[First Reprint]

SENATE, No. 297

STATE OF NEW JERSEY

220th LEGISLATURE

PRE-FILED FOR INTRODUCTION IN THE 2022 SESSION

Sponsored by:
Senator LINDA R. GREENSTEIN
District 14 (Mercer and Middlesex)
Senator FRED H. MADDEN, JR.
District 4 (Camden and Gloucester)
Assemblywoman CAROL A. MURPHY
District 7 (Burlington)
Assemblyman DANIEL R. BENSON
District 14 (Mercer and Middlesex)
Assemblyman CLINTON CALABRESE
District 36 (Bergen and Passaic)

Co-Sponsored by:
Senators O'Scanlon, Turner, Pou, Assemblywoman Quijano, Assemblyman Tully and Assemblywoman Mosquera

SYNOPSIS

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

CURRENT VERSION OF TEXT

As reported by the Senate Law and Public Safety Committee on March 21, 2022, with amendments.

(Sponsorship Updated As Of: 1/26/2023)

AN ACT requiring public agencies [1]and government contractors[1] to report cybersecurity incidents to the New Jersey Office of Homeland Security and Preparedness and supplementing Title 52 of the New Jersey Statutes.

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

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

a. "Public agency" means any public agency of the State or any political subdivision thereof.

b. "Government contractor" means an individual or entity that performs work for or on behalf of a public sector institution on a contract basis with access to or hosting of the public agency's network, systems, applications, or information.

c. "Cybersecurity incident" means a malicious or suspicious event occurring on or conducted through a computer network that jeopardizes the integrity, confidentiality, or availability of an information system or the information the system processes, stores, or transmits.

d. "Cyber threat indicator" means information that is necessary to describe or identify:

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

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

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

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

(5) malicious cyber command and control;

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

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

e. "Defensive measure" means an action, device, procedure, signature, technique, or other measure applied to an information

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:
[1]Senate SLP committee amendments adopted March 21, 2022.

system or information that is stored on, processed by, or transiting an information system that detects, prevents, or mitigates a known or suspected cyber threat or security vulnerability, but does not include a measure that destroys, renders unusable, provides unauthorized access to, or substantially harms an information system or information stored on, processed by, or transiting such information system not owned by the entity operating the measure, or another entity that is authorized to provide consent and has provided consent to that private entity for operation of such measure.

f. "Information resource" means information and related resources, such as personnel, equipment, funds, and information technology.

g. "Information system" means a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.

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

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

i. "Private entity" means any individual, corporation, company, partnership, firm, association, or other entity, but does not include a public agency as defined in this act, or a foreign government, or any component thereof.**]**[1]

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

"Cybersecurity incident" means a malicious or suspicious event occurring on or conducted through a computer network that jeopardizes the integrity, confidentiality, or availability of an information system or the information the system processes, stores, or transmits.

"Cyber threat indicator" means information that is necessary to describe or identify:

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

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

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

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

(5) malicious cyber command and control;

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

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

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

"Government contractor" means an individual or entity that performs work for or on behalf of a public agency on a contract basis with access to or hosting of the public agency's network, systems, applications, or information.

"Information resource" means information and related resources, such as personnel, equipment, funds, and information technology.

"Information system" means a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.

"Information technology" means any equipment or interconnected system or subsystem of equipment that is used in automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information used by a public agency or a government contractor under contract with a public agency which requires the use of such equipment or requires the use, to a significant extent, of such equipment in the performance of a service or the furnishing of a product.

The term information technology includes, but is not limited to, computers, ancillary equipment, software, firmware, and similar

procedures, services, including support services, and related resources.

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

"Public agency" means any public agency of the State or any political subdivision thereof.[1]

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

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

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

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

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

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

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

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

[1][e.] f.[1] Any cybersecurity incident notification submitted to the New Jersey Office of Homeland Security and Preparedness [1][as required under] pursuant to[1] P.L. ,c. (C.)(pending

before the Legislature as this bill) shall be deemed confidential, non-public, and not subject to the provisions of P.L.1963, c.73 (C.47:1A-1 et seq.), commonly known as the open public records act, as amended and supplemented, may not be discoverable in any civil or criminal action, and may not be subject to subpoena, unless the subpoena is issued by the New Jersey State Legislature and is deemed necessary for the purposes of legislative oversight.

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

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

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

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

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

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

4. This act shall take effect immediately.