

# STATE OF NEW YORK

9952--A

## IN ASSEMBLY

April 19, 2022

Introduced by M. of A. OTIS -- read once and referred 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 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:

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

### ARTICLE 4

#### CRITICAL INFRASTRUCTURE STANDARDS AND PROCEDURES ACT

Section 401. Short title.

402. Definitions.

403. Compliance with cybersecurity standards for critical infrastructure.

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

405. Operations and maintenance of critical infrastructure.

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

§ 402. Definitions. The following terms shall have the following meanings:

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

(a) public transportation;

(b) water and wastewater treatment facilities;

(c) public utilities and services subject to the jurisdiction, supervision, powers and duties of the public service commission and the department of public service;

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

(e) hospitals and public health facilities regulated pursuant to article twenty-eight of the public health law; and

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

LBD11950-02-2

1 (f) facilities created or existing under the public authorities law.

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

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

10 (a) control systems, whether physically separate or integrated,  
11 including distributed control systems, programmable logic controllers,  
12 remote terminal units, intelligent electronic devices, supervisory  
13 control and data acquisition, networked electronic sensing and control,  
14 and monitoring and diagnostic systems;

15 (b) associated information systems, such as advanced or multivariable  
16 control, online optimizers, dedicated equipment monitors, graphical  
17 interfaces, process historians, manufacturing execution systems and  
18 plant information management systems;

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

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

25 4. Asset owner shall mean the public or private owner or entity  
26 accountable and responsible for operation of the critical infrastructure  
27 and for the automation and control system. The asset owner shall be the  
28 operator of the automation and control system and of such equipment  
29 under control.

30 5. Operational technology shall mean the hardware and software that  
31 detects or causes a change in the critical infrastructure through the  
32 direct monitoring or control of physical devices, systems, processes and  
33 events.

34 § 403. Compliance with cybersecurity standards for critical infras-  
35 tructure. The office, in consultation with the department of homeland  
36 security and emergency services shall make a determination of critical  
37 infrastructure, including whose assets, systems, and networks, whether  
38 physical or virtual, are considered vital and vulnerable to cybersecuri-  
39 ty attacks.

40 § 404. Procurement, construction, reconstruction, alteration, design  
41 and commissioning of critical infrastructure or automation control  
42 systems or automation control system components. On or after July first,  
43 two thousand twenty-six, the asset owner, when procuring automation and  
44 control system components, as defined in subdivision three of section  
45 four hundred two of this article, services or solutions, or when  
46 contracting for facility upgrades or the construction of critical  
47 infrastructure facilities, shall require such components, services, and  
48 solutions to conform to the ISA/IEC 62443 series of standards. All  
49 contracts awarded for construction, reconstruction, alteration, design  
50 and commissioning of facilities identified as critical infrastructure  
51 under this article shall provide that such installed automation and  
52 control components meet the following minimum standards for cybersecuri-  
53 ty as defined by the ISA/IEC 62443 series of standards:

54 1. 2-4 requirements for IACS solutions providers;

55 2. 3-2 security risk assessment and systems design;

56 3. 3-3 system security requirements and security levels;

1 4. 4-1 product development requirements; and

2 5. 4-2 technical security requirements for IACS components.

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

10 1. 2-1 requirements for an IACS security management system;

11 2. 2-3 patch management in the IACS environment;

12 3. 2-4 security program requirements for service providers;

13 4. 3-2 security risk assessment and system design; and

14 5. 3-3 system security requirements and security levels.

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