STATE OF NEW YORK

5646

2023-2024 Regular Sessions

IN SENATE

March 10, 2023

Introduced by Sen. THOMAS -- 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 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:

§ 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;

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

LBD01897-02-3

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

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

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

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

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

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

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

(d) other processes as defined by the international society of automation including the ISA/IEC 62443 series of standards, as referenced by the national institute of standards and technology (NIST).

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

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

§ 403. Compliance with cybersecurity standards for critical infrastructure. The office, in consultation with the department of homeland security and emergency services shall make a determination of critical infrastructure, including whose assets, systems, and networks, whether physical or virtual, are considered vital and vulnerable to cybersecurity attacks.

§ 404. Procurement, construction, reconstruction, alteration, design and commissioning of critical infrastructure or automation control systems or automation control system components. On or after July first, two thousand twenty-seven, the asset owner, when procuring automation and control system components, as defined in subdivision three of section four hundred two of this article, services or solutions, or when contracting for facility upgrades or the construction of critical infrastructure facilities, shall require such components, services, and solutions to conform to the ISA/IEC 62443 series of standards. All contracts awarded for construction, reconstruction, alteration, design and commissioning of facilities identified as critical infrastructure under this article shall provide that such installed automation and control components meet the following minimum standards for cybersecurity as defined by the ISA/IEC 62443 series of standards:

1. 2-4 requirements for IACS solutions providers;

2. 3-2 security risk assessment and systems design;
3. 3-3 system security requirements and security levels;
4. 4-1 product development requirements; and
5. 4-2 technical security requirements for IACS components.

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

1. 2-1 requirements for an IACS security management system;
2. 2-3 patch management in the IACS environment;
3. 2-4 security program requirements for service providers;
4. 3-2 security risk assessment and system design; and
5. 3-3 system security requirements and security levels.

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