

# STATE OF NEW YORK

7331

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

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

(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 implement multifactor

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

LBD09003-02-3

1 authentication for local and remote network access to any email  
2 accounts, cloud storage accounts, web applications, networks, databases,  
3 or servers, maintained by such entity or on behalf of such entity, for  
4 the employees and officers of such entity or for any other individuals  
5 providing services to or on behalf of such entity.

6 2. Technical standard. The office shall promulgate rules to establish  
7 standard technical requirements for governmental entities for complying  
8 with subdivision one of this section. Such rules shall include regu-  
9 lations addressing inherence-based credentials including proper storage  
10 of traits relating to user-specific biological traits. Such rules shall  
11 additionally include provisions regarding compliance for individuals  
12 with disabilities or special needs. For the purposes of this subdivi-  
13 sion, the office may use and refer to the guidelines provided by the  
14 National Institute of Standards and Technology, the Federal Risk and  
15 Authorization Management Program (FedRAMP), the Federal Information  
16 Security Management Act of 2002 (FISMA) and the Defense Federal Acquisi-  
17 tion Regulation Supplement (DFARS).

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

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

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

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

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

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

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

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