



General Assembly

February Session, 2026

Raised Bill No. 403

LCO No. 2691



Referred to Committee on PUBLIC SAFETY AND SECURITY

Introduced by:
(PS)

AN ACT CONCERNING CYBERSECURITY.

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

1 Section 1. (NEW) (*Effective October 1, 2026*) As used in this section and
2 sections 2 to 11, inclusive, of this act:

3 (1) "Covered entity" means any business, health care entity or
4 government contractor operating in the state that maintains or possesses
5 sensitive data or operates critical infrastructure;

6 (2) "AAL3 identity assurance" means authentication requiring high-
7 confidence identity proofing and forensic-grade verification of identity
8 credentials that resists impersonation, replay and credential
9 compromise;

10 (3) "Non-repudiation" means a security state in which no party to a
11 transaction can deny the validity of such transaction or a corresponding
12 access log; and

13 (4) "Material security deficiency" means a systemic failure to maintain
14 cybersecurity standards that poses a foreseeable risk to public safety or

15 operational continuity.

16 Sec. 2. (NEW) (*Effective October 1, 2026*) (a) Notwithstanding any
17 provision of the general statutes, on and after July 1, 2027, any covered
18 entity that maintains a cybersecurity program in compliance with the
19 "Cybersecurity Framework 2.0" published by the National Institute of
20 Standards and Technology and AAL3 identity assurance standards shall
21 be deemed in compliance with all applicable state laws and regulations
22 that establish equivalent cybersecurity requirements.

23 (b) Not later than July 1, 2027, each critical infrastructure entity shall
24 utilize decentralized security architectures that provide non-
25 repudiation functions and eliminate centrally stored passwords or
26 biometrics.

27 Sec. 3. (NEW) (*Effective October 1, 2026*) (a) No employer shall
28 discharge, discipline or otherwise penalize or threaten an employee
29 who is a cybersecurity professional because such employee, or a person
30 acting on behalf of such employee, reports a material security deficiency
31 or a failure to maintain non-repudiation standards to a supervisor or the
32 Division of Emergency Management and Homeland Security within the
33 Department of Emergency Services and Public Protection.

34 (b) The protections provided under subsection (a) of this section shall
35 be in addition to any protections provided under section 31-51m of the
36 general statutes.

37 Sec. 4. (NEW) (*Effective October 1, 2026*) (a) Not later than seventy-two
38 hours after a covered entity discovers a cybersecurity incident resulting
39 in unauthorized access to sensitive data, disruption of public services or
40 operational continuity or material risk to such critical entity's sensitive
41 data, critical infrastructure, public services or operational continuity, the
42 covered entity shall notify the Division of Emergency Management and
43 Homeland Security within the Department of Emergency Services and
44 Public Protection.

45 (b) The notification shall include, to the extent known by the covered
46 entity: (1) A description of the nature and scope of the cybersecurity
47 incident, (2) a description of the affected systems, networks or data, (3)
48 an estimate of the duration of the cybersecurity incident, and (4) an
49 assessment of any impact on the covered entity's operations, financial
50 effects or public impact.

51 (c) The covered entity shall provide supplemental notice to the
52 division as additional information becomes available.

53 Sec. 5. (NEW) (*Effective October 1, 2026*) On and after January 1, 2027,
54 each covered entity shall implement and maintain minimum
55 cybersecurity safeguards consistent with "cybersecurity framework"
56 principles published by the National Institute of Standards and
57 Technology, including, but not necessarily limited to:

58 (1) The timely installation of critical security patches and system
59 updates;

60 (2) The encryption of sensitive data at rest and in transit;

61 (3) The implementation of backup systems capable of restoring
62 operations in the event of a ransomware incident or system
63 compromise; and

64 (4) A cybersecurity risk assessment conducted at least annually.

65 Sec. 6. (NEW) (*Effective October 1, 2026*) (a) On and after January 1,
66 2028, each critical infrastructure entity, health care provider, financial
67 institution and state agency shall adopt a quantum-transition readiness
68 posture, including, but not necessarily limited to, planning for
69 migration toward post-quantum cryptography approved by the
70 National Institute of Standards and Technology.

71 (b) On and after January 1, 2028, such entities, providers, institutions
72 and agencies shall implement cryptographic agility architectures
73 capable of rapid algorithm replacement in accordance with nationally

74 recognized standards.

