iv) The Federal Risk and Management Program's "FedRAMP
68 Security Assessment Framework";

69 (v) The Center for Internet Security's "Center for Internet Security
70 Critical Security Controls for Effective Cyber Defense"; or

71 (vi) The "ISO/IEC 27000-series" information security standards
72 published by the International Organization for Standardization and the
73 International Electrotechnical Commission.

74 (B) When a revision to a document listed in subparagraph (A) of this

75 section is published, a covered entity whose cybersecurity program
76 reasonably conforms to a prior version of said document, such covered
77 entity shall reasonably conform to such revision not later than one year
78 after the publication date of such revision.

79 (2) (A) The covered entity is regulated by the state or the federal
80 government or is otherwise subject to the requirements of any of the
81 laws or regulations identified in subparagraph (A)(i) to (A)(iv),
82 inclusive, of this subdivision, and such covered entity's cybersecurity
83 program reasonably conforms to the current version of:

84 (i) The security requirements of the Health Insurance Portability and
85 Accountability Act of 1996, P.L. 104-191, as amended from time to time,
86 as set forth in 45 CFR 164, Subpart C, as amended from time to time;

87 (ii) Title V of the Gramm-Leach-Bliley Act of 1999, P.L. 106-102, as
88 amended from time to time;

89 (iii) The Federal Information Security Modernization Act of 2014, P.L.
90 113-283, as amended from time to time;

91 (iv) The security requirements of the Health Information Technology
92 for Economic and Clinical Health Act, as amended from time to time, as
93 set forth in 45 CFR 162, as amended from time to time.

94 (B) If any of the laws or regulations identified in subparagraph (A)(i)
95 to (A)(iv), inclusive, of this subdivision are amended, a covered entity
96 whose cybersecurity program reasonably conforms to a prior version of
97 said laws or regulations, such covered entity shall reasonably conform
98 to such amended law or regulation not later than one year after the date
99 of such amendment.

100 (3) (A) The cybersecurity program reasonably complies with the
101 current version of the "Payment Card Industry Data Security Standard"
102 and the current version of another applicable industry recognized
103 cybersecurity framework described in subparagraph (A) of subdivision
104 (1) of this subsection.

105 (B) When a revision to the "Payment Card Industry Data Security
106 Standard" is published, a covered entity whose cybersecurity program
107 reasonably conforms to a prior version of said document, such covered
108 entity shall reasonably conform to such revision not later than one year
109 after the publication date of such revision.

110 (d) (1) A covered entity's cybersecurity program shall be designed to
111 do the following with respect to personal and restricted information: (A)
112 Protect the security and confidentiality of such information; (B) protect
113 against any anticipated threats or hazards to the security or integrity of
114 such information; and (C) protect against unauthorized access to and
115 acquisition of the information that is likely to result in a material risk of
116 identity theft or other fraud to the individual to whom the information
117 relates.

118 (2) The scale and scope of a covered entity's cybersecurity program
119 shall be based on the following factors: (A) The size and complexity of
120 the covered entity; (B) the nature and scope of the activities of the
121 covered entity; (C) the sensitivity of the information to be protected; (D)
122 the cost and availability of tools to improve information security and
123 reduce vulnerabilities; and (E) the resources available to the covered
124 entity.

This act shall take effect as follows and shall amend the following sections:		
Section 1	October 1, 2021	New section

CE

Joint Favorable C/R

JUD