SENATE COMMITTEE SUBSTITUTE FOR

SENATE, No. 808

STATE OF NEW JERSEY

217th LEGISLATURE

ADOPTED DECEMBER 12, 2016

Sponsored by:
Senator LORETTA WEINBERG
District 37 (Bergen)
Senator BRIAN P. STACK
District 33 (Hudson)

Co-Sponsored by:
Senator Gordon

SYNOPSIS

Establishes framework for cybersecurity information sharing and preparedness; creates NJ Cybersecurity Advisory Board.

CURRENT VERSION OF TEXT

Substitute as adopted by the Senate State Government, Wagering, Tourism and Historic Preservation Committee.

(Sponsorship Updated As Of: 12/20/2016)

AN ACT concerning cybersecurity information sharing and preparedness and supplementing Title 52 of the Revised Statutes.

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

1. This act shall be known and may be cited as the "New Jersey Cyber Threat Information Sharing Act."

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

"Board" means the New Jersey Cybersecurity Advisory Board, established pursuant to sections 13 through 16 of this act.

"Cyber threat" means any action that may result in unauthorized access in order to damage or impair the security, availability, confidentiality, or integrity of an information system or unauthorized exfiltration, deletion, or manipulation of information that is stored on, processed by, or transiting an information system. The term shall not include any action exceeding authorized access to an information system that involves solely a violation of a consumer term of service or a consumer licensing agreement.

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

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

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

(3) 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 unintentionally enable the defeat of a security, operational, or technical control or exploitation of a security vulnerability;

(4) malicious cyber command and control;

(5) the actual or potential harm caused by an incident, including, but not limited to, a description of the information appropriated as a result of a particular cyber threat;

(6) any other attribute of a cyber threat, if disclosure of such attribute is not otherwise prohibited by law; or

(7) any combination of items enumerated in paragraphs (1) through (6).

"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. The term shall not include a measure that destroys, renders unusable, or

substantially harms an information system or data on an information system not belonging to the entity operating the measure or to an entity authorized to provide consent and which has provided consent to the entity operating the measure.

"Director" means the Director of the New Jersey Office of Homeland Security and Preparedness.

"Governmental entity" means any agency, department, board, bureau, commission, division, office, council, instrumentality or other entity of, within, or created by federal or State government; the Legislature of this State and any agency, department, board, bureau, commission, division, office, council, instrumentality or other entity thereof, therein, or created thereby; any independent public agency, public authority or public benefit corporation; any county, municipality, or local authority; and any other public agency, public entity, or political subdivision in this State.

"Information system" means a discrete set of information resources that collects, processes, maintains, uses, shares, disseminates, or disposes of information, communications, or both.

"Malicious cyber command and control" means a method for the remote identification of, access to, or use of an information system or information that is stored on, processed by, or transiting an information system, that is known or reasonably suspected of being associated with a known or suspected cyber threat.

"Malicious reconnaissance" means a method for probing or monitoring an information system for the purpose of discerning technical vulnerabilities of the information system, if such method is known or reasonably suspected of being associated with a known or suspected cyber threat.

"Member" means any public or private entity, other than a partner, that has been approved by the director to receive from, and provide to, the NJCCIC information about cyber threats, cyber threat indicators and defensive measures.

"Mitigation 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, blocks, or nullifies a known or suspected cyber threat or security vulnerability.

"New Jersey Cybersecurity and Communications Integration Cell" (NJCCIC) means the Information Sharing and Analysis Organization established pursuant to Executive Order No. 178 (2015).

"Operational control" means a security control for an information system that is implemented and executed primarily in a non-automated fashion.

"Partner" means any of the public or private entities approved by the director to serve as constituent components of the NJCCIC.

"Personal information" means any information about an individual maintained by the NJCCIC or a member or partner of the

NJCCIC, including, but not limited to, an individual's first name or first initial and last name linked with any one or more of the following data elements: (1) Social Security number; (2) driver's license number or State identification card number; or (3) account number or credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account. Dissociated data that, if linked, would constitute personal information shall be considered personal information if the means to link the dissociated data were accessed in connection with access to the dissociated data.

