STATE OF NEW YORK

6769--A

Cal. No. 67

2025-2026 Regular Sessions

IN ASSEMBLY

March 13, 2025

Introduced by M. of A. JONES -- read once and referred to the Committee on Local Governments -- advanced to a third reading, passed by Assembly and delivered to the Senate, recalled from the Senate, vote reconsidered, bill amended, ordered reprinted, retaining its place on the order of third reading

AN ACT to amend the general municipal law and the executive law, in relation to requiring municipal cybersecurity incident reporting and exemptions such reports from freedom of information requirements; and to amend the state technology law, in relation to requiring cybersecurity awareness training for government employees, data protection standards, and cybersecurity protection

The People of the State of New York, represented in Senate and Assembly, do enact as follows:

Section 1. The general municipal law is amended by adding a new article 19-C to read as follows:

ARTICLE 19-C

CYBERSECURITY INCIDENT REPORTING REQUIREMENTS FOR MUNICIPAL CORPORATIONS AND PUBLIC AUTHORITIES

Section 995-a. Definitions.
995-b. Reporting of cybersecurity incidents.
995-c. Notice and explanation of ransom payment.

§ 995-a. Definitions. For the purposes of this article: 1. "Cybersecurity incident" means an event occurring on or conducted through a computer network that actually or imminently jeopardizes the integrity, confidentiality, or availability of computers, information or communications systems or networks, physical or virtual infrastructure controlled by computers or information systems, or information resident thereon.

2. "Cyber threat" means any circumstance or event with the potential to adversely impact organizational operations, organizational assets, or individuals through an information system via unauthorized access,

EXPLANATION--Matter in *italics* (underscored) is new; matter in brackets [-] is old law to be omitted.

LBD10937-05-5

destruction, disclosure, modification of information, and/or denial of service.

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

(a) malicious reconnaissance, including anomalous patterns of communications that appear to be transmitted for the purpose of gathering technical information related to a cybersecurity threat or security vulnerability;

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

(c) a security vulnerability, including anomalous activity that appears to indicate the existence of a security vulnerability;

(d) 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;

(e) malicious cyber command and control;

(f) the actual or potential harm caused by an incident, including a description of the information exfiltrated as a result of a particular cybersecurity threat;

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

(h) any combination thereof.

4. "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 cybersecurity threat or security vulnerability. The term "defensive measure" 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 municipal corporation or public authority operating the measure, or federal entity that is authorized to provide consent and has provided consent to that municipal corporation or public authority for operation of such measure.

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

6. "Municipal corporation" means:

(a) A municipal corporation as defined in section one hundred nineteen-n of this chapter; or

(b) A district as defined in section one hundred nineteen-n of this chapter.

7. "Public authority" means any state authority or local authority, as such terms are defined in section two of the public authorities law, or any subsidiary thereof.

8. "Ransom payment" means the transmission of any money or other property or asset, including virtual currency, or any portion thereof, which has at any time been delivered as ransom in connection with a ransomware attack.

9. "Ransomware attack":

(a) means an incident that includes the use or threat of use of unauthorized or malicious code on an information system, or the use or threat of use of another digital mechanism such as a denial of service attack, to interrupt or disrupt the operations of an information system or compromise the confidentiality, availability, or integrity of elec-

tronic data stored on, processed by, or transiting an information system to extort a demand for a ransom payment; and

(b) does not include any such event in which the demand for payment is:

(i) not genuine; or

(ii) made in good faith by an entity in response to a specific request by the owner or operator of the information system.

§ 995-b. Reporting of cybersecurity incidents. 1. Notwithstanding any other provision of law to the contrary, all municipal corporations and public authorities shall report cybersecurity incidents and when applicable, the demand of a ransom payment, to the commissioner of the division of homeland security and emergency services in the form and method prescribed by such commissioner. Such report shall include whether the reporting municipal corporation or public authority is requesting or declining advice and/or technical assistance from the division of homeland security and emergency services with respect to the reported cybersecurity incident or demand for a ransom payment.

2. All municipal corporations and public authorities shall report cybersecurity incidents, including demands for ransom payment, no later than seventy-two hours after the municipal corporation or public authority reasonably believes the cybersecurity incident has occurred.

3. Any cybersecurity incident report and any records related to a ransom payment submitted to the commissioner of the division of homeland security and emergency services pursuant to the requirements of this article shall be exempt from disclosure under article six of the public officers law.

§ 995-c. Notice and explanation of ransom payment. Notwithstanding any other provision of law to the contrary, each municipal corporation or public authority shall, in the event of a ransom payment made in connection with a cybersecurity incident involving the municipal corporation or public authority, provide the commissioner of the division of homeland security and emergency services through means prescribed by such commissioner with the following:

1. within twenty-four hours of the ransom payment, notice of the payment; and

2. within thirty days of the ransom payment, a written description of the reasons payment was necessary, the amount of the ransom payment, the means by which the ransom payment was made, a description of alternatives to payment considered, all diligence performed to find alternatives to payment and all diligence performed to ensure compliance with applicable state and federal rules and regulations including those of the United States department of the treasury's office of foreign assets control.

§ 2. The executive law is amended by adding a new section 711-c to read as follows:

§ 711-c. Cybersecurity incident reviews. 1. Definitions. As used in this section, the terms cybersecurity incident, cyber threat, cyber threat indicator, defensive measure, information system, municipal corporation, public authority, ransom payment and ransomware attack shall have the same meaning as such terms are defined in article nineteen-C of the general municipal law.

