

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:

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

3 **S 719. New York state cyber security initiative.** 1. Legislative find-
4 ings. The legislature finds and declares that repeated cyber intrusions
5 into critical infrastructure, effecting government, private sector busi-
6 ness, and citizens of the state of New York, have demonstrated the need
7 for improved cyber security.

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

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

23 The legislature further finds and declares that to create such a safe
24 and secure cyber environment for government, private sector business and
25 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

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

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

16 3. New York state cyber security advisory board. (a) There shall be
17 within the division of homeland security and emergency services, a New
18 York state cyber security advisory board, which shall advise the gover-
19 nor and the legislature on developments in cyber security and make
20 recommendations for protecting the state's critical infrastructure and
21 information systems.

22 (b) The board members shall consist of eleven members appointed by the
23 governor, with three members appointed upon recommendation of the tempo-
24 rary president of the senate, and three members appointed at the recom-
25 mendation of the speaker of the assembly. All members so appointed shall
26 have expertise in cyber security, telecommunications, internet service
27 delivery, public protection, computer systems and/or computer networks.

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

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

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

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

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

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

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

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

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

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

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

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

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

37 (i) The regulations shall also seek to develop strategies to maximize
38 the utility of cyber threat information sharing between and across the
39 private and public sectors, and shall further seek to promote the use of
40 private and public sector subject matter experts to address cyber secu-
41 rity needs in New York state, with these subject matter experts provid-
42 ing advice regarding the content, structure, and types of information
43 most useful to critical infrastructure owners and operators in reducing
44 and mitigating cyber risks.

45 (j) The regulations shall further seek to establish a consultative
46 process to coordinate improvements to the cyber security of critical
47 infrastructure, where as part of the consultative process, the public
48 and private entities of the state of New York shall engage and consider
49 the advice of the division of homeland security and emergency services,
50 the division of the state police, the state office of information tech-
51 nology services, the center for internet security, the New York state
52 cyber security advisory board, the programs established by this subdivi-
53 sion, and such other and further private and public sector entities,
54 universities, and cyber security experts as the division of homeland
55 security and emergency services may deem prudent.

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

9 (i) include a set of standards, methodologies, procedures, and proc-
10 esses that align policy, business, and technological approaches to
11 address cyber risks;

12 (ii) incorporate voluntary consensus standards and industry best prac-
13 tices to the fullest extent possible;

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

18 (iv) focus on identifying cross-sector security standards and guide-
19 lines applicable to critical infrastructure;

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

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

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

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

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

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

43 (m) In developing the New York state cyber security information shar-
44 ing and analysis program in accordance with the provisions of this
45 subdivision, the division of homeland security and emergency services,
46 in consultation with the division of state police, the state office of
47 information technology services, and the center for internet security,
48 shall produce and submit a report, to the governor, the temporary presi-
49 dent of the senate, and the speaker of the assembly, making recommenda-
50 tions on the feasibility, security benefits, and relative merits of
51 incorporating security standards into acquisition planning and contract
52 administration. Such report shall further address what steps can be
53 taken to harmonize and make consistent existing procurement requirements
54 related to cyber security and the feasibility of including risk-based
55 security standards into procurement and contract administration.

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

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

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

23 (d) The New York state cyber security critical infrastructure risk
24 assessment report shall be delivered to the governor, the temporary
25 president of the senate, the speaker of the assembly, the chair of the
26 senate standing committee on veterans, homeland security and military
27 affairs, and the chair of the assembly standing committee on govern-
28 mental operations.

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

34 (i) such confidential or sensitive information shall be provided to
35 the persons entitled to receive the report, in the form of a supple-
36 mental appendix to the report; and

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

40 (iii) the persons entitled to receive the report may disclose the
41 supplemental appendix to the report to their professional staff, but
42 shall not otherwise publicly disclose such confidential or secure infor-
43 mation.

44 § 2. This act shall take effect immediately.