
THE GENERAL ASSEMBLY OF PENNSYLVANIA

HOUSE BILL

No. 389 Session of
1997

INTRODUCED BY RAYMOND, BUNT, PESCI, MICOZZIE, OLASZ, TIGUE,
FLICK, CIVERA, MELIO, BOYES, BATTISTO, BELARDI, GEIST, FARGO,
L. I. COHEN, TRELLO, JOSEPHS, LAUGHLIN, HENNESSEY AND
PETRARCA, FEBRUARY 10, 1997

REFERRED TO COMMITTEE ON STATE GOVERNMENT, FEBRUARY 10, 1997

AN ACT

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

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

7 Section 1. Short title.

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

10 Section 2. Statement of purpose.

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

16 Section 3. Definitions.

17 The following words and phrases when used in this act shall
18 have the meanings given to them in this section unless the

1 context clearly indicates otherwise:

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

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

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

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

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

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

28 "Disaster." An event which disrupts State computers and
29 State computer systems beyond the point where a State agency can
30 achieve recovery through routine recovery procedures. The term

1 includes, but is not limited to, ecological events such as
2 storms, earthquakes and floods, accidents such as fire, power
3 loss and communications loss and deliberate disruptions such as
4 labor or management disputes, computer viruses and sabotage.

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

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

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

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

21 Section 4. Duties of State agencies.

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

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

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

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

24 (3) Procedures for computer system disaster recovery.

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

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

4 Section 5. Duties of the designated State agency.

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

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

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

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

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

1 computers and State computer systems.

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

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

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

12 (3) The use of improved computer security practices.

13 Section 6. Effective date.

14 This act shall take effect in 30 days.