

# STATE OF NEW YORK

2652

2021-2022 Regular Sessions

## IN SENATE

January 22, 2021

Introduced by Sen. SAVINO -- read twice and ordered printed, and when printed to be committed to the Committee on Internet and Technology

AN ACT to amend the state technology law, in relation to requiring governmental entities to implement multifactor authentication for local and network remote 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,  
19 such as security tokens, key fobs, SIM cards or smartphone applications;  
20 and

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

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

LBD08845-01-1

1     § 2. The state technology law is amended by adding two new sections  
2 209 and 210 to read as follows:

3     § 209. Multifactor authentication. 1. Multifactor authentication  
4 requirement. Every governmental entity shall implement multifactor  
5 authentication for local and remote network access to any email  
6 accounts, cloud storage accounts, web applications, networks, databases,  
7 or servers, maintained by such entity or on behalf of such entity, for  
8 the employees and officers of such entity or for any other individuals  
9 providing services to or on behalf of such entity.

10    2. Technical standard. The office shall promulgate rules to establish  
11 standard technical requirements for governmental entities for complying  
12 with subdivision one of this section. Such rules shall include  
13 provisions regarding compliance for individuals with disabilities or  
14 special needs. For the purposes of this subdivision, the office may use  
15 and refer to the guidelines provided by the National Institute of Stand-  
16 ards and Technology, the Federal Risk and Authorization Management  
17 Program (FedRAMP), the Federal Information Security Management Act of  
18 2002 (FISMA) and the Defense Federal Acquisition Regulation Supplement  
19 (DFARS).

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

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

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