

# STATE OF NEW YORK

5946--A

2017-2018 Regular Sessions

## IN SENATE

May 8, 2017

Introduced by Sen. CROCI -- read twice and ordered printed, and when printed to be committed to the Committee on Veterans, Homeland Security and Military Affairs -- recommitted to the Committee on Veterans, Homeland Security and Military Affairs in accordance with Senate Rule 6, sec. 8 -- committee discharged, bill amended, ordered reprinted as amended and recommitted to said committee

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

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  
2 to read as follows:

3 § 719. Cyber security. 1. Cyber security action plan. The commissioner,  
4 in consultation with the chief information officer of the office of  
5 information technology, the superintendent of state police, the commis-  
6 sioner of general services, the superintendent of financial services,  
7 the office of the state comptroller, and such other experts from the  
8 public, private and not-for-profit sectors who maintain experience and  
9 knowledge in the area of cyber security as the commissioner deems  
10 prudent, shall develop a cyber security action plan for New York state.  
11 The plan shall make recommendations to the governor and the legislature  
12 regarding the establishment of a new state office of cyber security,  
13 under the command and control of the commissioner and within the divi-  
14 sion, including identifying such bureaus, responsibilities and duties  
15 that should be contained and performed within such office, the budget  
16 and personnel necessary to establish such office, and the site locations  
17 at which such office should be situated. The purpose of the plan shall  
18 be to develop a comprehensive and effective strategy to provide meaning-  
19 ful cyber security for the state of New York, its state agencies, its  
20 public authorities, its assets, its infrastructure, its local govern-

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

LBD11004-02-8

1 ments, and its private sector businesses, not-for-profit corporations  
2 and individuals.

3 2. Cyber security defense unit. The cyber security action plan estab-  
4 lished pursuant to subdivision one of this section shall further make  
5 recommendations to the governor and the legislature on the establish-  
6 ment, within the office of cyber security, of a cyber security defense  
7 unit. The cyber security action plan shall detail how the cyber security  
8 defense unit, would consist of such persons as the commissioner deems  
9 necessary to perform its mission. The cyber security action plan shall  
10 further detail the mission of the cyber security defense unit, with such  
11 mission being to help prevent, respond to, and recover from cyber  
12 attacks targeted against the state, its assets, and its infrastructure,  
13 together with such other and further duties and responsibilities as the  
14 cyber security action plan may additionally prescribe. The cyber secu-  
15 rity action plan shall further detail that the personnel of the cyber  
16 security defense unit must be expert in computer and programming tech-  
17 nology so as to prevent and respond to unauthorized invasion, hacking  
18 and attacks against computer networks, systems, databases, and informa-  
19 tion storage. The cyber security action plan shall further detail how  
20 the personnel of the cyber security defense unit must have background  
21 and experience in computer, system and network operations and vulner-  
22 abilities, programming code, data recovery and cyber security. The  
23 cyber security action plan shall also provide that, in addition to any  
24 other tasks the commissioner may wish to assign the cyber security  
25 defense unit, that such cyber security defense unit shall also be  
26 assigned the mission of using and developing software, hardware, and  
27 protocols to prevent such unauthorized invasions, hacking and attacks,  
28 and to develop response activities, procedures, and protocols to address  
29 any such invasion, hacking or attack on any state computer network,  
30 system, database, and/or information storage. The cyber security action  
31 plan shall further detail how the cyber security defense unit should  
32 interact and deploy the use of other cyber experts, educators, law  
33 enforcement, intelligence experts, and other public and private sector  
34 entities to assist it in the performance of its mission.

35 3. Cyber incident response teams. The cyber security action plan  
36 established pursuant to subdivision one of this section shall further  
37 make recommendations to the governor and the legislature on the estab-  
38 lishment, within the office of cyber security, of a group of cyber inci-  
39 dent response teams. The cyber security action plan shall detail how the  
40 cyber incident response teams would consist of such persons as the  
41 commissioner deems necessary to perform its mission. The cyber security  
42 action plan shall further detail the mission of the cyber incident  
43 response teams, with such mission being to help prevent, respond to, and  
44 recover from, cyber attacks targeted against state entities, public  
45 authorities, local governments, and/or private sector businesses, not-  
46 for-profit corporations and individuals, together with such other and  
47 further duties and responsibilities as the cyber security action plan  
48 may additionally prescribe. The cyber security action plan shall  
49 further detail that the personnel of the cyber incident response teams  
50 must be expert in computer and programming technology so as to prevent  
51 and respond to an unauthorized invasion, hacking and attacks against  
52 computer networks, systems, databases, and information storage. The  
53 cyber security action plan shall additionally detail how the personnel  
54 of the cyber incident response teams must have background and experience  
55 in computer, system and network operations and vulnerabilities, program-  
56 ming code, data recovery and cyber security. The cyber security action

1 plan shall also provide, in addition to any other tasks the commissioner  
2 may wish to assign the cyber incident response teams, that such cyber  
3 incident response teams shall also be assigned the mission of using and  
4 developing software, hardware, and protocols to prevent such unauthor-  
5 ized invasions, hacking and attacks, and to develop response activities,  
6 procedures, and protocols to address any such invasion, hacking or  
7 attack on any state computer network, system, database, and/or informa-  
8 tion storage. The cyber security action plan shall also provide that it  
9 would further be the mission of each cyber incident response team to  
10 respond to, and help the targeted entity to recover from, cyber inva-  
11 sion, hacking and attacks. The cyber security action plan shall also  
12 provide that within resources available, the commissioner may deploy a  
13 cyber incident response team to a state entity, public authority, local  
14 government, private sector business, or not-for-profit corporation that  
15 has experienced a cyber attack, to promote and assist in such entity's  
16 response and recovery efforts. The cyber security action plan shall  
17 further detail how the cyber incident response team should interact and  
18 deploy the use of other cyber experts, educators, law enforcement,  
19 intelligence experts, and other public and private sector entities to  
20 assist them in the performance of their mission.

