

# STATE OF NEW YORK

7331--B

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 -- reported and referred to the Committee on Ways and Means -- 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:

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

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

11 10. "Multifactor authentication" shall mean using two or more differ-  
12 ent types of identification credentials to achieve authentication. The  
13 types of identification credentials shall include:

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

17 (b) possession-based credentials, which is authentication that  
18 requires individuals to have something specific in their possession,

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

LBD09003-05-4

1 such as security tokens, key fobs, SIM cards or smartphone applications;  
2 and

3 (c) biometric information, which is any measurable physical, physio-  
4 logical or behavioral characteristics that are attributable to a person,  
5 including but not limited to facial characteristics, fingerprint charac-  
6 teristics, hand characteristics, eye characteristics, vocal character-  
7 istics, and any other characteristics that can be used to identify a  
8 person including, but not limited to: fingerprints; handprints; retina  
9 and iris patterns; DNA sequence; voice; gait; and facial geometry.

10 § 2. The state technology law is amended by adding three new sections  
11 210, 211, and 212 to read as follows:

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

20 2. Technical standard. The office shall promulgate rules to establish  
21 standard technical requirements for governmental entities for complying  
22 with subdivision one of this section. Such rules shall include regu-  
23 lations addressing biometric information including proper storage of  
24 traits relating to user-specific biological traits. Such rules shall  
25 additionally include provisions regarding compliance for individuals  
26 with disabilities or special needs. For the purposes of this subdivi-  
27 sion, the office may use and refer to the guidelines provided by the  
28 National Institute of Standards and Technology, the Federal Risk and  
29 Authorization Management Program (FedRAMP), the Federal Information  
30 Security Management Act of 2002 (FISMA) and the Defense Federal Acquisi-  
31 tion Regulation Supplement (DFARS).

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

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

42 1. No governmental entity shall require the use of biometric informa-  
43 tion to access local and/or remote network access.

44 2. No governmental entity that facilitates the use of biometric infor-  
45 mation to access local and remote network access shall sell or monetize  
46 such data.

47 3. No governmental entity that facilitates the use of biometric infor-  
48 mation to access local and remote network access shall share such data  
49 with law enforcement without a warrant.

50 4. Any governmental entity and any applicable third-party contractors  
51 that facilitate the use of biometric information shall agree to comply  
52 with the standards established by the office and all statutory privacy  
53 standards.

54 § 212. Public website encryption. Every website maintained by or on  
55 behalf of a governmental entity shall encrypt all exchanges and trans-  
56 fers between a web server, maintained by or on behalf of a governmental

1 entity, and a web browser of hypertext or of electronic information, and  
2 require web browsers to request such encrypted exchange or transfer at  
3 all times for such websites, provided that such encryption shall not be  
4 required if such exchanges or transfers are conducted in a manner that  
5 provides at least an equivalent level of confidentiality, data integrity  
6 and authentication.

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