



Legislation Text

File #: Int 1190-2025, Version: *

Int. No. 1190

By Council Members Narcisse, Banks, Louis and Brannan

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 1 of title 33 of the administrative code of the city of New York is amended by adding a new section 33-102 to read as follows:

§33-102 Special inspector of cybersecurity. a. Definitions. For the purposes of this section, the following terms have the following meanings:

Breach of security. The term “breach of security” 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 private information, in electronic or printed form, that results in the potential compromise of the confidentiality, integrity, or availability of the data.

Cyberattack. The term “cyberattack” 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 a cyberattack or breach of security.

Private information. The term “private information” has the same meaning as set forth in section 10-501.

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

1. investigate any city agency breaches of security in electronic form and cyberattacks against the city

committed by any officer, employee of the city, or city contractor. Such investigation shall include, but not be 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; and

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

c. On or before February 1, 2026, and annually thereafter, the special inspector of cybersecurity shall submit to the mayor and speaker of the council a report on cyberattacks or incidents of a breach of security.

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 private information.

§ 2. Subdivisions a, b and c of section 10-502 of the administrative code of the city of New York is amended to read as follows:

a. Any city agency or city contractor that owns, leases, or licenses data that includes private information shall promptly disclose to the chief privacy officer, office of cyber command, [and] department of information technology and telecommunications, 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 private information was, or is reasonably believed to have been, accessed, acquired, disclosed, or used 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, leases, or licenses data that includes private information shall disclose, in accordance with the procedures set forth in subdivisions d, e and f 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 individual whose private information was, or is reasonably believed to have been, accessed,

acquired, disclosed, or used by an unauthorized person.

c. Any city agency or city contractor that maintains but does not own, lease, or license data that includes private information shall disclose 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 private information was, or is reasonably believed to have been, accessed, acquired, disclosed, or used by an unauthorized person.

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

IB
LS #11712
01/17/2025