

P.L. 2023, CHAPTER 19, *approved March 13, 2023*
Senate, No. 297 (*First Reprint*)

1 AN ACT requiring public agencies ¹and government contractors¹ to
2 report cybersecurity incidents to the New Jersey Office of
3 Homeland Security and Preparedness and supplementing Title 52
4 of the New Jersey Statutes.

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

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

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

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

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

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

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

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

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

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

37 (5) malicious cyber command and control;

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

EXPLANATION – Matter enclosed in bold-faced brackets **[thus]** in the above bill is
not enacted and is intended to be omitted in the law.

Matter underlined thus is new matter.

Matter enclosed in superscript numerals has been adopted as follows:

¹Senate SLP committee amendments adopted March 21, 2022.

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

3 e. “Defensive measure” means an action, device, procedure,
4 signature, technique, or other measure applied to an information
5 system or information that is stored on, processed by, or transiting
6 an information system that detects, prevents, or mitigates a known
7 or suspected cyber threat or security vulnerability, but does not
8 include a measure that destroys, renders unusable, provides
9 unauthorized access to, or substantially harms an information
10 system or information stored on, processed by, or transiting such
11 information system not owned by the entity operating the measure,
12 or another entity that is authorized to provide consent and has
13 provided consent to that private entity for operation of such
14 measure.

15 f. “Information resource” means information and related
16 resources, such as personnel, equipment, funds, and information
17 technology.

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

21 h. “Information technology” means any equipment or
22 interconnected system or subsystem of equipment that is used in
23 automatic acquisition, storage, manipulation, management,
24 movement, control, display, switching, interchange, transmission,
25 or reception of data or information used by a public sector
26 institution or a government contractor under contract with a public
27 sector institution which requires the use of such equipment or
28 requires the use, to a significant extent, of such equipment in the
29 performance of a service or the furnishing of a product.

30 The term information technology includes, but is not limited to,
31 computers, ancillary equipment, software, firmware, and similar
32 procedures, services, including support services, and related
33 resources.

34 i. “Private entity” means any individual, corporation,
35 company, partnership, firm, association, or other entity, but does
36 not include a public agency as defined in this act, or a foreign
37 government, or any component thereof. **1**¹

38
39 ¹1. As used in this act, P.L. _____, c. _____ (C. _____)(pending before
40 the Legislature as this bill):

41 “Cybersecurity incident” means a malicious or suspicious event
42 occurring on or conducted through a computer network that
43 jeopardizes the integrity, confidentiality, or availability of an
44 information system or the information the system processes, stores,
45 or transmits.

46 “Cyber threat indicator” means information that is necessary to
47 describe or identify:

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

5 (2) a method of defeating a security control or exploitation of a
6 security vulnerability;

7 (3) a security vulnerability, including, but not limited to,
8 anomalous activity that appears to indicate the existence of a
9 security vulnerability;

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

14 (5) malicious cyber command and control;

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

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

20 “Defensive measure” means an action, device, procedure,
21 signature, technique, or other measure applied to an information
22 system or information that is stored on, processed by, or transiting
23 an information system that detects, prevents, or mitigates a known
24 or suspected cyber threat or security vulnerability, but does not
25 include a measure that destroys, renders unusable, provides
26 unauthorized access to, or substantially harms an information
27 system or information stored on, processed by, or transiting such
28 information system not owned by the entity operating the measure,
29 or another entity that is authorized to provide consent and has
30 provided consent to that private entity for operation of such
31 measure.

32 “Government contractor” means an individual or entity that
33 performs work for or on behalf of a public agency on a contract
34 basis with access to or hosting of the public agency’s network,
35 systems, applications, or information.

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

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

41 “Information technology” means any equipment or
42 interconnected system or subsystem of equipment that is used in
43 automatic acquisition, storage, manipulation, management,
44 movement, control, display, switching, interchange, transmission,
45 or reception of data or information used by a public agency or a
46 government contractor under contract with a public agency which
47 requires the use of such equipment or requires the use, to a

1 significant extent, of such equipment in the performance of a
2 service or the furnishing of a product.

3 The term information technology includes, but is not limited to,
4 computers, ancillary equipment, software, firmware, and similar
5 procedures, services, including support services, and related
6 resources.