"Private entity" means any individual, corporation, company, partnership, firm, association, or other entity, but shall not include a governmental entity, foreign government, or any component thereof.

"Technical control" means a technological restriction on, audit of, access to, or use of an information system or information that is stored on, processed by, or transiting an information system that is intended to ensure the confidentiality, integrity, or availability of that information system or the information stored on, processed by or transiting by that information system.

"Technical vulnerability" means any attribute of hardware, firmware, or software that could enable or facilitate the defeat of technical control.

3. a. The Attorney General and the Director of the New Jersey Office of Homeland Security and Preparedness shall jointly develop and promulgate procedures that:

(1) designate the NJCCIC as the central State-civilian interface to receive and distribute information about cyber threats, cyber threat indicators, and defensive measures consistent and in accordance with the purpose of P.L. , c. (C.) (pending before the Legislature as this bill) and Executive Order No. 178 (2015);

(2) govern the receipt, retention, use, and disclosure of cyber threat indicators and defensive measures by the NJCCIC obtained in connection with activities pursuant to P.L. , c. (C.) (pending before the Legislature as this bill) that reasonably limit the acquisition, interception, retention, use, and disclosure of cyber threat indicators that are reasonably likely to identify specific persons, consistent with the need to carry out the responsibilities of P.L. , c. (C.) (pending before the Legislature as this bill), which shall include but not be limited to:

(a) establishing a process for the timely destruction of information that is known not to be directly related to a purpose or use authorized under P.L. , c. (C.) (pending before the Legislature as this bill); and

(b) establishing a process to anonymize and safeguard information received and disclosed, that can be used to identify specific persons unrelated to a cyber threat or defensive measure;

(3) ensure that cyber threats, cyber threat indicators, and defensive measures received and disclosed by the NJCCIC are shared with governmental and private entities in as close to real time as practicable, consistent, and in accordance with, the purposes of P.L. , c. (C.) (pending before the Legislature as this bill);

(4) provide notification to entities that have received a cyber threat, cyber threat indicator, or defensive measure from the NJCCIC that is known or determined to be in error or in contravention to the requirements of P.L. , c. (C.) (pending before the Legislature as this bill) or another provision of State or federal law;

(5) require that the NJCCIC implement and utilize appropriate security controls to protect against unauthorized access to, or acquisition of, cyber threat indicators shared with the NJCCIC;

(6) incorporate appropriate criteria or classification designations to govern the sharing of cyber threat indicators, such as whether information is classified or unclassified, controlled or uncontrolled, and any other appropriate criteria or classification designations related to the sensitivity of the information relevant to the imposition of restrictions on dissemination and handling in order to protect the confidentiality and integrity of sources and methods; and

(7) set forth the process, including establishing relevant qualifications and criteria, for evaluating and validating entities to be partners and members of the NJCCIC, and for confirming and periodically re-validating the qualification of such entities.

b. The procedures established under this section shall preserve, to the greatest extent practicable, the confidentiality of disclosed proprietary information and require recipients of such information to be informed that the cyber threat indicators or defensive measures disclosed may only be used for the purposes authorized pursuant to P.L. , c. (C.) (pending before the Legislature as this bill).

c. In developing the procedures required under this section, the Attorney General and the director shall consult with such NJCCIC partners and members, as may be appropriate, to promote the effective implementation of protocols that will facilitate the sharing, in a timely manner, of information about cyber threats, cyber threat indicators, and defensive measures.

