SENATE BILL No. 717

August 5, 2009, Introduced by Senator GARCIA and referred to the Committee on Homeland Security and Emerging Technologies.

A bill to create the information security program standards act; to provide for standards for safeguarding personal information; and to provide for certain civil immunity.

THE PEOPLE OF THE STATE OF MICHIGAN ENACT:

Sec. 1. This act shall be known and may be cited as the "information security program standards act".

Sec. 3. As used in this act:

(a) "Breach of security" or "security breach" means the unauthorized access or acquisition of data or electronic data that compromises the security, availability, confidentiality, or integrity of personal information maintained by a person. Breach of security or security breach does not include unauthorized access to data or electronic data by an employee or other individual if the access meets all of the following criteria:

SENATE BILL No. 717

(*i*) The employee or other individual acted in good faith in accessing the data.

(*ii*) The access was related to the activities of the person.

(*iii*) The employee or other individual did not misuse any personal information or disclose any personal information to an unauthorized person.

(b) "Electronic" means relating to technology having electrical, digital, magnetic, wireless, optical, electromagnetic, or similar capabilities.

(c) "Encrypted" means transformation of data through the use of an algorithmic process, or an alternative method at least as secure, into a form in which there is a low probability of assigning meaning without use of a confidential process or key, or securing information by another method that renders the data elements unreadable or unusable.

(d) "Person" means an individual, partnership, corporation, limited liability company, association, or other legal entity.

(e) "Personal information", other than information lawfully obtained from publicly available information, or from federal, state, or local government records lawfully made available to the public, means the first name or first initial and last name linked to 1 or more of the following data elements of a resident of this state:

(*i*) Social security number.

(*ii*) Driver license number or state personal identification card number.

(*iii*) Demand deposit or other financial account number, or

credit card or debit card number, in combination with or without any required security code, access code, or password that would permit access to any financial accounts.

(f) "Record" or "records" means any material upon which written, drawn, spoken, visual, or electromagnetic information or images are recorded or preserved, regardless of physical form or characteristics.

Sec. 5. (1) A person that owns, licenses, stores, or maintains personal information about a resident of this state has the civil immunity provided under section 13 if the person develops, implements, maintains, and monitors a comprehensive written information security program as provided in this act. A comprehensive written information security program shall be consistent with industry best practices, such as ISO 27000 or the most current industry standard, and shall contain administrative, technical, and physical safeguards to ensure the security and confidentiality of those records. The safeguards contained in a comprehensive written information security program must be consistent with the requirements of any other regulations of this state or any federal regulations applicable to the person that owns, licenses, stores, or maintains personal information.

(2) Without limiting the generality of subsection (1), every comprehensive information security program shall include, but not be limited to:

(a) Designating 1 or more employees to maintain the comprehensive information security program.

(b) Identifying and assessing foreseeable internal and

external risks to the security, confidentiality, or integrity of any electronic, paper, or other records containing personal information, and evaluating and improving, where necessary, the effectiveness of the current safeguards for limiting those risks, including, but not limited to:

(*i*) Ongoing employee training, including temporary and contract employees.

(*ii*) Employee compliance with policies and procedures.

(*iii*) Means for detecting and preventing security system failures.

(c) Developing security policies for employees that take into account whether and how employees should be allowed to keep, access, and transport records containing personal information outside of business premises.

(d) Imposing disciplinary measures for violations of the comprehensive information security program rules.

(e) Preventing terminated employees from accessing records containing personal information by immediately terminating their physical and electronic access to those records, including deactivating their passwords and user names.

(f) Taking steps to verify that third-party service providers with access to personal information have the capacity to protect that personal information, including selecting and retaining service providers that are capable of maintaining safeguards for personal information and contractually requiring service providers to maintain those safeguards. Before permitting third-party service providers with access to personal information, the person

permitting the access shall obtain from the third-party service provider a contractual or statutory obligation that the service provider has a written, comprehensive information security program that complies with the requirements of this act.

(g) Limiting the amount of personal information collected to that necessary to accomplish the legitimate purpose for which it is collected; limiting the time during which the personal information is retained to that necessary to accomplish that purpose; and limiting access to those persons who are required to know the information in order to accomplish that purpose or to comply with state or federal record retention requirements.

(h) Identifying paper, electronic, and other records, computing systems, and storage media, including laptops, portable devices, and electronic media storage used to store personal information, to determine which records contain personal information, except where the comprehensive information security program provides for the handling of all records as if they all contained personal information.

(i) Restrictions upon physical access to records containing personal information, including a written procedure that sets forth the manner in which physical access to those records is restricted; and storage of the records and data in locked facilities, storage areas, or containers.

(j) Regular monitoring to ensure that the comprehensive information security program is operating in a manner calculated to prevent unauthorized access to or unauthorized use of personal information, and upgrading information safeguards as necessary to

limit risks.

(k) Reviewing the scope of the security measures at least annually or whenever there is a material change in business practices that may implicate the security or integrity of records containing personal information.

(*l*) Documenting responsive actions taken in connection with any incident involving a breach of security, and mandatory post-incident review of events and actions taken, if any, to make changes in business practices relating to protection of personal information.

Sec. 7. The administrative safeguards required as part of a comprehensive written information security program are the administrative actions and policies and procedures for managing the selection, development, implementation, and maintenance of security measures to protect electronic or paper data and to manage the conduct of the covered entity's workforce in relation to the protection of that information. Administrative safeguards include all of the following:

(a) Management direction and support for information security and privacy of data in accordance with business requirements and relevant laws and regulations.

(b) Monitoring and analyzing security alerts and information, and distributing the alerts and information to appropriate personnel.

(c) Ensuring that the security policies and procedures clearly define information security responsibilities for all employees and contractors.

