STATE OF NEW YORK

3448

2017-2018 Regular Sessions

IN ASSEMBLY

January 27, 2017

Introduced by M. of A. DenDEKKER -- read once and referred to the Committee on Governmental Operations

AN ACT to amend the executive law, in relation to a cyber security initiative

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

Section 1. The executive law is amended by adding a new section 719 to read as follows:

§ 719. New York state cyber security initiative. 1. Legislative findings. The legislature finds and declares that repeated cyber intrusions into critical infrastructure, effecting government, private sector business, and citizens of the state of New York, have demonstrated the need for improved cyber security.

The legislature further finds and declares that this cyber threat continues to grow and represents one of the most serious public security challenges that New York must confront. Moreover, the security of the state of New York depends on the reliable functioning of New York state's critical infrastructure, and private sector business interests, as well as the protection of the finances and individual liberties of every citizen, in the face of such threats.

The legislature additionally finds and declares that to enhance the security, protection and resilience of New York state's critical infrastructure, and private sector business interests, as well as the protection of the finances and individual liberties of every citizen, the state of New York must promote a cyber environment that encourages efficiency, innovation, and economic prosperity, and that can operate with safety, security, business confidentiality, privacy, and civil liberty.

The legislature further finds and declares that to create such a safe and secure cyber environment for government, private sector business and individual citizens, New York must advance, in addition to its current

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

LBD02129-01-7

efforts in this field, a New York state cyber security initiative, that establishes a New York state cyber security advisory board; a New York state cyber security partnership program with the owners and operators of critical infrastructure, private sector business, academia, and individual citizens to improve, develop and implement risk-based standards for government, private sector businesses and individual citizens; and a New York state cyber security information sharing program.

2. Critical infrastructure and information systems. As used in this section, the term "critical infrastructure and information systems" shall mean all systems and assets, whether physical or virtual, so vital to the government, private sector businesses and individual citizens of the state of New York that the incapacity or destruction of such systems and assets would have a debilitating impact to the security, economy, or public health of the individual citizens, government, or private sector businesses of the state of New York.

3. New York state cyber security advisory board. (a) There shall be within the division of homeland security and emergency services, a New York state cyber security advisory board, which shall advise the governor and the legislature on developments in cyber security and make recommendations for protecting the state's critical infrastructure and information systems.

(b) The board members shall consist of eleven members appointed by the governor, with three members appointed upon recommendation of the temporary president of the senate, and three members appointed at the recommendation of the speaker of the assembly. All members so appointed shall have expertise in cyber security, telecommunications, internet service delivery, public protection, computer systems and/or computer networks.

(c) The board shall investigate, discuss and make recommendations concerning cyber security issues involving both the public and private sectors and what steps can be taken by New York state to protect critical cyber infrastructure, financial systems, telecommunications networks, electrical grids, security systems, first responder systems and infrastructure, physical infrastructure systems, transportation systems, and such other and further sectors of state government and the private sector as the advisory board shall deem prudent.

(d) The purpose of the advisory board shall be to promote the development of innovative, actionable policies to ensure that New York state is in the forefront of public cyber security defense.

(e) The members of the advisory board shall receive no compensation for their services, but may receive actual and necessary expenses, and shall not be disqualified for holding any other public office or employment by means of their service as a member of the advisory board.

(f) The advisory board shall be entitled to request and receive, and shall be provided with, such facilities, resources and data of any agency, department, division, board, bureau, commission, or public authority of the state, as they may reasonably request, to carry out properly their powers, duties and purpose.

4. New York state cyber security information sharing and analysis program. (a) The division of homeland security and emergency services, in consultation with the division of the state police, the state office of information technology services, and the center for internet security, shall establish, within sixty days of the effective date of this section, a voluntary New York state cyber security information sharing and analysis program.

(b) It shall be the purpose of the New York state cyber security information sharing and analysis program to increase the volume, timeli-

ness, and quality of cyber threat information shared with New York state public and private sector entities so that these entities may better protect and defend themselves against cyber threats and to promote the development of effective defenses and strategies to combat, and protect against, cyber threats and attacks.

(c) To facilitate the purposes of the New York state cyber security information sharing and analysis program, the division of homeland security and emergency services, shall promulgate regulations, in accordance with the provisions of this subdivision.

(d) The regulations shall provide for the timely production of unclassified reports of cyber threats to New York state and its public and private sector entities, including threats that identify a specific targeted entity.

(e) The regulations shall address the need to protect intelligence and law enforcement sources, methods, operations, and investigations, and shall further establish a process that rapidly disseminates the reports produced pursuant to paragraph (d) of this subdivision, to both any targeted entity as well as such other and further public and private entities as the division shall deem necessary to advance the purposes of this subdivision.

(f) The regulations shall provide for protections from liability for entities sharing and receiving information with the New York State cyber security information and analysis program, so long as the entity acted in good faith.

(g) The regulations shall further establish a system for tracking the production, dissemination, and disposition of the reports produced in accordance with the provisions of this subdivision.