21 4. Cyber education and attack prevention. The cyber security action  
22 plan established pursuant to subdivision one of this section shall  
23 further make recommendations to the governor and the legislature on the  
24 establishment, within the office of cyber security, of a cyber education  
25 and attack prevention unit to assist state agencies, public authorities,  
26 local governments, and/or private sector businesses, not-for-profit  
27 corporations and individuals. The cyber security action plan shall  
28 detail how the cyber education and attack prevention unit would consist  
29 of such persons as the commissioner deems necessary to perform its  
30 mission. The cyber security action plan shall further detail the mission  
31 of the cyber education and attack prevention unit, with such mission  
32 being to help educate state agencies, public authorities, local govern-  
33 ments, and/or private sector businesses, not-for-profit corporations and  
34 individuals on how to prevent and respond to a cyber attack, together  
35 with such other and further duties and responsibilities as the cyber  
36 security action plan may additionally prescribe. The cyber security  
37 action plan shall further detail that the commissioner may deploy within  
38 resources available the cyber education and attack prevention unit to  
39 state agencies, public authorities, local governments, private sector  
40 businesses, and/or not-for-profit corporations, to educate and/or  
41 instruct such entities, hold informational programs, and/or provide  
42 instructional or informational materials. The cyber security action plan  
43 shall further detail how the cyber education and attack prevention unit  
44 should interact and deploy the use of other cyber experts, educators,  
45 law enforcement, intelligence experts, and other public and private  
46 sector entities to assist it in the performance of its mission.

47 5. Reporting of cyber entities. The cyber security action plan estab-  
48 lished pursuant to subdivision one of this section shall further make  
49 recommendations on the reporting of the new state office of cyber secu-  
50 rity. The cyber security action plan shall further require that such  
51 reporting should contain a requirement that on or before December first,  
52 two thousand nineteen, and then every year thereafter, that the commis-  
53 sioner shall submit a report to the governor, the speaker of the assem-  
54 bly, the temporary president of the senate, the chair of the senate  
55 standing committee on veterans, homeland security and military affairs,  
56 and the chair of the assembly standing committee on governmental oper-

1 ations, which provides a comprehensive review detailing all the activ-  
2 ities and operations of the office of cyber security, the cyber security  
3 defense unit, the cyber incident response teams and the cyber education  
4 and attack prevention unit, during the past year. The cyber security  
5 action plan shall further provide that where compliance with such a  
6 report would require the disclosure of confidential information, or the  
7 disclosure of sensitive information which in the judgement of the  
8 commissioner would jeopardize the cyber security of the state, then such  
9 confidential or sensitive information shall be provided to the persons  
10 entitled to receive the report, in the form of a supplemental appendix  
11 to the report, and that such supplemental appendix to the report, shall  
12 not be subject to the provisions of the freedom of information law  
13 pursuant to article six of the public officers law, and although the  
14 persons entitled to receive the report may disclose the supplemental  
15 appendix to the report to their professional staff, they shall not  
16 otherwise publicly disclose such confidential or secure information. The  
17 cyber security action plan shall further provide that, except with the  
18 respect to any confidential or sensitive information contained in the  
19 supplemental appendix to the report, the commissioner shall direct that  
20 a copy of the report shall be posted on the division's website, not more  
21 than fifteen days after such report is delivered to the persons entitled  
22 to receive such report. The cyber security action plan should further  
23 provide that the division may further post any and all additional infor-  
24 mation it may deem appropriate, on its website, regarding cyber securi-  
25 ty, and the protection of public and private computer systems, networks,  
26 hardware and software.

27 6. Reimbursement for cost of service. The cyber security action plan  
28 established pursuant to subdivision one of this section shall further  
29 make recommendations with respect to the division charging non-govern-  
30 mental entities for the reasonable cost of the services provided by the  
31 cyber security incident response teams and the cyber education and  
32 attack prevention unit. The cyber security action plan shall further  
33 detail how the proceeds from the charging for such costs shall be depos-  
34 ited with the state comptroller into a cyber security support services  
35 account, of which the comptroller would have custody. The cyber security  
36 action plan shall additionally detail how the comptroller may disburse  
37 monies held in such cyber security account for the purposes of providing  
38 supplemental funds for the operation of the new state office of cyber  
39 security.

40 7. Timing of cyber security action plan. The commissioner, on or  
41 before December first, two thousand eighteen, shall deliver a copy of  
42 the cyber security action plan required to be produced by this section,  
43 to the the governor, the speaker of the assembly, the temporary presi-  
44 dent of the senate, the chair of the senate standing committee on veter-  
45 ans, homeland security and military affairs, and the chair of the assem-  
46 bly standing committee on governmental operations.

47 § 2. This act shall take effect immediately.