(d) Ensuring that information security goals are identified, meet the organizational requirements, and are integrated in relevant processes.

(e) Providing clear direction and visible management support for security initiatives.

(f) Providing the resources needed for information security.

(g) Establishing, publishing, maintaining, and disseminating security policies.

(h) Formulating, reviewing, and approving information security policies.

(i) Initiating plans and programs to maintain information security awareness.

(j) Education and training of employees on security awareness, the proper use of the computer security system, and the importance of personal information security.

(k) Oversight of third parties involving accessing, processing, communicating, or managing sensitive data.

(*l*) Classifying, labeling, and handling information to receive an appropriate level of protection that has varying degrees of sensitivity and criticality to the organization.

(m) Communicating information security events and weaknesses associated with information systems in a manner allowing timely corrective action to be taken.

(n) Reporting of suspected security weaknesses in the systems or services in a timely matter.

(o) Performing an annual process that identifies threats and vulnerabilities and results in a formal risk assessment.

(p) Performing a review at least once a year and updates when the environment changes.

Sec. 9. The physical safeguards required as part of a comprehensive written information security program are physical measures, policies, and procedures to protect electronic and paper information systems and related buildings and equipment where personal identifiable information is located. Physical safeguards include all of the following:

(a) Protecting secure areas by appropriate entry controls to ensure that only authorized personnel are allowed access to sensitive information.

(b) Using appropriate facility entry controls to limit and monitor physical access to systems that store, process, or transmit data.

(c) Maintaining physical security access controls for offices, rooms, and facilities that contain sensitive data.

(d) Developing procedures to help all personnel easily distinguish between employees and visitors with logging requirements.

(e) Implementing a clear desk policy for papers and removable storage media and a clear screen policy for sensitive data classified accordingly.

(f) Designing and applying physical protection and guidelines for working in secure areas.

(g) Informing personnel only on a need-to-know basis.

(h) Applying security to off-site equipment, taking into account the different risks of working outside the organization's

premises.

(i) Checking all items of equipment containing storage media to ensure that any sensitive data and licensed software has been removed or securely overwritten prior to disposal.

(j) Requiring prior authorization before equipment, portable storage devices, information, or software is taken off site.

Sec. 11. The technical safeguards required as part of a comprehensive written information security program are the technology and the policy and procedures for use of electronic protected information that protect that information and control access to it. Technical safeguards required under this act include all of the following:

(a) Managing, monitoring, and reviewing third-party services reports and records provided by the third party, and carrying out regular audits.

(b) Implementing protection against malicious and mobile codes to detect, prevent, and recover data.

(c) Adequately managing, controlling, and testing networks in order to protect against threats, and to maintain security for the systems and applications using the network, including information in transit.

(d) Identify and include all network services in any network services agreement, whether these services are provided in-house or outsourced.

(e) Media and storage devices should be controlled and physically protected.

(f) Disposing of media securely and safely when no longer

required, using formal procedures.

(g) Maintaining the security of information and software when exchanged within an organization or with any external entity.

(h) Protecting against unauthorized access, misuse, or corruption of media containing information during transportation beyond an organization's physical boundaries.

(i) With regard to on-line transactions, maintaining the confidentiality and integrity of data, verifying the credentials, retaining the privacy, using secure methods of communication, and securing all aspects of the transaction.

(j) Monitoring, logging, and testing systems, and recording information security events.

(k) Using network content intrusion detection systems, host-based intrusion detection systems, and intrusion prevention systems to monitor all network traffic and alert personnel to suspected compromises; and keeping all intrusion detection and prevention engines up to date.

(*l*) Protecting logging information against tampering and unauthorized access.

(m) Analyzing logging each day and taking appropriate action.

(n) Employing secure user authentication protocols, including all of the following:

(*i*) Control of user identification and other identifiers.

(*ii*) Use of a reasonably secure method of assigning and selecting passwords, or use of unique identifier technologies, such as biometrics or token devices.

(*iii*) Control of data security passwords to ensure that the

passwords are kept in a location or format that does not compromise the security of the data they protect.

(*iv*) Restriction of access to active users and active user accounts only.

(*v*) Blocking access to user identification after multiple unsuccessful attempts to gain access or the limitation placed on access for the particular system.

(o) Employing secure access control measures that do all of the following:

(*i*) Restrict access to records and files containing personal information to those who need that information to perform their job duties.

(*ii*) Assign unique identifications plus passwords that are not vendor-supplied default passwords to each individual with computer access, and that are reasonably designed to maintain the integrity of the security of the access controls.

(*iii*) To the extent technically feasible, encrypt all transmitted records and files containing personal information that will travel across public networks, and encrypt all data that are transmitted wirelessly.

(*iv*) Reasonably monitor systems for unauthorized use of or access to personal information.

(p) Encrypting all personal information stored on laptops or other portable devices.

(q) Maintaining up-to-date firewall protection and operating security patches to protect the integrity of personal information on a system that is connected to the internet.

(r) Using reasonably up-to-date versions of system security agent software, which must include malware protection and reasonably up-to-date patches and virus definitions, or a version of that software that can still be supported with up-to-date patches and virus definitions, and which is set to the most current security updates on a regular basis.

(s) Protecting important records from loss, destruction, and falsification, in accordance with statutory, regulatory, contractual, and business requirements.

(t) Planning and agreeing to audit requirements and activities involving checks on operational systems to minimize the risk.

Sec. 13. (1) A person that develops, implements, maintains, and monitors a comprehensive written information security program as described in sections 5 to 11 is immune from civil liability for any damages resulting from unauthorized access or acquisition of data or electronic data that compromises the security, availability, confidentiality, or integrity of personal information maintained by that person.

(2) The immunity provided under this section is in addition to any immunity otherwise provided by law.