File #: Int 2066-2020, **Version:** *

Int. No. 2066

By Council Members Kallos, Salamanca, Gjonaj and Chin

A Local Law to amend the administrative code of the city of New York, in relation to establishing a special inspector of cybersecurity within the department of investigation

Be it enacted by the Council as follows:

Section 1. Chapter 3 of title 33 of the administrative code of the city of New York is amended by adding a new section 33-301 to read as follows:

§33-301 Special inspector of cybersecurity. a. Defenitions. For the purposes of this section, the following terms have the following meanings:

Adequate security. The term "adequate security" means protective measures that are commensurate with a potential security breach and the protection of sensitive information from cyber-attacks. To provide adequate security, any agency or contractor shall implement, at a minimum, security requirements in accordance with National Institute of Standards and Technology Special Publication 800-171, "Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations" or successor version.

City contractor information system. The term "city contractor information system" means an information system that is owned or operated by or on behalf of a contractor that processes, stores, or transmits data, sensitive information or any combination thereof on behalf of the city.

Cyber-attack. The term "cyber-attack" means the attempt, or successful completion of an attempt to damage, destroy, or deny service to a computer or computer system, whether physical or virtual.

Cybersecurity. The term "cybersecurity" means the protection of information by preventing, detecting, and responding to cyber-attacks or security breach.

Security breach. The term "security breach" means a loss, theft, unauthorized access, or an exceeded authorized access, other than an unauthorized access incidental to the scope of employment, to data containing personal identifying information as defined in section 10-501, in electronic or printed form, that results in the potential compromise of the confidentiality, integrity, or availability of the data.

b. The commissioner shall appoint a special inspector of cybersecurity, who shall be authorized to:

1. investigate any city agency security breaches in electronic form and ransomware attacks committed by any officer, employee of the city, or city contractor. Such investigation shall include, but not limited to, identifying compromised computers, servers, specific data, or user accounts;

2. assist and ensure compliance with federal, state, and local data breach notification requirements;

3. refer cyber attacks or incidents of a security breach to appropriate agencies.

c. On or before February 1, 2021 and annually thereafter, the special inspector of cybersecurity shall submit to the mayor and speaker of the council a report on cyber attacks or incidents of a security breach. Such report shall include, but need not be limited to, the following information:

1. The date and time at which each incident occurred;

2. The name of the agency or city contractor involved in each incident; and

3. The type of data contained on such system that was the subject to each incident;

No report required pursuant to this subdivision shall contain personal identifying information.

§ 2. Subdivision a of section 10-502 of the administrative code of the city of New York, as added by local law number 11 for the year 2017, is amended to read as follows:

a. Any city agency or city contractor that owns or leases data that includes personal identifying information and any city agency that maintains but does not own data that includes personal identifying information, shall immediately disclose to the police department and to the special inspector of cybersecurity any breach of security following discovery by a supervisor or manager, or following notification to a supervisor or manager, of such breach if such personal identifying information was, or is reasonably believed to have been, acquired by an unauthorized person.

b. Subsequent to compliance with the provisions set forth in subdivision a of this section, any city agency or city contractor that owns or leases data that includes personal identifying information shall disclose, in accordance with the procedures set forth in subdivision d of this section, any breach of security following discovery by a supervisor or manager, or following notification to a supervisor or manager, of such breach to any person whose personal identifying information was, or is reasonably believed to have been, acquired by an unauthorized person.

c. Subsequent to compliance with the provisions set forth in subdivision a of this section, any city agency or city contractor that maintains but does not own data that includes personal identifying information shall disclose, in accordance with the procedures set forth in subdivision d of this section, any breach of security following discovery by a supervisor or manager, or following notification to a supervisor or manager, of such breach to the owner, lessor or licensor of the data if the personal identifying information was, or is reasonably believed to have been, acquired by an unauthorized person.

d. The disclosures required by subdivisions b and c of this section shall be made as soon as practicable by a method reasonable under the circumstances. Provided said method is not inconsistent with the legitimate needs of law enforcement or any other investigative or protective measures necessary to restore the reasonable integrity of the data system, disclosure shall be made by at least one of the following means:

1. Written notice to the individual at his or her last known address; or
2. Verbal notification to the individual by telephonic communication; or
3. Electronic notification to the individual at his or her last known e-mail address.

e. Should disclosure pursuant to paragraph one, two or three of subdivision d be impracticable or inappropriate given the circumstances of the breach and the identity of the victim, such disclosure shall be made by a mechanism of the agency's election, provided such mechanism is reasonably targeted to the individual in a manner that does not further compromise the integrity of the personal information.

§ 3. This local law takes effect 120 days after it becomes law.

IB
LS #14024
06/23/2020 3PM