4. a. Notwithstanding any other provision of law to the contrary, a private entity may disclose to the NJCCIC lawfully obtained cyber threats, cyber threat indicators, or defensive measures, consistent with P.L. , c. (C.) (pending before the Legislature as this bill) and the procedures established thereunder. The provision of information to the NJCCIC in accordance with this

subsection shall not be deemed to satisfy any mandatory information disclosure obligations or requirements established under the law, including but not limited to the breach of security disclosure requirements established under section 12 of P.L.2005, c.226 (C.56:8-163).

b. Notwithstanding any other provision of law to the contrary, a private entity may receive from the NJCCIC a cyber threat indicator or defensive measure disclosed under this section. The sharing of a cyber threat indicator or defensive measure with a private entity pursuant to this subsection shall not create a right or benefit to similar information by such entity or any other entity.

c. A private entity disclosing or receiving cyber threat indicators or defensive measures pursuant to this section:

(1) may use, retain, or further disclose such cyber threat indicators or defensive measures solely for the purpose of protecting an information system or information that is stored on, processed by, or transiting an information system from cyber threats or identifying or mitigating such threats, or for reporting a crime;

(2) shall take reasonable efforts to remove information that can be used to identify specific persons and that is reasonably believed to be unrelated to a cyber threat, and to safeguard information that can be used to identify specific persons from unintended disclosure and unauthorized access or acquisition; and

(3) shall comply with reasonable restrictions that a private entity places on the subsequent disclosure or retention of cyber threat indicators that are disclosed through NJCCIC.

5. a. Prior to sharing a cyber threat indicator with the NJCCIC pursuant to the procedures established in accordance with section 3 of P.L. , c. (C.) (pending before the Legislature as this bill), the entity providing the information shall:

(1) review the cyber threat indicator to assess whether it contains any information that the entity knows or reasonably should know at the time of sharing to be personal information of, or identifying, a specific individual not directly related to a cyber threat, and remove such information; or

(2) implement or utilize a technical capability configured to remove any personal information of, or identifying, a specific individual not directly related to a cyber threat.

b. Prior to sharing a cyber threat indicator with an NJCCIC member or partner pursuant to the procedures established in accordance with section 3 of P.L. , c. (C.) (pending before the Legislature as this bill), the NJCCIC shall:

(1) review the cyber threat indicator to assess whether it contains any information that the NJCCIC knows or reasonably should know at the time of sharing to be personal information of, or identifying, a specific individual not directly related to a cyber threat, and remove such information; or

(2) implement or utilize a technical capability configured to remove any personal information of, or identifying, a specific individual not directly related to a cyber threat.

6. a. Any individual or entity acting in good faith that voluntarily provides or shares cyber threats, cyber threat indicators, or defensive measures to the NJCCIC in accordance with P.L. , c. (C.) (pending before the Legislature as this bill) and the procedures established thereunder, which the individual or entity is not otherwise required to disclose, shall have immunity from any liability, civil or criminal, that might otherwise be incurred or imposed as a result of such act.

b. Any individual or entity that voluntarily monitors an information system and information in accordance with P.L. , c. (C.) (pending before the Legislature as this bill) and the procedures established thereunder, provided the individual or entity is not otherwise required to monitor an information system and information, shall have immunity from any liability, civil or criminal, that might otherwise be incurred or imposed as a result of such act.

c. Nothing in this section shall be construed to provide immunity to an individual or entity that has engaged in gross negligence or willful misconduct in the course of conducting activities in accordance with P.L. , c. (C.) (pending before the Legislature as this bill).

7. a. Subject to the provisions of any other applicable law, a cyber threat indicator or defensive measure shared with the NJCCIC in accordance P.L. , c. (C.) (pending before the Legislature as this bill) and the procedures established thereunder may be disclosed to, retained by, and used by, any component, officer, employee, or agent of the New Jersey Office of Homeland Security and Preparedness, including the NJCCIC, solely for the purpose of:

(1) identifying a cyber threat against a governmental entity, or an NJCCIC partner or member, including the source of the cyber threat or the existence of a security vulnerability;

(2) identifying the unauthorized access of an information system belonging to a governmental entity or an NJCCIC partner or member; or

(3) responding to, or otherwise preventing or mitigating, an imminent or ongoing cyber threat against a critical infrastructure asset in the State of New Jersey.

b. The NJCCIC or an NJCCIC partner or member may apply a cyber threat indicator or defensive measure shared or received through NJCCIC to perform a mitigation measure on:

(1) an information system of the State, county or local government;

