§ 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, 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

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.