Sen. Iris Y. Martinez

Filed: 5/4/2017

AMENDMENT TO HOUSE BILL 3737

AMENDMENT NO. _____. Amend House Bill 3737 by replacing everything after the enacting clause with the following:

"Section 1. Short title. This Act may be cited as the Illinois Information Security Improvement Act.

Section 5. Definitions. As used in this Act:

"Critical information system" means any information system (including any telecommunications system) used or operated by a State agency or by a contractor of a State agency or other organization or entity on behalf of a State agency: that contains health insurance information, medical information, or personal information as defined in the Personal Information Protection Act; where the unauthorized disclosure, modification, destruction of information in the information system could be expected to have a serious, severe, or catastrophic adverse effect on State agency operations,

assets, or individuals; or where the disruption of access to or use of the information or information system could be expected to have a serious, severe, or catastrophic adverse effect on State operations, assets, or individuals.

"Department" means the Department of Innovation and Technology.

"Information security" means protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide: integrity, which means guarding against improper information modification or destruction, and includes ensuring information nonrepudiation and authenticity; confidentiality, which means preserving authorized restrictions on access and disclosure, including means for protecting personal privacy and proprietary information; and availability, which means ensuring timely and reliable access to and use of information.

"Incident" means an occurrence that: actually or imminently jeopardizes, without lawful authority, the confidentiality, integrity, or availability of information or an information system; or constitutes a violation or imminent threat of violation of law, security policies, security procedures, or acceptable use policies or standard security practices.

"Information system" means a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of

information created or maintained by or for the State of Illinois.

"Office" means the Office of the Statewide Chief Information Security Officer.

"Secretary" means the Secretary of Innovation and Technology.

"Security controls" means the management, operational, and technical controls (including safeguards and countermeasures) for an information system that protect the confidentiality, integrity, and availability of the system and its information.

"State agency" means any agency under the jurisdiction of the Governor.

Section 10. Purpose. The purposes of this Act are to:

(1) provide a comprehensive framework for ensuring the effectiveness of information security controls over information resources that support State agency operations and assets;

(2) recognize the critical role of information and information systems in the provision of life, health, safety, and other crucial services to the citizens of the State of Illinois and the risk posed to these services due to the ever-evolving cybersecurity threat;

(3) recognize the highly networked nature of the current State of Illinois working environment and provide effective statewide management and oversight of the

related information security risks, including coordination of information security efforts across State agencies;

(4) provide for the development and maintenance of minimum security controls required to protect State of Illinois information and information systems;

(5) provide a mechanism for improved oversight of State agency information security programs, including through automated security tools to continuously diagnose and improve security;

(6) recognize that information security risk is both a business and public safety issue, and the acceptance of risk is a decision to be made at the executive levels of State government; and

(7) ensure a continued and deliberate effort to reduce the risk posed to the State by cyberattacks and other information security incidents that could impact the information security of the State.

Section 15. Office of the Statewide Chief Information Security Officer.

(a) The Office of the Statewide Chief Information Security Officer is established within the Department of Innovation and Technology. The Office is directly subordinate to the Secretary of Innovation and Technology.

(b) The Office shall:

(1) serve as the strategic planning, facilitation, and

coordination office for information technology security in this State and as the lead and central coordinating entity to guide and oversee the information security functions of State agencies;

(2) provide information security services to support the secure delivery of State agency services that utilize information systems and to assist State agencies with fulfilling their responsibilities under this Act;

(3) conduct information and cybersecurity strategic, operational, and resource planning and facilitating an effective enterprise information security architecture capable of protecting the State;

(4) identify information security risks in each State agency and recommend risk mitigation strategies, methods, and procedures to reduce these risks;

(5) manage the response to information security and information security incidents involving State of Illinois information systems and ensure the completeness of information system security plans for critical information systems;

(6) conduct pre-deployment information security assessments for critical information systems and submit findings and recommendations to the Secretary and State agency heads;

(7) develop and conduct targeted operational evaluations, including threat and vulnerability

assessments on information systems;

(8) monitor and report compliance of each State agency with State information security policies, standards, and procedures;

(9) coordinate statewide information security awareness and training programs; and

(10) develop and execute other strategies as necessary to protect this State's information technology infrastructure and the data stored on or transmitted by such infrastructure.

