

# STATE OF NEW YORK

7312

2021-2022 Regular Sessions

## IN SENATE

August 4, 2021

Introduced by Sen. THOMAS -- read twice and ordered printed, and when printed to be committed to the Committee on Rules

AN ACT to amend the state technology law, in relation to enacting the "critical infrastructure standards and procedures act"

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

1 Section 1. The state technology law is amended by adding a new article  
2 4 to read as follows:

### ARTICLE 4

#### CRITICAL INFRASTRUCTURE STANDARDS AND PROCEDURES ACT

3 Section 401. Short title.

4 402. Definitions.

5 403. Compliance with cybersecurity standards for critical  
6 infrastructure.

7 404. Procurement, construction, reconstruction, alteration,  
8 design and commissioning of critical infrastructure or  
9 automation control systems or automation control system  
10 components.

11 405. Operations and maintenance of critical infrastructure.

12 § 401. Short title. This article shall be known and may be cited as  
13 the "critical infrastructure standards and procedures (CRISP) act".

14 § 402. Definitions. The following terms shall have the following mean-  
15 ings:

16 1. Critical infrastructure shall include, but shall not be limited to:

17 (a) public transportation;

18 (b) water and wastewater treatment facilities;

19 (c) public utilities and services subject to the jurisdiction, super-  
20 vision, powers and duties of the public service commission and the  
21 department of public service;

22 (d) public buildings, including those operated by the state university  
23 of New York;

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

LBD11950-01-1

1 (e) hospitals and public health facilities regulated pursuant to arti-  
2 cle twenty-eight of the public health law;

3 (f) facilities created or existing under the public authorities law;  
4 and

5 (g) financial services organizations regulated under the financial  
6 services law.

7 2. Automation and control system shall include personnel, hardware,  
8 software and policies involved in the operation of the critical infras-  
9 tructure that may affect or influence its safe, secure and reliable  
10 operation.

11 3. Automation and control system components shall mean control systems  
12 and any complementary hardware and software components that have been  
13 installed and configured to operate in an automation and control system.  
14 Such systems shall include, but shall not be limited to:

15 (a) control systems, whether physically separate or integrated,  
16 including distributed control systems, programmable logic controllers,  
17 remote terminal units, intelligent electronic devices, supervisory  
18 control and data acquisition, networked electronic sensing and control,  
19 and monitoring and diagnostic systems;

20 (b) associated information systems, such as advanced or multivariable  
21 control, online optimizers, dedicated equipment monitors, graphical  
22 interfaces, process historians, manufacturing execution systems and  
23 plant information management systems;

24 (c) associated internal, human, network, or machine interfaces used to  
25 provide control, safety, and manufacturing operations functionality to  
26 continuous, batch, discrete; and

27 (d) other processes as defined by the international society of auto-  
28 mation including the ISA/IEC 62443 series of standards, as referenced by  
29 the national institute of standards and technology (NIST).

30 4. Asset owner shall mean the public or private owner or entity  
31 accountable and responsible for operation of the critical infrastructure  
32 and for the automation and control system. The asset owner shall be the  
33 operator of the automation and control system and of such equipment  
34 under control.

35 5. Operational technology shall mean the hardware and software that  
36 detects or causes a change in the critical infrastructure through the  
37 direct monitoring or control of physical devices, systems, processes and  
38 events.

39 § 403. Compliance with cybersecurity standards for critical infras-  
40 tructure. The office, in consultation with the department of homeland  
41 security and emergency services and the superintendent of financial  
42 services shall make a determination of critical infrastructure, includ-  
43 ing whose assets, systems, and networks, whether physical or virtual,  
44 are considered vital and vulnerable to cybersecurity attacks.

45 § 404. Procurement, construction, reconstruction, alteration, design  
46 and commissioning of critical infrastructure or automation control  
47 systems or automation control system components. On or after July first,  
48 two thousand twenty-six, the asset owner, when procuring automation and  
49 control system components, as defined in subdivision three of section  
50 four hundred two of this article, services or solutions, or when  
51 contracting for facility upgrades or the construction of critical  
52 infrastructure facilities, shall require such components, services, and  
53 solutions to conform to the ISA/IEC 62443 series of standards as refer-  
54 enced by NIST for defining measures to assure conformance. All contracts  
55 awarded for construction, reconstruction, alteration, design and commis-  
56 sioning of facilities identified as critical infrastructure under this

1 article shall provide that such installed automation and control compo-  
2 ments meet the minimum standards for cybersecurity as defined by the  
3 ISA/IEC 62443 series of standards as referenced by NIST.

4 § 405. Operations and maintenance of critical infrastructure. On or  
5 after July first, two thousand twenty-four, the asset owner shall be  
6 responsible for ensuring that the operation and maintenance of opera-  
7 tional technology, including critical infrastructure, automation control  
8 systems and automation control system components conform with the  
9 ISA/IEC 62443 series of standards as referenced by NIST, including annu-  
10 al risk assessments and shall create a mitigation plan.

11 § 2. This act shall take effect on the one hundred eightieth day after  
12 it shall have become a law. Effective immediately, the office, the  
13 commissioner of homeland security and emergency services and the super-  
14 intendent of financial services may promulgate rules and regulations and  
15 take other actions reasonably necessary to implement this act on that  
16 date.