STATE OF NEW YORK

6769

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

AN ACT to amend the general municipal law and the executive law, in relation to requiring municipal cybersecurity incident or ransomeware attack reporting and exempting such reports from freedom of information requirements; and to amend the state technology law, in relation to requiring cybersecurity awareness training

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

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

3. "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.

4. "Ransom payment" means the transmission of any money or other property or asset, including virtual currency, or any portion thereof, which

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

LBD10937-01-5

has at any time been delivered as ransom in connection with a ransomware attack.

5. "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 electronic 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 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.

2. All municipal corporations shall report cybersecurity incidents, and demands for a ransom payment, no later than seventy-two hours after the municipality reasonably believes the cybersecurity incident has occurred or demand for a ransom payment has been made.

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 shall, in the event of a ransom payment made in connection with a cybersecurity incident or ransomware attack involving the municipal corporation, provide the commissioner of the division of homeland security and emergency services through means prescribed by such commissioner with the following:

(a) within twenty-four hours of the ransom payment, notice of the payment; and

(b) 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. For the purposes of this section:

(a) "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.

(b) "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, destruction, disclosure, modification of information, and/or denial of service.

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

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

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

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

(iv) 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;

(v) malicious cyber command and control;

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

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

(viii) any combination thereof.

(d) "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 "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 operating the measure, or federal entity that is authorized to provide consent and has provided consent to that municipal corporation for operation of such measure.

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

(f) "Municipal corporation" means:

(i) A municipal corporation as defined in section one hundred nineteen-n of the general municipal law; or

(ii) A district as defined in section one hundred nineteen-n of the general municipal law.

(g) "Ransomware attack":

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

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

(A) not genuine; or

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

2. The commissioner, or their designee, shall review each cybersecurity incident report and notice of ransom payment 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 designee, may work with appropriate state agencies, federal law enforcement, and federal homeland security agencies to provide municipal corporations 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 shall coordinate and share such reported information with municipal corporations, and may coordinate and share such reported information with state agencies, and federal law enforcement and homeland security agencies as necessary to respond to and mitigate cyber threats.

4. Within forty-eight hours of receiving a cybersecurity incident report or notice of a demand for ransom payment pursuant to article nineteen-c of the general municipal law, the commissioner, or their designee, shall provide advice and technical assistance to the municipal corporation that reported such cybersecurity incident or demand for ransom in connection with a cybersecurity incident or ransomware attack, and shall further notify any municipal corporation that may be affected or impacted by such cybersecurity threat or ransomware attack within forty-eight hours of receiving such report.

5. 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.

§ 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, 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, or a village at no charge.

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. This act shall take effect on the one hundred eightieth day after it shall have become a law.