(h) The regulations shall also establish an enhanced cyber security services program, within New York state, to provide for procedures, methods and directives, for a voluntary information sharing program, that will provide cyber threat and technical information collected from both public and private sector entities, to such private and public sector entities as the division deems prudent, to advise eligible critical infrastructure companies or commercial service providers that offer security services to critical infrastructure on cyber security threats and defense measures.

(i) The regulations shall also seek to develop strategies to maximize the utility of cyber threat information sharing between and across the private and public sectors, and shall further seek to promote the use of private and public sector subject matter experts to address cyber security needs in New York state, with these subject matter experts providing advice regarding the content, structure, and types of information most useful to critical infrastructure owners and operators in reducing and mitigating cyber risks.

(j) The regulations shall further seek to establish a consultative process to coordinate improvements to the cyber security of critical infrastructure, where as part of the consultative process, the public and private entities of the state of New York shall engage and consider the advice of the division of homeland security and emergency services, the division of the state police, the state office of information technology services, the center for internet security, the New York state cyber security advisory board, the programs established by this subdivision, and such other and further private and public sector entities, universities, and cyber security experts as the division of homeland security and emergency services may deem prudent.

(k) The regulations shall further seek to establish a baseline framework to reduce cyber risk to critical infrastructure, and shall seek to have the division of homeland security and emergency services, in consultation with the division of state police, the state office of information technology services, and the center for internet security, lead the development of a voluntary framework to reduce cyber risks to critical infrastructure, to be known as the cyber security framework, which shall:

(i) include a set of standards, methodologies, procedures, and processes that align policy, business, and technological approaches to address cyber risks;

(ii) incorporate voluntary consensus standards and industry best practices to the fullest extent possible;

(iii) provide a prioritized, flexible, repeatable, performance-based, and cost-effective approach, including information security measures and controls, to help owners and operators of critical infrastructure identify, assess, and manage cyber risk;

(iv) focus on identifying cross-sector security standards and guidelines applicable to critical infrastructure;

(v) identify areas for improvement that should be addressed through future collaboration with particular sectors and standards-developing organizations;

(vi) enable technical innovation and account for organizational differences, to provide guidance that is technology neutral and that enables critical infrastructure sectors to benefit from a competitive market for products and services that meet the standards, methodologies, procedures, and processes developed to address cyber risks;

(vii) include guidance for measuring the performance of an entity in implementing the cyber security framework;

(viii) include methodologies to identify and mitigate impacts of the cyber security framework and associated information security measures or controls on business confidentiality, and to protect individual privacy and civil liberties; and

(ix) engage in the review of threat and vulnerability information and technical expertise.

(l) The regulations shall additionally establish a voluntary critical infrastructure cyber security program to support the adoption of the cyber security framework by owners and operators of critical infrastructure and any other interested entities, where under this program implementation guidance or supplemental materials would be developed to address sector-specific risks and operating environments, and recommend legislation for enactment to address cyber security issues.

(m) In developing the New York state cyber security information sharing and analysis program in accordance with the provisions of this subdivision, the division of homeland security and emergency services, in consultation with the division of state police, the state office of information technology services, and the center for internet security, shall produce and submit a report, to the governor, the temporary president of the senate, and the speaker of the assembly, making recommendations on the feasibility, security benefits, and relative merits of incorporating security standards into acquisition planning and contract administration. Such report shall further address what steps can be taken to harmonize and make consistent existing procurement requirements related to cyber security and the feasibility of including risk-based security standards into procurement and contract administration.

5. New York state cyber security critical infrastructure risk assessment report. (a) The division of homeland security and emergency services, in consultation with the division of state police, the state office of information technology services, and the center for internet security, within one hundred twenty days of the effective date of this section, shall produce a New York state cyber security critical infrastructure risk assessment report.

(b) The production of the New York state cyber security critical infrastructure risk assessment report shall use a risk-based approach to identify critical infrastructure where a cyber security incident could reasonably result in catastrophic regional or state-wide effects on public health or safety, economic distress, and/or threaten public protection of the people and/or property of New York state.

(c) The production of the report shall further use the consultative process and draw upon the expertise of and advice of the division of homeland security and emergency services, the division of state police, the state office of information technology services, the center for internet security, the New York state cyber security advisory board, the programs established by this section, and such other and further private and public sector entities, universities, and cyber security experts as the division of homeland security and emergency services may deem prudent.

(d) The New York state cyber security critical infrastructure risk assessment report shall be delivered to the governor, the temporary president of the senate, the speaker of the assembly, the chair of the senate standing committee on veterans, homeland security and military affairs, and the chair of the assembly standing committee on governmental operations.

(e) Where compliance with this section shall require the disclosure of confidential information, or the disclosure of sensitive information which in the judgment of the commissioner of the division of homeland security and emergency services would jeopardize the cyber security of the state:

(i) such confidential or sensitive information shall be provided to the persons entitled to receive the report, in the form of a supplemental appendix to the report; and

(ii) such supplemental appendix to the report shall not be subject to the provisions of the freedom of information law pursuant to article six of the public officers law; and

(iii) the persons entitled to receive the report may disclose the supplemental appendix to the report to their professional staff, but shall not otherwise publicly disclose such confidential or secure information.

§ 2. This act shall take effect immediately.