

# STATE OF NEW YORK

924

2017-2018 Regular Sessions

## IN SENATE

January 5, 2017

Introduced by Sens. CROCI, AKSHAR, AVELLA, DeFRANCISCO, FUNKE, GOLDEN --  
read twice and ordered printed, and when printed to be committed to  
the Committee on Veterans, Homeland Security and Military Affairs

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 Assem-  
bly, do enact as follows:

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

3 § 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

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

LBD02129-01-7

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

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

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

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

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

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

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

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

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

1 (b) It shall be the purpose of the New York state cyber security  
2 information sharing and analysis program to increase the volume, timeli-  
3 ness, and quality of cyber threat information shared with New York state  
4 public and private sector entities so that these entities may better  
5 protect and defend themselves against cyber threats and to promote the  
6 development of effective defenses and strategies to combat, and protect  
7 against, cyber threats and attacks.

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

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

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

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

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

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

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

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

1 universities, and cyber security experts as the division of homeland  
2 security and emergency services may deem prudent.

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

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

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

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

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

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

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

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

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

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

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

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

1 related to cyber security and the feasibility of including risk-based  
2 security standards into procurement and contract administration.

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

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

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

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

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

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

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

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

46 § 2. This act shall take effect immediately.