STATE OF NEW YORK

_____

3094

2023-2024 Regular Sessions

IN ASSEMBLY

February 2, 2023
_____

Introduced by M. of A. OTIS -- read once and referred to the Committee on Science and Technology

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:
3   **ARTICLE 4**
4   **CRITICAL INFRASTRUCTURE STANDARDS AND PROCEDURES ACT**
5 **Section 401. Short title.**
6   **402. Definitions.**
7   **403. Compliance with cybersecurity standards for critical**
8   **infrastructure.**
9   **404. Procurement, construction, reconstruction, alteration,**
10   **design and commissioning of critical infrastructure or**
11   **automation control systems or automation control system**
12   **components.**
13   **405. Operations and maintenance of critical infrastructure.**
14   **§ 401. Short title. This article shall be known and may be cited as**
15 **the "critical infrastructure standards and procedures (CRISP) act".**
16   **§ 402. Definitions. The following terms shall have the following mean-**
17 **ings:**
18   **1. Critical infrastructure shall include, but shall not be limited to:**
19   **(a) public transportation;**
20   **(b) water and wastewater treatment facilities;**
21   **(c) public utilities and services subject to the jurisdiction, super-**
22 **vision, powers and duties of the public service commission and the**
23 **department of public service;**
24   **(d) public buildings, including those operated by the state university**
25 **of New York;**

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

1   (e) hospitals and public health facilities regulated pursuant to arti-
2   cle twenty-eight of the public health law; and
3   (f) facilities created or existing under the public authorities law.
4   2. Automation and control system shall include personnel, hardware,
5   software and policies involved in the operation of the critical infras-
6   tructure that may affect or influence its safe, secure and reliable
7   operation.
8   3. Automation and control system components shall mean control systems
9   and any complementary hardware and software components that have been
10   installed and configured to operate in an automation and control system.
11   Such systems shall include, but shall not be limited to:
12   (a) control systems, whether physically separate or integrated,
13   including distributed control systems, programmable logic controllers,
14   remote terminal units, intelligent electronic devices, supervisory
15   control and data acquisition, networked electronic sensing and control,
16   and monitoring and diagnostic systems;
17   (b) associated information systems, such as advanced or multivariable
18   control, online optimizers, dedicated equipment monitors, graphical
19   interfaces, process historians, manufacturing execution systems and
20   plant information management systems;
21   (c) associated internal, human, network, or machine interfaces used to
22   provide control, safety, and manufacturing operations functionality to
23   continuous, batch, discrete; and
24   (d) other processes as defined by the international society of auto-
25   mation including the ISA/IEC 62443 series of standards, as referenced by
26   the national institute of standards and technology (NIST).
27   4. Asset owner shall mean the public or private owner or entity
28   accountable and responsible for operation of the critical infrastructure
29   and for the automation and control system. The asset owner shall be the
30   operator of the automation and control system and of such equipment
31   under control.
32   5. Operational technology shall mean the hardware and software that
33   detects or causes a change in the critical infrastructure through the
34   direct monitoring or control of physical devices, systems, processes and
35   events.
36   § 403. Compliance with cybersecurity standards for critical infras-
37   tructure. The office, in consultation with the department of homeland
38   security and emergency services shall make a determination of critical
39   infrastructure, including whose assets, systems, and networks, whether
40   physical or virtual, are considered vital and vulnerable to cybersecuri-
41   ty attacks.
42   § 404. Procurement, construction, reconstruction, alteration, design
43   and commissioning of critical infrastructure or automation control
44   systems or automation control system components. On or after July first,
45   two thousand twenty-seven, the asset owner, when procuring automation
46   and control system components, as defined in subdivision three of
47   section four hundred two of this article, services or solutions, or when
48   contracting for facility upgrades or the construction of critical
49   infrastructure facilities, shall require such components, services, and
50   solutions to conform to the ISA/IEC 62443 series of standards. All
51   contracts awarded for construction, reconstruction, alteration, design
52   and commissioning of facilities identified as critical infrastructure
53   under this article shall provide that such installed automation and
54   control components meet the following minimum standards for cybersecuri-
55   ty as defined by the ISA/IEC 62443 series of standards:
56   1. 2-4 requirements for IACS solutions providers;

 1   **2. 3-2 security risk assessment and systems design;**
 2   **3. 3-3 system security requirements and security levels;**
 3   **4. 4-1 product development requirements; and**
 4   **5. 4-2 technical security requirements for IACS components.**
 5   **§ 405. Operations and maintenance of critical infrastructure. On or**
 6   **after July first, two thousand twenty-five, the asset owner shall be**
 7   **responsible for ensuring that the operation and maintenance of opera-**
 8   **tional technology, including critical infrastructure, automation control**
 9   **systems and automation control system components conform with the**
10   **following ISA/IEC 62443 series of standards, including annual risk**
11   **assessments and shall create a mitigation plan:**
12   **1. 2-1 requirements for an IACS security management system;**
13   **2. 2-3 patch management in the IACS environment;**
14   **3. 2-4 security program requirements for service providers;**
15   **4. 3-2 security risk assessment and system design; and**
16   **5. 3-3 system security requirements and security levels.**
17   § 2. This act shall take effect on the one hundred eightieth day after
18   it shall have become a law. Effective immediately, the office, the
19   commissioner of homeland security and emergency services and the super-
20   intendent of financial services may promulgate rules and regulations and
21   take other actions reasonably necessary to implement this act on that
22   date.