7 “Private entity” means any individual, corporation, company,
8 partnership, firm, association, or other entity, but does not include a
9 public agency as defined in this act, or a foreign government, or any
10 component thereof.

11 “Public agency” means any public agency of the State or any
12 political subdivision thereof.¹

13
14 2. a. ¹Every public agency and government contractor shall
15 report cybersecurity incidents to the New Jersey Office of
16 Homeland Security and Preparedness. The report shall be made
17 within 72 hours of when the public agency or government
18 contractor reasonably believes that a cybersecurity incident has
19 occurred.

20 b.¹ The New Jersey Office of Homeland Security and
21 Preparedness shall receive and maintain cybersecurity incident
22 notifications from public agencies ¹[and] ¹ government
23 contractors ¹, and private entities¹ in accordance with this act.

24 ¹[b.] c.¹ No later than 90 days after the effective date of this
25 act, the Director of the New Jersey Office of Homeland Security
26 and Preparedness shall establish cyber incident reporting
27 capabilities to facilitate submission of timely, secure, and
28 confidential cybersecurity incident notifications from public
29 agencies ¹[and] ¹ government contractors ¹, and private entities¹ to
30 the office.

31 ¹[c.] d.¹ No later than 90 days after the effective date of this
32 act, the New Jersey Office of Homeland Security and Preparedness
33 shall prominently post instructions for submitting cybersecurity
34 incident notifications on its website. The instructions shall include,
35 at a minimum, the types of cybersecurity incidents to be reported
36 and any other information to be included in the notifications made
37 through the established cyber incident reporting system.

38 ¹[d.] e.¹ The cyber incident reporting system shall ¹[include
39 the ability for] permit¹ the New Jersey Office of Homeland
40 Security and Preparedness to:

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

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

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

4 ¹**[e.] f.**¹ Any cybersecurity incident notification submitted to
5 the New Jersey Office of Homeland Security and Preparedness ¹**[as**
6 **required under]** pursuant to¹ P.L. ,c. (C.)(pending
7 before the Legislature as this bill) shall be deemed confidential,
8 non-public, and not subject to the provisions of P.L.1963, c.73
9 (C.47:1A-1 et seq.), commonly known as the open public records
10 act, as amended and supplemented, may not be discoverable in any
11 civil or criminal action, and may not be subject to subpoena, unless
12 the subpoena is issued by the New Jersey State Legislature and is
13 deemed necessary for the purposes of legislative oversight.

14 ¹**[f.] g.**¹ Notwithstanding the provisions of ¹**[section e.]**
15 **subsection f.**¹ of this ¹**[act] section**¹, the New Jersey Office of
16 Homeland Security and Preparedness may anonymize and share
17 cyber threat indicators and relevant defensive measures to help
18 prevent additional or future attacks and share cybersecurity incident
19 notifications with relevant law enforcement authorities.

20 ¹**[g.] h.**¹ Information submitted to the New Jersey Office of
21 Homeland Security and Preparedness through the cyber incident
22 reporting system shall be subject to privacy and protection
23 procedures developed and implemented by the office, which shall
24 be based on the comparable privacy protection procedures
25 developed for information received and shared pursuant to the
26 federal Cyber Security Information Sharing Act of 2015 (6 U.S.C.
27 s.1501 et seq.).
28

29 3. Not later than one year after the date on which the cyber
30 incident reporting system is established and at least once each year
31 thereafter, the Director of the New Jersey Office of Homeland
32 Security and Preparedness shall submit an annual report on its
33 activities to the Governor, and to the Legislature, pursuant to
34 ¹**section 2 of**¹ P.L.1991, c.164 (C.52:14-19.1). The report shall
35 include, at a minimum:

36 a. information on the number of notifications received and a
37 description of the ¹**cybersecurity**¹ incident types and associated
38 mitigating measures taken during the one-year period preceding the
39 publication of the report;

40 b. the categories of public agencies and government contractors
41 that submitted cybersecurity notifications; and

42 c. ¹**[the types of cybersecurity incidents and]** ¹**any**¹ other
43 information required in the submission of a cybersecurity incident
44 notification, noting any changes from the report published in the
45 previous year.
46

47 4. This act shall take effect immediately.

S297 [1R]

6

1

2

3

Requires public agencies and government contractors to report

4

cybersecurity incidents to New Jersey Office of Homeland Security

5

and Preparedness.