

STATE OF NEW YORK

8501

2017-2018 Regular Sessions

IN ASSEMBLY

June 16, 2017

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

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
25 recommendations to the governor and the legislature on the establish-

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

LBD11004-01-7

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

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

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

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

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

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

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

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

42 § 2. This act shall take effect immediately.