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:

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

§ 719. Cyber security. 1. Cyber security action plan. The commissioner, in consultation with the chief information officer of the office of information technology, the superintendent of state police, the commissioner of general services, the superintendent of financial services, the office of the state comptroller, and such other experts from the public, private and not-for-profit sectors who maintain experience and knowledge in the area of cyber security as the commissioner deems prudent, shall develop a cyber security action plan for New York state. The plan shall make recommendations to the governor and the legislature regarding the establishment of a new state office of cyber security, under the command and control of the commissioner and within the division, including identifying such bureaus, responsibilities and duties that should be contained and performed within such office, the budget and personnel necessary to establish such office, and the site locations at which such office should be situated. The purpose of the plan shall be to develop a comprehensive and effective strategy to provide meaningful cyber security for the state of New York, its state agencies, its public authorities, its assets, its infrastructure, its local governments, and its private sector businesses, not-for-profit corporations and individuals.

2. Cyber security defense unit. The cyber security action plan established pursuant to subdivision one of this section shall further make 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

ment, within the office of cyber security, of a cyber security defense unit. The cyber security action plan shall detail how the cyber security defense unit, would consist of such persons as the commissioner deems necessary to perform its mission. The cyber security action plan shall further detail the mission of the cyber security defense unit, with such mission being to help prevent, respond to, and recover from cyber attacks targeted against the state, its assets, and its infrastructure, together with such other and further duties and responsibilities as the cyber security action plan may additionally prescribe. The cyber security action plan shall further detail that the personnel of the cyber security defense unit must be expert in computer and programming technology so as to prevent and respond to unauthorized invasion, hacking and attacks against computer networks, systems, databases, and information storage. The cyber security action plan shall further detail how the personnel of the cyber security defense unit must have background and experience in computer, system and network operations and vulnerabilities, programming code, data recovery and cyber security. The cyber security action plan shall also provide that, in addition to any other tasks the commissioner may wish to assign the cyber security defense unit, that such cyber security defense unit shall also be assigned the mission of using and developing software, hardware, and protocols to prevent such unauthorized invasions, hacking and attacks, and to develop response activities, procedures, and protocols to address any such invasion, hacking or attack on any state computer network, system, database, and/or information storage. The cyber security action plan shall further detail how the cyber security defense unit should interact and deploy the use of other cyber experts, educators, law enforcement, intelligence experts, and other public and private sector entities to assist it in the performance of its mission.

3. Cyber incident response teams. The cyber security action plan established pursuant to subdivision one of this section shall further make recommendations to the governor and the legislature on the establishment, within the office of cyber security, of a group of cyber incident response teams. The cyber security action plan shall detail how the cyber incident response teams would consist of such persons as the commissioner deems necessary to perform its mission. The cyber security action plan shall further detail the mission of the cyber incident response teams, with such mission being to help prevent, respond to, and recover from, cyber attacks targeted against state entities, public authorities, local governments, and/or private sector businesses, not-for-profit corporations and individuals, together with such other and further duties and responsibilities as the cyber security action plan may additionally prescribe. The cyber security action plan shall further detail that the personnel of the cyber incident response teams must be expert in computer and programming technology so as to prevent and respond to an unauthorized invasion, hacking and attacks against computer networks, systems, databases, and information storage. The cyber security action plan shall additionally detail how the personnel of the cyber incident response teams must have background and experience in computer, system and network operations and vulnerabilities, programming code, data recovery and cyber security. The cyber security action plan shall also provide, in addition to any other tasks the commissioner may wish to assign the cyber incident response teams, that such cyber incident response teams shall also be assigned the mission of using and developing software, hardware, and protocols to prevent such unauthorized invasions, hacking and attacks, and to develop response activities,

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

4. Cyber education and attack prevention. The cyber security action plan established pursuant to subdivision one of this section shall further make recommendations to the governor and the legislature on the establishment, within the office of cyber security, of a cyber education and attack prevention unit to assist state agencies, public authorities, local governments, and/or private sector businesses, not-for-profit corporations and individuals. The cyber security action plan shall detail how the cyber education and attack prevention unit would consist of such persons as the commissioner deems necessary to perform its mission. The cyber security action plan shall further detail the mission of the cyber education and attack prevention unit, with such mission being to help educate state agencies, public authorities, local governments, and/or private sector businesses, not-for-profit corporations and individuals on how to prevent and respond to a cyber attack, together with such other and further duties and responsibilities as the cyber security action plan may additionally prescribe. The cyber security action plan shall further detail that the commissioner may deploy within resources available the cyber education and attack prevention unit to state agencies, public authorities, local governments, private sector businesses, and/or not-for-profit corporations, to educate and/or instruct such entities, hold informational programs, and/or provide instructional or informational materials. The cyber security action plan shall further detail how the cyber education and attack prevention unit should interact and deploy the use of other cyber experts, educators, law enforcement, intelligence experts, and other public and private sector entities to assist it in the performance of its mission.

5. Reporting of cyber entities. The cyber security action plan established pursuant to subdivision one of this section shall further make recommendations on the reporting of the new state office of cyber security. The cyber security action plan shall further require that such reporting should contain a requirement that on or before December first, two thousand eighteen, and then every year thereafter, that the commissioner shall submit a report to the governor, the speaker of the assembly, the temporary president of the senate, the chair of the senate standing committee on veterans, homeland security and military affairs, and the chair of the assembly standing committee on governmental operations, which provides a comprehensive review detailing all the activities and operations of the office of cyber security, the cyber security defense unit, the cyber incident response teams and the cyber education and attack prevention unit, during the past year. The cyber security action plan shall further provide that where compliance with such a

report would require the disclosure of confidential information, or the disclosure of sensitive information which in the judgement of the commissioner would jeopardize the cyber security of the state, then such confidential or sensitive information shall be provided to the persons entitled to receive the report, in the form of a supplemental appendix to the report, and that such supplemental appendix to the report, shall not be subject to the provisions of the freedom of information law pursuant to article six of the public officers law, and although the persons entitled to receive the report may disclose the supplemental appendix to the report to their professional staff, they shall not otherwise publicly disclose such confidential or secure information. The cyber security action plan shall further provide that, except with the respect to any confidential or sensitive information contained in the supplemental appendix to the report, the commissioner shall direct that a copy of the report shall be posted on the division's website, not more than fifteen days after such report is delivered to the persons entitled to receive such report. The cyber security action plan should further provide that the division may further post any and all additional information it may deem appropriate, on its website, regarding cyber security, and the protection of public and private computer systems, networks, hardware and software.

6. Reimbursement for cost of service. The cyber security action plan established pursuant to subdivision one of this section shall further make recommendations with respect to the division charging non-governmental entities for the reasonable cost of the services provided by the cyber security incident response teams and the cyber education and attack prevention unit. The cyber security action plan shall further detail how the proceeds from the charging for such costs shall be deposited with the state comptroller into a cyber security support services account, of which the comptroller would have custody. The cyber security action plan shall additionally detail how the comptroller may disburse monies held in such cyber security account for the purposes of providing supplemental funds for the operation of the new state office of cyber security.

7. Timing of cyber security action plan. The commissioner, on or before December first, two thousand seventeen, shall deliver a copy of the cyber security action plan required to be produced by this section, to the the governor, the speaker of the assembly, the temporary president of the senate, the chair of the senate standing committee on veterans, homeland security and military affairs, and the chair of the assembly standing committee on governmental operations.

§ 2. This act shall take effect immediately.