

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 ransomware 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

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. "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

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

3 5. "Ransomware attack":

4 (a) means an incident that includes the use or threat of use of unau-
5 thorized or malicious code on an information system, or the use or
6 threat of use of another digital mechanism such as a denial of service
7 attack, to interrupt or disrupt the operations of an information system
8 or compromise the confidentiality, availability, or integrity of elec-
9 tronic data stored on, processed by, or transiting an information system
10 to extort a demand for a ransom payment; and

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

13 (i) not genuine; or

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

16 § 995-b. Reporting of cybersecurity incidents. 1. Notwithstanding any
17 other provision of law to the contrary, all municipal corporations shall
18 report cybersecurity incidents and when applicable, the demand of a
19 ransom payment, to the commissioner of the division of homeland security
20 and emergency services in the form and method prescribed by such commis-
21 sioner.

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

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

31 § 995-c. Notice and explanation of ransom payment. Notwithstanding any
32 other provision of law to the contrary, each municipal corporation
33 shall, in the event of a ransom payment made in connection with a
34 cybersecurity incident or ransomware attack involving the municipal
35 corporation, provide the commissioner of the division of homeland secu-
36 rity and emergency services through means prescribed by such commission-
37 er with the following:

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

40 (b) within thirty days of the ransom payment, a written description of
41 the reasons payment was necessary, the amount of the ransom payment, the
42 means by which the ransom payment was made, a description of alterna-
43 tives to payment considered, all diligence performed to find alterna-
44 tives to payment and all diligence performed to ensure compliance with
45 applicable state and federal rules and regulations including those of
46 the United States department of the treasury's office of foreign assets
47 control.

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

50 § 711-c. Cybersecurity incident reviews. 1. For the purposes of this
51 section:

52 (a) "Cybersecurity incident" means an event occurring on or conducted
53 through a computer network that actually or imminently jeopardizes the
54 integrity, confidentiality, or availability of computers, information or
55 communications systems or networks, physical or virtual infrastructure

1 controlled by computers or information systems, or information resident
2 thereon.

3 (b) "Cyber threat" means any circumstance or event with the potential
4 to adversely impact organizational operations, organizational assets, or
5 individuals through an information system via unauthorized access,
6 destruction, disclosure, modification of information, and/or denial of
7 service.

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

10 (i) malicious reconnaissance, including anomalous patterns of communi-
11 cations that appear to be transmitted for the purpose of gathering tech-
12 nical information related to a cyber threat or security vulnerability;

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

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

17 (iv) a method of causing a user with legitimate access to an informa-
18 tion system or information that is stored on, processed by, or transit-
19 ing an information system to unwittingly enable the defeat of a security
20 control or exploitation of a security vulnerability;

21 (v) malicious cyber command and control;

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

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

27 (viii) any combination thereof.

28 (d) "Defensive measure" means an action, device, procedure, signature,
29 technique, or other measure applied to an information system or informa-
30 tion that is stored on, processed by, or transiting an information
31 system that detects, prevents, or mitigates a known or suspected cyber
32 threat or security vulnerability. The term "defensive measure" does not
33 include a measure that destroys, renders unusable, provides unauthorized
34 access to, or substantially harms an information system or information
35 stored on, processed by, or transiting such information system not owned
36 by the municipal corporation operating the measure, or federal entity
37 that is authorized to provide consent and has provided consent to that
38 municipal corporation for operation of such measure.

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

42 (f) "Municipal corporation" means:

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

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

47 (g) "Ransomware attack":

48 (i) means an incident that includes the use or threat of use of unau-
49 thorized or malicious code on an information system, or the use or
50 threat of use of another digital mechanism such as a denial of service
51 attack, to interrupt or disrupt the operations of an information system
52 or compromise the confidentiality, availability, or integrity of elec-
53 tronic data stored on, processed by, or transiting an information system
54 to extort a demand for a ransom payment; and

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

1 (A) not genuine; or
2 (B) made in good faith by an entity in response to a specific request
3 by the owner or operator of the information system.

4 2. The commissioner, or their designee, shall review each cybersecurity
5 incident report and notice of ransom payment and explanation of
6 ransom payment submitted pursuant to sections nine hundred ninety-five-b
7 and nine hundred ninety-five-c of the general municipal law to assess
8 potential impacts of cybersecurity incidents and ransom payments on the
9 health, safety, welfare or security of the state, or its residents.

10 3. The commissioner, or their designee, may work with appropriate
11 state agencies, federal law enforcement, and federal homeland security
12 agencies to provide municipal corporations with reports of cybersecurity
13 incidents and trends, including but not limited to, to the maximum
14 extent practicable, related contextual information, cyber threat indica-
15 tors, and defensive measures. The commissioner shall coordinate and
16 share such reported information with municipal corporations, and may
17 coordinate and share such reported information with state agencies, and
18 federal law enforcement and homeland security agencies as necessary to
19 respond to and mitigate cyber threats.

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

29 5. Such reports, assessments, records, reviews, documents, recommenda-
30 tions, guidance and any information contained or used in its preparation
31 shall be exempt from disclosure under article six of the public officers
32 law.

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

35 § 103-f. Cybersecurity awareness training. 1. (a) Employees of the
36 state who use technology as a part of their official job duties shall
37 take annual cybersecurity awareness training beginning January first,
38 two thousand twenty-six. Employees of the state shall be required to
39 complete the training provided by the office.

40 (b) For purposes of this section, "employees of the state" shall
41 include employees of all state agencies and all public benefit corpo-
42 rations, the heads of which are appointed by the governor.

43 2. Employees of a county, a city, a town, village, or a district as
44 defined in section one hundred nineteen-n of the general municipal law
45 who use technology as a part of their official job duties shall take
46 annual cybersecurity awareness training beginning January first, two
47 thousand twenty-six. The office shall make a cybersecurity training
48 available for use by a county, a city, a town, or a village at no
49 charge.

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

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