PRINTER'S NO. 887

THE GENERAL ASSEMBLY OF PENNSYLVANIA

HOUSE BILL

No. 829 Session of 1999

INTRODUCED BY RAYMOND, BELARDI, CIVERA, L. I. COHEN, GEIST, GIGLIOTTI, HARHAI, HENNESSEY, KENNEY, LAUGHLIN, MAHER, NAILOR, PESCI, PISTELLA, ROSS, RUBLEY, SEYFERT AND TRELLO, MARCH 10, 1999

REFERRED TO COMMITTEE ON STATE GOVERNMENT, MARCH 10, 1999

AN ACT

Providing for governmentwide computer security and for the training in security matters of persons who are involved in the management, operation and use of State computers and State computer systems.

The General Assembly of the Commonwealth of Pennsylvania hereby enacts as follows:

Section 1. Short title.

This act shall be known and may be cited as the Computer Security Act.

Section 2. Statement of purpose.

The General Assembly declares that improving the security and privacy of sensitive information and critical data in State computers and State computer systems is in the public interest, and hereby creates a means for establishing minimum acceptable security practices for these computers and computer systems.

Section 3. Definitions.

The following words and phrases when used in this act shall have the meanings given to them in this section unless the context clearly indicates otherwise:

"Automatic data processing equipment." Equipment or the interconnected system or subsystems of equipment that are used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission or reception of data or information. The term includes electronic data processing equipment.

"Computer." An electronic, optical, electrochemical or other high-speed data processing device performing logical, arithmetic and storage functions.

"Computer system." Equipment or the interconnected system or subsystems of equipment that are used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission or reception of data or information. The term includes computers, peripheral devices, software, firmware and similar procedures; and services, including support services.

"Computer virus." A program or set of computer instructions with the ability to replicate all or part of itself when inserted into a computer's memory, operating system, files or application programs, which may include malicious computer instructions designed to alter or destroy data.

"Critical data." Computer data vital to the operations of the Commonwealth or to the citizens of this Commonwealth.

"Designated State agency." The Office of Administration or the State agency designated by the Governor to administer this act.

"Disaster." An event which disrupts State computers and State computer systems beyond the point where a State agency can achieve recovery through routine recovery procedures. The term includes, but is not limited to, ecological events such as storms, earthquakes and floods, accidents such as fire, power loss and communications loss and deliberate disruptions such as labor or management disputes, computer viruses and sabotage.

"Peripheral device." Includes a data storage facility or communications facility directly related to or operating in conjunction with a computer.

"Sensitive information." Information, the loss, misuse or unauthorized access to or modification of which could adversely affect the State interest or the conduct of State programs.

"State agency." A Commonwealth agency, as defined in 2 Pa.C.S. § 101 (relating to definitions), except criminal justice agencies which maintain information which is subject to the requirements of 18 Pa.C.S. § 9131 (relating to security requirements for repositories).

"State computer system." A computer system operated by a State agency or by a contractor of a State agency or other organization that processes information using a computer system on behalf of the State to accomplish a State function. The term includes automatic data processing equipment.

Section 4. Duties of State agencies.

(a) Designate sensitive information.--State agencies shall, within nine months of the effective date of this act and annually thereafter, identify as part of the security plan each State computer and State computer system, and systems under development, which are within or under the supervision of that agency and which contain sensitive information or critical data. The State agencies shall identify what sensitive information and critical data is contained in these computers and computer systems.

(b) Security plan.--State agencies shall, within one year of the effective date of this act, establish a security contingency disaster recovery plan for State computers and State computer systems within or under the supervision of that agency. The plan shall be based upon the generic plan developed by the designated State agency. The plan shall not be considered a public record as defined by the act of June 21, 1957 (P.L.390, No.212), referred to as the Right-to-Know Law. The plan shall be implemented by the State agency upon approval by the designated State agency, and it shall be updated annually by the agency and submitted to the designated State agency by December 15 of each year. This plan shall include, at a minimum, the following:

(1) A process to assess the risk and an assessment of the risk of each computer and computer system within or under the supervision of that agency against disasters, including infection from computer viruses, computer-related fraud and misuse, ecological events and other disasters and a description of the action necessary to reduce and minimize the risk of such disasters and abuses. Specific attention and emphasis should be given in the plan to those actions necessary to protect sensitive information and critical data.

(2) Procedures for the routine backup for sensitive information and critical data.

(3) Procedures for computer system disaster recovery.

(c) Training.--State agencies shall provide for mandatory periodic training in computer security awareness and accepted computer security practice for employees involved with the management, use or operation of a State computer or State computer system that is within or under the supervision of that agency and that contains critical data or sensitive information.

The training shall be provided in accordance with the regulations developed pursuant to section 5(a) by the designated State agency.

Section 5. Duties of the designated State agency.

(a) Regulations.--Within six months of the effective date of this act, the designated State agency shall develop regulations pertaining to implementation of this act and the required development of the State agencies' plans, training, research and coordinated activity provided for in this act for State computers and State computer systems.

(b) Computer security plan.--Within six months of the effective date of this act, the designated State agency shall initiate a generic computer security contingency disaster recovery plan for use by State agencies in the establishment of the plans required under section 4(b).

(c) Review of plans.--The designated State agency shall annually review and approve State agencies' plans for compliance with the regulations developed pursuant to subsection (a).

(d) Research.--The designated State agency shall perform research and conduct studies to determine the nature and extent of the vulnerabilities of, and to devise techniques for, the cost-effective security and privacy of sensitive information and critical data in State computers and State computer systems.

(e) Coordination.--The designated State agency shall coordinate closely with other offices and agencies to assure maximum use of existing and planned programs, materials, studies and reports relating to computer systems security and privacy in order to avoid unnecessary and costly duplication of effort. This coordination shall include periodic meetings with State agency personnel primarily responsible for management of State computers and State computer systems.

(f) Training.--In addition to developing regulations pertaining to training as required by subsection (a), the designated State agency shall act as a central repository of computer security training information and shall develop and provide training activity to include, at minimum, the following:

(1) Instruction as to the nature and character of computer viruses, computer-related fraud and misuse and other disasters.

(2) Enhanced awareness of the threats to and vulnerability of computer systems.

(3) The use of improved computer security practices.

Section 6. Effective date.

This act shall take effect in 30 days.