

COMPUTER SECURITY ACT

PL 100-235

SECTION 1. SHORT TITLE.

This Act (enacting sections 278g-3 and 278g-4 of Title 15, Commerce and Trade, amending section 759 of this title and section 272 of Title 15, and enacting provisions set out as a note under section 271 of Title 15) may be cited as the 'Computer Security Act of 1987'.

SEC. 2. PURPOSE.

(a) In General. - The Congress declares that improving the security and privacy of sensitive information in Federal computer systems is in the public interest, and hereby creates a means for establishing minimum acceptable security practices for such systems, without limiting the scope of security measures already planned or in use.

(b) Specific Purposes. - The purposes of this Act are -

(1) by amending the Act of March 3, 1901 (15 U.S.C. 271 et seq.), to assign to the National Bureau of Standards responsibility for developing standards and guidelines for Federal computer systems, including responsibility for developing standards and guidelines needed to assure the cost-effective security and privacy of sensitive information in Federal computer systems, drawing on the technical advice and assistance (including work products) of the National Security Agency, where appropriate;

(2) to provide for promulgation of such standards and guidelines by amending section 111(d) of the Federal Property and Administrative Services Act of 1949 (40 U.S.C. 759(d));

(3) to require establishment of security plans by all operators of Federal computer systems that contain sensitive information; and

(4) to require mandatory periodic training for all persons

involved in management, use, or operation of Federal computer systems that contain sensitive information.

SEC. 5. FEDERAL COMPUTER SYSTEM SECURITY TRAINING.

(a) In General. - Each Federal agency shall provide for the mandatory periodic training in computer security awareness and accepted computer security practice of all employees who are involved with the management, use, or operation of each Federal computer system within or under the supervision of that agency. Such training shall be -

(1) provided in accordance with the guidelines developed pursuant to section 20(a)(5) of the National Bureau of Standards Act (as added by section 3 of this Act) (15 U.S.C. 278g-3(a)(5)), and in accordance with the regulations issued under subsection (c) of this section for Federal civilian employees; or

(2) provided by an alternative training program approved by the head of that agency on the basis of a determination that the alternative training program is at least as effective in accomplishing the objectives of such guidelines and regulations.

(b) Training Objectives. - Training under this section shall be started within 60 days after the issuance of the regulations described in subsection (c). Such training shall be designed -

(1) to enhance employees' awareness of the threats to and vulnerability of computer systems; and

(2) to encourage the use of improved computer security practices.

(c) Regulations. - Within six months after the date of the enactment of this Act (Jan. 8, 1988), the Director of the Office of Personnel Management shall issue regulations prescribing the procedures and scope of the training to be provided Federal civilian employees under subsection (a) and the manner in which such training is to be carried out.

SEC. 6. ADDITIONAL RESPONSIBILITIES FOR COMPUTER SYSTEMS SECURITY AND PRIVACY.

(a) Identification of Systems That Contain Sensitive Information. - Within 6 months after the date of enactment of this

Act (Jan. 8, 1988), each Federal agency shall identify each Federal computer system, and system under development, which is within or under the supervision of that agency and which contains sensitive information.

(b) Security Plan. - Within one year after the date of enactment of this Act (Jan. 8, 1988), each such agency shall, consistent with the standards, guidelines, policies, and regulations prescribed pursuant to section 111(d) of the Federal Property and Administrative Services Act of 1949 (40 U.S.C. 759(d)), establish a plan for the security and privacy of each Federal computer system identified by that agency pursuant to subsection (a) that is commensurate with the risk and magnitude of the harm resulting from the loss, misuse, or unauthorized access to or modification of the information contained in such system. Copies of each such plan shall be transmitted to the National Bureau of Standards and the National Security Agency for advice and comment. A summary of such plan shall be included in the agency's five-year plan required by section 3505 of title 44, United States Code. Such plan shall be subject to disapproval by the Director of the Office of Management and Budget. Such plan shall be revised annually as necessary.

SEC. 7. DEFINITIONS.

As used in this Act, the terms 'computer system', 'Federal computer system', 'operator of a Federal computer system', 'sensitive information', and 'Federal agency' have the meanings given in section 20(d) of the National Bureau of Standards Act (as added by section 3 of this Act) (15 U.S.C. 278g-3(d)).

SEC. 8. RULES OF CONSTRUCTION OF ACT.

Nothing in this Act, or in any amendment made by this Act, shall be construed -

(1) to constitute authority to withhold information sought pursuant to section 552 of title 5, United States Code; or

(2) to authorize any Federal agency to limit, restrict, regulate, or control the collection, maintenance, disclosure, use, transfer, or sale of any information (regardless of the medium in which the information may be maintained) that is -

(A) privately-owned information;

(B) disclosable under section 552 of title 5, United States Code, or other law requiring or authorizing the public disclosure of information; or

(C) public domain information.