(c) The Office may temporarily suspend operation of an information system or information technology infrastructure that is owned, leased, outsourced, or shared by one or more State agencies in order to isolate the source of, or stop the spread of, an information security breach or other similar information security incident. State agencies shall comply with directives to temporarily discontinue or suspend operations of information systems or information technology infrastructure.

Section 20. Statewide Chief Information Security Officer. The position of Statewide Chief Information Security Officer is established within the Office. The Secretary shall appoint a Statewide Chief Information Security Officer who shall serve at the pleasure of the Secretary. The Statewide Chief Information Security Officer shall report to and be under the supervision

of the Secretary. The Statewide Chief Information Security Officer shall exhibit a background and experience in information security, information technology, or risk management, or exhibit other appropriate expertise required to fulfill the duties of the Statewide Chief Information Security Officer. If the Statewide Chief Information Security Officer is unable or unavailable to perform the duties and responsibilities under Section 25, all powers and authority granted to the Statewide Chief Information Security Officer may be exercised by the Secretary or his or her designee.

Section 25. Responsibilities.

(a) The Secretary shall:

(1) appoint a Statewide Chief Information Security Officer pursuant to Section 20;

(2) provide the Office with the staffing and resources deemed necessary by the Secretary to fulfill the responsibilities of the Office;

(3) oversee statewide information security policies and practices, including:

(A) directing and overseeing the development, implementation, and communication of statewide information security policies, standards, and guidelines;

(B) overseeing the education of State agency personnel regarding the requirement to identify and

provide information security protections commensurate with the risk and magnitude of the harm resulting from the unauthorized access, use, disclosure, disruption, modification, or destruction of information in a critical information system;

(C) overseeing the development and implementation of a statewide information security risk management program;

(D) overseeing State agency compliance with the requirements of this Section;

(E) coordinating Information Security policies and practices with related information and personnel resources management policies and procedures; and

(F) providing an effective and efficient process to assist State agencies with complying with the requirements of this Act.

(b) The Statewide Chief Information Security Officer shall:

(1) serve as the head of the Office and ensure the execution of the responsibilities of the Office as set forth in subsection (c) of Section 15, the Statewide Chief Information Security Officer shall also oversee State agency personnel with significant responsibilities for information security and ensure a competent workforce that keeps pace with the changing information security environment;

(2) develop and recommend information security policies, standards, procedures, and guidelines to the Secretary for statewide adoption and monitor compliance with these policies, standards, guidelines, and procedures through periodic testing;

(3) develop and maintain risk-based, cost-effective information security programs and control techniques to address all applicable security and compliance requirements throughout the life cycle of State agency information systems;

(4) establish the procedures, processes, and technologies to rapidly and effectively identify threats, risks, and vulnerabilities to State information systems, and ensure the prioritization of the remediation of vulnerabilities that pose risk to the State;

(5) develop and implement capabilities and procedures for detecting, reporting, and responding to information security incidents;

(6) establish and direct a statewide information security risk management program to identify information security risks in State agencies and deploy risk mitigation strategies, processes, and procedures;

(7) establish the State's capability to sufficiently protect the security of data through effective information system security planning, secure system development, acquisition, and deployment, the application of protective

technologies and information system certification, accreditation, and assessments;

(8) ensure that State agency personnel, including contractors, are appropriately screened and receive information security awareness training;

(9) convene meetings with agency heads and other State officials to help ensure:

(A) the ongoing communication of risk and risk reduction strategies,

(B) effective implementation of information security policies and practices, and

(C) the incorporation of and compliance with information security policies, standards, and guidelines into the policies and procedures of the agencies;

(10) provide operational and technical assistance to State agencies in implementing policies, principles, standards, and guidelines on information security, including implementation of standards promulgated under subparagraph (A) of paragraph (3) of subsection (a) of this Section, and provide assistance and effective and efficient means for State agencies to comply with the State agency requirements under this Act;

(11) in coordination and consultation with the Secretary and the Governor's Office of Management and Budget, review State agency budget requests related to

Information Security systems and provide recommendations to the Governor's Office of Management and Budget;

(12) ensure the preparation and maintenance of plans and procedures to provide cyber resilience and continuity of operations for critical information systems that support the operations of the State; and

(13) take such other actions as the Secretary may direct.

Section 99. Effective date. This Act takes effect January 1, 2018, but this Act does not take effect at all unless Senate Bill 1606 of the 100th General Assembly becomes law.".