

# STATE OF NEW YORK

5946

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

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 commission-  
4 er, 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-  
21 ments, and its private sector businesses, not-for-profit corporations  
22 and individuals.

23 2. Cyber security defense unit. The cyber security action plan estab-  
24 lished pursuant to subdivision one of this section shall further make

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

LBD11004-01-7

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

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

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

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

43 5. Reporting of cyber entities. The cyber security action plan estab-  
44 lished pursuant to subdivision one of this section shall further make  
45 recommendations on the reporting of the new state office of cyber secu-  
46 rity. The cyber security action plan shall further require that such  
47 reporting should contain a requirement that on or before December first,  
48 two thousand eighteen, and then every year thereafter, that the commis-  
49 sioner shall submit a report to the governor, the speaker of the assem-  
50 bly, the temporary president of the senate, the chair of the senate  
51 standing committee on veterans, homeland security and military affairs,  
52 and the chair of the assembly standing committee on governmental oper-  
53 ations, which provides a comprehensive review detailing all the activ-  
54 ities and operations of the office of cyber security, the cyber security  
55 defense unit, the cyber incident response teams and the cyber education  
56 and attack prevention unit, during the past year. The cyber security

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

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

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

43 § 2. This act shall take effect immediately.