(2) an information system of an NJCCIC partner or member; or

(3) an information system of any other entity, upon written consent of that entity.

c. The Attorney General, in consultation with the director, may establish guidelines to permit law enforcement use of cyber threat indicators received by a governmental entity to investigate, prosecute, disrupt, or otherwise respond to situations involving:

(1) computer criminal activity, or an attempt or conspiracy to commit computer criminal activity;

(2) a threat of death or serious bodily harm; or

(3) a serious threat to a minor, including sexual exploitation and threats to the physical safety thereof.

d. Nothing in P.L. , c. (C.) (pending before the Legislature as this bill) shall be construed to prohibit any entity from disclosing lawfully obtained cyber threat indicators to a governmental entity for investigative purposes consistent with that governmental entity's lawful authority.

8. a. Notwithstanding any other provision of law to the contrary, a private entity may, to defend against a cyber threat, operate a defensive measure that is applied to:

(1) the private entity's own information system;

(2) another private entity's information system, upon the authorization and written consent of the other entity; or

(3) a State, county, or local governmental entity's information system, upon the authorization and written consent of an authorized representative of such entity.

b. Notwithstanding any other provision of law to the contrary, a private entity may, for purposes related to evaluating cyber threats or cyber threat indicators, monitor:

(1) the private entity's own information system;

(2) another private entity's information system, upon the authorization and written consent of the other entity;

(3) a State, county, or local governmental entity's information system, upon the authorization and written consent of an authorized representative of such entity; or

(4) information that is stored on, processed by, or transiting an information system monitored by the private entity under this subsection.

c. Nothing in subsection b. of this section shall be construed to authorize the monitoring of an information system, or the use of any information obtained through such monitoring, other than as provided in P.L. , c. (C.) (pending before the Legislature as this bill), nor shall be construed to in any way limit otherwise lawful activity.

9. a. A cyber threat indicator or defensive measure shared with the NJCCIC in accordance with P.L. , c. (C.) (pending before the Legislature as this bill) and the procedures established

thereunder shall not be used by a State, county, or local governmental entity as evidence in a regulatory enforcement action against an entity that disclosed such cyber threat indicator to the NJCCIC. Provided, however, that nothing in this subsection shall be construed to prevent a State, county, or local governmental entity from using a cyber threat indicator or defensive measure received independently through other lawful means in a regulatory enforcement action, even if such cyber threat indicator is also received pursuant to P.L. , c. (C.) (pending before the Legislature as this bill).

b. Nothing in this section shall prevent a governmental entity from considering any such cyber threat indicator or defensive measure in the development or implementation of a regulation related to the prevention or mitigation of cyber threats to information systems, or inform the development or implementation of a regulation relating to such information systems.

10. a. The Legislature finds and declares that, notwithstanding any potential direct or indirect anti-competitive impact, the sharing of cyber threat indicators, the provision and receipt of assistance relating to the prevention, investigation, or mitigation of a cyber threat conducted in accordance with P.L. , c. (C.)(pending before the Legislature as this bill), and the procedures established thereunder, advance the policy of promoting Statewide coordination to effectively ensure cybersecurity preparedness and awareness, and the NJCCIC's performance of the role of central State-civilian interface as authorized under Executive Order No. 178 (2015) and this act is in furtherance of this policy.

b. It shall not be considered a violation of any provision of the "New Jersey Antitrust Act," P.L.1970, c.73 (C.56:9-1 et seq.), for two or more NJCCIC partners or members to share, provide or receive a cyber threat indicator or defensive measure, or to provide or receive assistance relating to the prevention, investigation, or mitigation of a cyber threat, if such activities are conducted in accordance with P.L. , c. (C.) (pending before the Legislature as this bill) and the procedures established thereunder.

