

SENATE, No. 4278

STATE OF NEW JERSEY
219th LEGISLATURE

INTRODUCED DECEMBER 13, 2021

Sponsored by:

Senator LINDA R. GREENSTEIN

District 14 (Mercer and Middlesex)

SYNOPSIS

Requires public agencies report cybersecurity incidents to New Jersey Office of Homeland Security and Preparedness.

CURRENT VERSION OF TEXT

As introduced.



1 **AN ACT** requiring public agencies to report cybersecurity incidents
2 to the New Jersey Office of Homeland Security and Preparedness
3 and supplementing Title 52 of the New Jersey Statutes.

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

7
8 1. As used in this act, P.L. , c. (C.)(pending before
9 the Legislature as this bill):

10 a. “Public agency” means any public agency of the State or any
11 political subdivision thereof.

12 b. “Government contractor” means an individual or entity that
13 performs work for or on behalf of a public sector institution on a
14 contract basis with access to or hosting of the public agency’s
15 network, systems, applications, or information.

16 c. “Cybersecurity incident” means a malicious or suspicious
17 event occurring on or conducted through a computer network that
18 jeopardizes the integrity, confidentiality, or availability of an
19 information system or the information the system processes, stores,
20 or transmits.

21 d. “Cyber threat indicator” means information that is necessary
22 to describe or identify:

23 (1) malicious reconnaissance, including, but not limited to,
24 anomalous patterns of communication that appear to be transmitted
25 for the purpose of gathering technical information related to a
26 cybersecurity threat or vulnerability;

27 (2) a method of defeating a security control or exploitation of a
28 security vulnerability;

29 (3) a security vulnerability, including, but not limited to,
30 anomalous activity that appears to indicate the existence of a
31 security vulnerability;

32 (4) a method of causing a user with legitimate access to an
33 information system or information that is stored on, processed by,
34 or transiting an information system to unwittingly enable the defeat
35 of a security control or exploitation of a security vulnerability;

36 (5) malicious cyber command and control;

37 (6) the actual or potential harm caused by an incident, including
38 but not limited to, a description of the data exfiltrated as a result of
39 a particular cyber threat; and

40 (7) any other attribute of a cyber threat, if disclosure of such
41 attribute is not otherwise prohibited by law.

42 e. “Defensive measure” means an action, device, procedure,
43 signature, technique, or other measure applied to an information
44 system or information that is stored on, processed by, or transiting
45 an information system that detects, prevents, or mitigates a known
46 or suspected cyber threat or security vulnerability, but does not
47 include a measure that destroys, renders unusable, provides
48 unauthorized access to, or substantially harms an information

1 system or information stored on, processed by, or transiting such
2 information system not owned by the entity operating the measure,
3 or another entity that is authorized to provide consent and has
4 provided consent to that private entity for operation of such
5 measure.

6 f. “Information resource” means information and related
7 resources, such as personnel, equipment, funds, and information
8 technology.

9 g. “Information system” means a discrete set of information
10 resources organized for the collection, processing, maintenance,
11 use, sharing, dissemination, or disposition of information.

12 h. “Information technology” means any equipment or
13 interconnected system or subsystem of equipment that is used in
14 automatic acquisition, storage, manipulation, management,
15 movement, control, display, switching, interchange, transmission,
16 or reception of data or information used by a public sector
17 institution or a government contractor under contract with a public
18 sector institution which requires the use of such equipment or
19 requires the use, to a significant extent, of such equipment in the
20 performance of a service or the furnishing of a product.

21 The term information technology includes, but is not limited to,
22 computers, ancillary equipment, software, firmware, and similar
23 procedures, services, including support services, and related
24 resources.

25 i. “Private entity” means any individual, corporation,
26 company, partnership, firm, association, or other entity, but does
27 not include a public agency as defined in this act, or a foreign
28 government, or any component thereof.

29

30 2. a. The New Jersey Office of Homeland Security and
31 Preparedness shall receive and maintain cybersecurity incident
32 notifications from public agencies and government contractors in
33 accordance with this act.

34 b. No later than 90 days after the effective date of this act, the
35 Director of the New Jersey Office of Homeland Security and
36 Preparedness shall establish cyber incident reporting capabilities to
37 facilitate submission of timely, secure, and confidential
38 cybersecurity incident notifications from public agencies and
39 government contractors to the office.

40 c. No later than 90 days after the effective date of this act, the
41 New Jersey Office of Homeland Security and Preparedness shall
42 prominently post instructions for submitting cybersecurity incident
43 notifications on its website. The instructions shall include, at a
44 minimum, the types of cybersecurity incidents to be reported and
45 any other information to be included in the notifications made
46 through the established cyber incident reporting system.

1 d. The cyber incident reporting system shall include the ability
2 for the New Jersey Office of Homeland Security and Preparedness
3 to:

4 (1) securely accept a cybersecurity incident notification from
5 any individual or private entity, regardless of whether the entity is a
6 public agency or government contractor;

7 (2) track and identify trends in cybersecurity incidents reported
8 through the cyber incident reporting system; and

9 (3) produce reports on the types of incidents, indicators,
10 defensive measures, and entities reported through the cyber incident
11 reporting system.

12 e. Any cybersecurity incident notification submitted to the
13 New Jersey Office of Homeland Security and Preparedness as
14 required under P.L. ,c. (C.)(pending before the
15 Legislature as this bill) shall be deemed confidential, non-public,
16 and not subject to the provisions of P.L.1963, c.73 (C.47:1A-1 et
17 seq.), commonly known as the open public records act, as amended
18 and supplemented, may not be discoverable in any civil or criminal
19 action, and may not be subject to subpoena, unless the subpoena is
20 issued by the New Jersey State Legislature and is deemed necessary
21 for the purposes of legislative oversight.

22 f. Notwithstanding the provisions of section e. of this act, the
23 New Jersey Office of Homeland Security and Preparedness may
24 anonymize and share cyber threat indicators and relevant defensive
25 measures to help prevent additional or future attacks and share
26 cybersecurity incident notifications with relevant law enforcement
27 authorities.

28 g. Information submitted to the New Jersey Office of
29 Homeland Security and Preparedness through the cyber incident
30 reporting system shall be subject to privacy and protection
31 procedures developed and implemented by the office, which shall
32 be based on the comparable privacy protection procedures
33 developed for information received and shared pursuant to the
34 federal Cyber Security Information Sharing Act of 2015 (6 U.S.C.
35 s.1501 et seq.).

36

37 3. Not later than one year after the date on which the cyber
38 incident reporting system is established and at least once each year
39 thereafter, the Director of the New Jersey Office of Homeland
40 Security and Preparedness shall submit an annual report on its
41 activities to the Governor, and to the Legislature, pursuant to
42 P.L.1991, c.164 (C.52:14-19.1). The report shall include, at a
43 minimum:

44 a. information on the number of notifications received and a
45 description of the incident types and associated mitigating measures
46 taken during the one-year period preceding the publication of the
47 report;

