STATE OF NEW YORK

7331--A

2023-2024 Regular Sessions

IN ASSEMBLY

May 17, 2023

Introduced by M. of A. OTIS -- read once and referred to the Committee on Governmental Employees -- reference changed to the Committee on Science and Technology -- committee discharged, bill amended, ordered reprinted as amended and recommitted to said committee

AN ACT to amend the state technology law, in relation to requiring governmental entities to implement multifactor authentication for local and remote network access

The People of the State of New York, represented in Senate and Assembly, do enact as follows:

Section 1. Section 202 of the state technology law is amended by adding two new subdivisions 9 and 10 to read as follows:

9. "Governmental entity" shall mean any state or local department, board, bureau, division, commission, committee, school district, public authority, public benefit corporation, council or office, including all entities defined pursuant to section two of the public authorities law. Such term shall include the state university of New York and the city university of New York. Further, such term shall include any county, city, town or village but shall not include the judiciary or state and local legislatures.

10. "Multifactor authentication" shall mean using two or more different types of identification credentials to achieve authentication. The types of identification credentials shall include:

(a) knowledge-based credentials, which is a knowledge-based authentication that requires the user to provide information that they know such as passwords or PINs;

(b) possession-based credentials, which is authentication that requires individuals to have something specific in their possession, such as security tokens, key fobs, SIM cards or smartphone applications; and

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

LBD09003-03-4

(c) inherence-based credentials, which is authentication that requires user-specific biological traits to confirm identity for login, such as fingerprints or facial recognition.

§ 2. The state technology law is amended by adding three new sections 210, 211, and 212 to read as follows:

§ 210. Multifactor authentication. 1. Multifactor authentication requirement. Every governmental entity shall, whenever possible and feasable, consider implementing multifactor authentication for local and remote network access to any email accounts, cloud storage accounts, web applications, networks, databases, or servers, maintained by such entity or on behalf of such entity, for the employees and officers of such entity or for any other individuals providing services to or on behalf of such entity.

2. Technical standard. The office shall promulgate rules to establish standard technical requirements for governmental entities for complying with subdivision one of this section. Such rules shall include regulations addressing inherence-based credentials including proper storage of traits relating to user-specific biological traits. Such rules shall additionally include provisions regarding compliance for individuals with disabilities or special needs. For the purposes of this subdivision, the office may use and refer to the guidelines provided by the National Institute of Standards and Technology, the Federal Risk and Authorization Management Program (FedRAMP), the Federal Information Security Management Act of 2002 (FISMA) and the Defense Federal Acquisition Regulation Supplement (DFARS).

3. Waivers. The office, upon application by a governmental entity, may completely or partially waive the requirements of this section for such governmental entity. Such waiver shall be valid for no longer than two years and shall be reapproved after expiration. The office shall promulgate rules to establish the application process and criteria for such waivers.

§ 211. Privacy requirements. This section shall apply to the use of multifactor authentication at governmental entities and to any vendors and/or third-party contractors administering the multifactor authentication on behalf of the governmental entity.

1. No governmental entity shall require the use of an inherence-based credential to access local and/or remote network access.

2. No governmental entity that facilitates the use of inherence-based credentials to access local and remote network access shall sell or monetize such data.

3. No governmental entity that facilitates the use of inherence-based credentials to access local and remote network access shall share such data with law enforcement without a warrant.

4. Any governmental entity and any applicable third-party contractors that facilitate the use of inherence-based credentials shall agree to comply with the standards established by the office and all statutory privacy standards.

§ 212. Public website encryption. Every website maintained by or on behalf of a governmental entity shall encrypt all exchanges and transfers between a web server, maintained by or on behalf of a governmental entity, and a web browser of hypertext or of electronic information, and require web browsers to request such encrypted exchange or transfer at all times for such websites, provided that such encryption shall not be required if such exchanges or transfers are conducted in a manner that provides at least an equivalent level of confidentiality, data integrity and authentication.

§ 3. This act shall take effect one year after it shall have become a law. Effective immediately, the addition, amendment, and/or repeal of any rule or regulation necessary for the implementation of this act on its effective date are authorized to be made and completed on or before such effective date.