11. Nothing in P.L. , c. (C.) (pending before the Legislature as this bill) shall be construed to:

a. authorize the NJCCIC to investigate any alleged violation of any provision of federal or State law;

b. permit a governmental entity:

(1) to require a private entity to share information with the NJCCIC or any State, county, or local governmental entity;

(2) to condition the disclosure of cyber threat indicators or defensive measures pursuant to P.L. , c. (C.) (pending before the Legislature as this bill) to a private entity on the

provision of cyber threat information to the NJCCIC or any State, county, or local governmental entity; or

(3) to condition the award of any State grant, contract, or purchase on the provision of cyber threat indicators to the NJCCIC or any State, county, or local governmental entity, if the provision of such indicators does not reasonably relate to the protection of the State, county, or local governmental entity's information system or information, goods, or services covered by the award;

c. affect or in any way limit any law or regulation that requires the disclosure, receipt, or retention of information;

d. affect or in any way limit an entity's authority to share information concerning potential criminal activity or investigations with law enforcement entities;

e. affect or prohibit otherwise lawful disclosures of information by a private entity to any governmental or private entity not conducted under P.L. , c. (C.) (pending before the Legislature as this bill);

f. allow the otherwise unauthorized disclosure by a private entity of information or material that has been determined by a State, county, or local governmental entity to require protection against unauthorized disclosure;

g. authorize the NJCCIC, or any State, county, or local governmental entity, to conduct surveillance of any private entity; or

h. authorize the monitoring of an information system, or the use of any information obtained through such monitoring, other than as provided in P.L. , c. (C.) (pending before the Legislature as this bill).

12. a. Notwithstanding the provisions of any other law to the contrary, any information furnished pursuant to P.L. , c. (C.) (pending before the Legislature as this bill) and the procedures established thereunder shall be treated as confidential and shall not be deemed a public record under P.L.1963, c.73 (C.47:1A-1 et seq.) or the common law concerning access to public records.

b. Any otherwise privileged communication obtained in accordance with, or in violation of, the provision of P.L. , c. (C.) (pending before the Legislature as this bill) shall retain its privileged status.

c. A cyber threat, cyber threat indicator, or defensive measure provided by a private entity to the NJCCIC, or State, county, or local governmental entity under this act shall be considered the proprietary, commercial, and financial information of the private entity when so designated by the private entity or a third party acting in accordance with the written authorization of the private entity. Information provided under this subsection shall not be considered proprietary if anonymized to remove any references to the identity of the private entity.

13. There is established in the Department of Law and Public Safety, in the Office of the Attorney General, a board which shall be known as the New Jersey Cybersecurity Advisory Board.

14. a. The board shall consist of 13 members. Six members of the board shall be designees of the following officers, serving ex officio: one by the Attorney General, one by the Chief Technology Officer of the Office of Information Technology, one by the Chief Executive Officer of the New Jersey Economic Development Authority, one by the Commissioner of the Department of Education, one by the Superintendent of State Police, and one by the Director of the Office of Homeland Security and Preparedness. Seven members of the board shall be private citizens who shall be appointed by the Governor, with the advice and consent of the Senate, who shall not hold elective public office while serving as a member of the board. Not more than four of the members appointed by the Governor shall be of the same political party. Of the seven members appointed by the Governor, two shall be individuals with expertise in technology; two shall be individuals with expertise in finance, business administration, or economics, of which one shall be upon the recommendation of the New Jersey Business and Industry Association; two shall be individuals with expertise in public safety; and one shall be an individual with expertise in education. The board shall select a chairperson and vice chairperson who shall be members of the board.

b. All nominations for appointment to the board shall be made within 90 days after the date of enactment of this act, P.L. , c. (pending before the Legislature as this bill). Each member appointed by the Governor shall hold office for a term of three years and until his successor is appointed and qualified. All vacancies shall be filled in the same manner as the original appointment. A member appointed to fill a vacancy occurring in the membership of the board for any reason other than the expiration of the term shall have a term of appointment for the unexpired term only. A member may be appointed for any number of successive terms. Any member appointed by the Governor may be removed from office by the Governor, for cause, after a hearing and may be suspended by the Governor pending the completion of the hearing. Members of the board appointed by the Governor shall serve without compensation, but shall be reimbursed for necessary expenses incurred in the performance of their duties as members.

c. The board shall serve as an advisory board to the New Jersey Cybersecurity and Communications Integration Cell (NJCCIC), and shall meet upon the call of the chairman at least four times per year. In addition, the board shall issue an annual report and any other reports and recommendations as necessary or as requested by the Governor.