75 Sec. 7. (NEW) (*Effective October 1, 2026*) There is established the
76 "Connecticut Cybersecurity Seed Fund" grant program. The Deputy
77 Commissioner of the Division of Emergency Management and
78 Homeland Security within the Department of Emergency Services and
79 Public Protection shall administer the program. Pursuant to such
80 program, the deputy commissioner shall provide grants-in-aid for the
81 establishment of decentralized and non-repudiated security solutions
82 by entities based in the state. An entity may submit an application for a
83 grant under this section in a form and manner prescribed by the deputy
84 commissioner. Not later than January 1, 2028, and annually thereafter,
85 the deputy commissioner shall submit a report on the program to the
86 joint standing committee of the General Assembly having cognizance of
87 matters relating to public safety and security in accordance with the
88 provisions of section 11-4a of the general statutes.

89 Sec. 8. (NEW) (*Effective October 1, 2026*) Not later than January 1, 2028,
90 the Division of Emergency Management and Homeland Security within
91 the Department of Emergency Services and Public Protection shall
92 establish a "bug bounty" program. Pursuant to such program, vetted
93 security researchers shall be authorized to identify cybersecurity
94 vulnerabilities in designated state-owned systems. Researchers
95 operating in good faith within the scope of the program shall be immune
96 from any liability, civil or criminal, which might otherwise be incurred
97 or imposed.

98 Sec. 9. (NEW) (*Effective October 1, 2026*) The Connecticut Intelligence
99 Center within the Division of Emergency Management and Homeland
100 Security within the Department of Emergency Services and Public
101 Protection shall collect and disseminate cybersecurity intelligence on
102 behalf of the state.

103 Sec. 10. (NEW) (*Effective October 1, 2026*) (a) There is established a
104 State Cybersecurity Intelligence Task Force to analyze cybersecurity

105 intelligence matters, coordinate actions relating to cybersecurity and
106 identify systemic cybersecurity risks.

107 (b) The task force shall consist of the following members:

108 (1) The Commissioner of Emergency Services and Public Protection,
109 or the commissioner's designee;

110 (2) The Commissioner of Administrative Services, or the
111 commissioner's designee;

112 (3) The Adjutant General of the Military Department, or the Adjutant
113 General's designee; and

114 (4) The Deputy Commissioner of the Division of Emergency
115 Management and Homeland Security within the Department of
116 Emergency Services and Public Protection, or the deputy
117 commissioner's designee.

118 (c) The Commissioner of Emergency Services and Public Protection
119 shall select the chairpersons of the task force from among the members
120 of the task force. Such chairpersons shall schedule the first meeting of
121 the task force, which shall be held not later than December 1, 2026.

122 (d) The task force shall meet not less than quarterly and shall report
123 its findings and recommendations to the joint standing committee of the
124 General Assembly having cognizance of matters relating to public safety
125 and security in accordance with the provisions of section 11-4a of the
126 general statutes as the task force deems appropriate.

127 Sec. 11. (NEW) (*Effective October 1, 2026*) (a) The Division of
128 Emergency Management and Homeland Security within the
129 Department of Emergency Services and Public Protection shall
130 coordinate the state's operational response to cybersecurity
131 emergencies.

132 (b) The Deputy Commissioner of the Division of Emergency

133 Management and Homeland Security within the Department of
134 Emergency Services and Public Protection, or the deputy
135 commissioner's designee, shall serve as the primary liaison between the
136 State Cybersecurity Intelligence Task Force established pursuant to
137 section 10 of this act and local emergency management directors.

This act shall take effect as follows and shall amend the following sections:		
Section 1	<i>October 1, 2026</i>	New section
Sec. 2	<i>October 1, 2026</i>	New section
Sec. 3	<i>October 1, 2026</i>	New section
Sec. 4	<i>October 1, 2026</i>	New section
Sec. 5	<i>October 1, 2026</i>	New section
Sec. 6	<i>October 1, 2026</i>	New section
Sec. 7	<i>October 1, 2026</i>	New section
Sec. 8	<i>October 1, 2026</i>	New section
Sec. 9	<i>October 1, 2026</i>	New section
Sec. 10	<i>October 1, 2026</i>	New section
Sec. 11	<i>October 1, 2026</i>	New section

Statement of Purpose:

To establish various cybersecurity provisions relating to (1) a cybersecurity framework, (2) a prohibition on penalizing cybersecurity employees for certain reports, (3) notifications regarding cybersecurity incidents, (4) minimum safeguards, (5) quantum-transition readiness requirements, (6) the "Connecticut Cybersecurity Seed Fund" grant program, (7) a "bug bounty" program, (8) the dissemination of cybersecurity intelligence, (9) the State Cybersecurity Intelligence Task Force, and (10) the state's operational response to cybersecurity emergencies.

[Proposed deletions are enclosed in brackets. Proposed additions are indicated by underline, except that when the entire text of a bill or resolution or a section of a bill or resolution is new, it is not underlined.]