2. The commissioner, or their designees, shall review each cybersecurity incident report and notice and explanation of ransom payment submitted pursuant to sections nine hundred ninety-five-b and nine hundred ninety-five-c of the general municipal law to assess potential impacts

of cybersecurity incidents and ransom payments on the health, safety, welfare or security of the state, or its residents.

3. The commissioner, or their designees, may work with appropriate state agencies, federal law enforcement, and federal homeland security agencies to provide municipal corporations and public authorities with reports of cybersecurity incidents and trends, including but not limited to, to the maximum extent practicable, related contextual information, cyber threat indicators, and defensive measures. The commissioner may coordinate and share such reported information with municipal corporations, public authorities, state agencies, and federal law enforcement and homeland security agencies to respond to and mitigate cybersecurity threats.

4. Such reports, assessments, records, reviews, documents, recommendations, guidance and any information contained or used in its preparation shall be exempt from disclosure under article six of the public officers law.

5. No later than forty-eight hours after receiving a cybersecurity incident report containing a request for advice and/or technical assistance from the division pursuant to subdivision one of section nine hundred ninety-five-b of the general municipal law, the commissioner or the commissioner's designees shall acknowledge receipt of such request. As soon as possible after receiving such a request, the commissioner or the commissioner's designees, subject to the commissioner's discretion in prioritizing the division's response to the municipal corporation's or public authority's cybersecurity incident report, shall provide advice to the requesting municipal corporation or public authority and, to the extent practicable, provide technical assistance.

§ 3. The state technology law is amended by adding a new section 103-f to read as follows:

§ 103-f. Cybersecurity awareness training. 1. (a) Employees of the state who use technology as a part of their official job duties shall take annual cybersecurity awareness training beginning January first, two thousand twenty-six. Employees of the state shall be required to complete the training provided by the office.

(b) For purposes of this section, "employees of the state" shall include employees of all state agencies and all public benefit corporations, the heads of which are appointed by the governor.

2. Employees of a county, a city, a town, a village, or a district as defined in section one hundred nineteen-n of the general municipal law, who use technology as a part of their official job duties shall take annual cybersecurity awareness training beginning January first, two thousand twenty-six. The office shall make a cybersecurity training available for use by a county, a city, a town, a village, or a district as defined in section one hundred nineteen-n of the general municipal law, at no charge, provided however, no employee of a county, a city, a town, a village, or a district as defined in section one hundred nineteen-n of the general municipal law shall be required to complete such training provided by the office and the cybersecurity awareness training requirements of this section may be satisfied by the completion of other cybersecurity awareness training.

3. All training mandated by this section shall be conducted during the employee's regular working hours and employees shall receive compensation at their regular rate of pay for any time spent participating in such training.

§ 4. The state technology law is amended by adding a new section 210 to read as follows:

§ 210. Cybersecurity protection. 1. Definitions. For purposes of this section, the following terms shall have the following meanings:

(a) "Breach of the security of the system" shall have the same meaning as such term is defined in section two hundred eight of this article.

(b) "Data subject" means any natural person about whom personal information has been collected by a state agency.

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

(d) "State agency-maintained personal information" means personal information stored by a state agency that was generated by a state agency or provided to the state agency by the data subject, a state agency, a federal governmental entity, or any other third-party source. Such term shall also include personal information provided by an adverse party in the course of litigation or other adversarial proceeding.

(e) "State agency" shall have the same meaning as such term is defined in section one hundred one of this chapter.

2. Data protection standards. The director shall issue policies and standards for:

(a) protection against breaches of the security of the information systems and for personal information used by such information systems;

(b) data backup;

(c) information system recovery;

(d) secure sanitization and deletion of data;

(e) vulnerability management and assessment; and

(f) annual workforce training regarding protection against breaches of the security of the system, as well as processes and procedures that should be followed in the event of a breach of the security of the system.

3. Information system inventory. (a) No later than two years after the effective date of this section, each state agency shall create, then maintain, an inventory of its information systems.

(b) Upon written request from the office, a state agency shall provide the office with the state agency-maintained information systems inventories required to be created or updated pursuant to this subdivision.

(c) Notwithstanding paragraph (a) of this subdivision, the state agency-maintained information systems inventories required to be created or updated pursuant to this subdivision shall be kept confidential, as disclosure of such information would jeopardize the security of a state agency's information systems and information technology assets and, further, shall not be made available for disclosure or inspection under the state freedom of information law.

4. Incident management and recovery. (a) No later than eighteen months after the effective date of this section, each state agency shall have created an incident response plan for incidents involving a breach of the security of the system that render an information system or its data unavailable, and incidents involving a breach of the security of the system that result in the alteration or deletion of or unauthorized access to, personal information.

(b) Such incident response plan shall include, but not be limited to, a procedure for situations where information systems have been adversely affected by a breach of the security of the system, as well as a procedure for the recovery of personal information and information systems.

(c) Beginning January first, two thousand twenty-eight and on an annual basis thereafter, each state agency shall complete at least one exercise of its incident response plan. Upon completion of such exercise,

the state agency shall document the incident response plan's successes and shortcomings in an incident response plan exercise report. The incident response plan and any incident response plan exercise reports shall be kept confidential, as disclosure of such information would jeopardize the security of a state agency's information systems and information technology assets, and, further, shall not be made available for disclosure or inspection under the state freedom of information law.

5. No private right of action. Nothing set forth in this section shall be construed as creating or establishing a private cause of action.

§ 5. Severability. The provisions of this act shall be severable and if any portion thereof or the applicability thereof to any person or circumstances shall be held to be invalid, the remainder of this act and the application thereof shall not be affected thereby.

§ 6. This act shall take effect immediately; provided, however, that sections one and two of this act shall take effect on the thirtieth day after such effective date.