15. a. The Office of Homeland Security and Preparedness, and such other agencies and offices as designated by the Governor, shall provide the support staff necessary for the board to perform its duties. The board also may, subject to the availability of funds, hire and employ, pursuant to Title 11A, Civil Service, of the New Jersey Statutes, other professional, technical, and clerical staff as may be necessary to perform the functions needed by the board.

b. The board may call to its assistance and avail itself of the services of the employees of any other State agencies as it may require and as may be available to it for that purpose, and the other State agencies shall provide the board with such information as may be necessary for the board to perform its functions.

c. Necessary funding to support the board and its staff may be provided from federal funds, private funds, and State funds appropriated for the same purposes as those of the board, as well as any other private sources of funding that may be identified and appropriate. To implement its purpose, the board is authorized, subject to the provisions of this act, to contract for and accept any gifts, grants, or loans of funds, property or financial, or other aid in any form from any public or private source as deemed appropriate.

d. The board shall submit an annual budget to the Attorney General for inclusion, as necessary, in the budget of the Department of Law and Public Safety, which shall include any proposals of the board for additional State agencies to participate in this initiative.

16. a. The purpose of the board is to:

(1) bring public and private sector experts together to make recommendations as to ways in which New Jersey may become both a leader in cybersecurity and improve its own cybersecurity infrastructure;

(2) develop better policies and enhanced standards in the area of cybersecurity to produce more efficient and protected proprietary networks, strengthen New Jersey’s cybersecurity framework, and advance vital prospects for economic development;

(3) suggest ways in which New Jersey can cultivate conditions to attract and retain, as well as secure a competitive advantage for, cybersecurity companies in the marketplace; and

(4) develop cybersecurity instruction, training, and programs to help prepare those currently seeking new occupational opportunities, as well as the next generation, for the rapidly developing cybersecurity workplace, reinforcing its dedication to education and coupling it with investment in cybersecurity.

b. To implement its purpose, the board shall:

(1) identify high risk cybersecurity issues facing the State;

(2) provide advice and recommendations related to securing New Jersey’s State networks, systems, and data, including interoperability, standardized plans and procedures, and evolving

threats and best practices to prevent the unauthorized access, theft, alteration, and destruction of the State's data;

(3) provide suggestions for the addition of cybersecurity to the New Jersey Office of Emergency Management's response capabilities, including testing cybersecurity incident response scenarios, recovery and restoration plans, and coordination with the federal government, in consultation with the New Jersey Office of Information Technology;

(4) present recommendations for science, technology, engineering, and math educational and training programs for all ages, offered through elementary schools, community colleges, and universities, in order to foster an improved cybersecurity workforce pipeline and equip cybersecurity professionals with a wide range of expertise;

(5) offer strategies to advance private sector cybersecurity economic development opportunities, including innovative technologies, research and development, and start-up firms, and maximize public-private partnerships throughout the State;

(6) provide suggestions for coordinating the review of and assessing opportunities for cybersecurity private sector growth as it relates to military facilities and defense activities in the State;

(7) offer suggestions for promoting awareness of cyber hygiene among the State's citizens, businesses, and government entities; and

(8) gather data about cybersecurity and cybersecurity threats and issue an annual report of its summary of the data collected to the Governor and the NJCCIC, which shall include any recommendations the board finds appropriate for changes in laws or regulations concerning programs and policies regarding cybersecurity, information and technology, or other matters of public safety related thereto.

c. At the end of three years after the date of enactment of this act, the purposes and activities of the New Jersey Cybersecurity Advisory Board shall come before the Legislature for review through hearings held by appropriate legislative standing reference committees.

17. This act shall take effect on the first day of the sixth month following enactment, but the Attorney General and Director of the Office of Homeland Security and Preparedness may take such anticipatory action as may be necessary to effectuate the provisions of this act.