

SENATE, No. 4036

STATE OF NEW JERSEY
219th LEGISLATURE

INTRODUCED NOVEMBER 4, 2021

Sponsored by:

Senator LINDA R. GREENSTEIN

District 14 (Mercer and Middlesex)

SYNOPSIS

Requires businesses in financial, essential infrastructure, and health care industries to report cybersecurity incidents.

CURRENT VERSION OF TEXT

As introduced.



1 AN ACT requiring certain businesses to report cybersecurity
2 incidents and supplementing P.L.1960, c.39 (C.56:8-1 et seq.).
3

4 **BE IT ENACTED** *by the Senate and General Assembly of the State*
5 *of New Jersey:*
6

7 1. As used in this act:

8 “Cybersecurity incident” means an event occurring on or
9 conducted through a computer network that jeopardizes the
10 integrity, confidentiality, or availability of, or information residing
11 on, computers, information systems, communications systems
12 networks, physical or virtual infrastructure controlled by computers,
13 or information systems.

14 “Industrial control system” means an information system used to
15 control industrial processes such as manufacturing, product
16 handling, production, or distribution. “Industrial control system”
17 includes supervisory control and data acquisition systems used to
18 control geographically dispersed assets, and distributed control
19 systems and smaller control systems using programmable logic
20 controllers to control localized processes.

21 “Information resource” means information and related resources,
22 such as personnel, equipment, funds, and information technology.

23 “Information system” means a discrete set of information
24 resources organized for the collection, processing, maintenance,
25 use, sharing, dissemination, or disposition of information.

26 “New Jersey Cybersecurity and Communications Integration
27 Cell” means the New Jersey Cybersecurity and Communications
28 Integration Cell established pursuant to Executive Order No. 178 of
29 2015 in the New Jersey Office of Homeland Security and
30 Preparedness, or any successor entity.

31 “Sensitive business” means a sole proprietorship, partnership,
32 corporation, association, or other entity, however organized and
33 whether or not organized to operate at a profit, including a financial
34 institution organized, chartered, or holding a license or
35 authorization certificate under the laws of this State, any other state,
36 the United States, or of any other country, or the parent or the
37 subsidiary of a financial institution, that is engaged in the financial,
38 essential infrastructure, or healthcare industries and does business
39 in this State.
40

41 2. a. A sensitive business shall report to the New Jersey
42 Cybersecurity and Communications Integration Cell, promptly after
43 an employee is made aware of a cybersecurity incident, and in
44 accordance with all applicable laws, rules, and regulations:

45 (1) any cybersecurity incident that results in the compromise of
46 the confidentiality, integrity, availability, or privacy of the sensitive
47 business’ billing, communications, data management, or business
48 information systems, or the information thereon; and

1 (2) any cybersecurity incident against the sensitive business'
2 industrial control system, if applicable, including monitoring,
3 operations, and centralized control systems, that adversely impact,
4 disable, or manipulate infrastructure, resulting in loss of service or
5 damage to infrastructure.

6 b. No later than 30 days after receiving a report of a
7 cybersecurity incident from a sensitive business pursuant to
8 subsection a. of this section, the New Jersey Cybersecurity and
9 Communications Integration Cell shall cause to be audited the
10 sensitive business' cybersecurity program and any actions the
11 sensitive business took in response to the cybersecurity incident.
12 The audit shall identify cyber threats and vulnerabilities to the
13 sensitive business, weaknesses in the sensitive business'
14 cybersecurity program, and strategies to address those weaknesses
15 so as to protect the sensitive business from the threat of future
16 cybersecurity incidents. The audit shall be conducted by a qualified
17 and independent cybersecurity company, at the sensitive business'
18 expense. Following the audit, the sensitive business shall submit
19 the audit and any corrective action plans derived from the audit to
20 the New Jersey Cybersecurity and Communications Integration
21 Cell.

22
23 3. This act shall take effect on the 90th day after the date of
24 enactment.

25 26 27 STATEMENT

28
29 This bill would require sensitive businesses to report certain
30 cybersecurity incidents promptly to the New Jersey Cybersecurity
31 and Communications Integration Cell (NJCCIC). For the purposes
32 of this bill, a "cybersecurity incident" means an event occurring on
33 or conducted through a computer network that jeopardizes the
34 integrity, confidentiality, or availability of, or information residing
35 on, computers, information systems, communications systems
36 networks, physical or virtual infrastructure controlled by computers,
37 or information systems. The bill would direct the NJCCIC to audit
38 the relevant business no later than 30 days after being made aware
39 of an incident. Cybersecurity audits would be conducted by a
40 qualified and independent cybersecurity company at the sensitive
41 business' expense.