108TH CONGRESS
1ST SESSION

S. 187

To provide for the elimination of significant vulnerabilities in the information technology of the Federal Government, and for other purposes.

IN THE SENATE OF THE UNITED STATES

JANUARY 16, 2003

Mr. EDWARDS introduced the following bill; which was read twice and referred to the Committee on Governmental Affairs

---

A BILL

To provide for the elimination of significant vulnerabilities in the information technology of the Federal Government, and for other purposes.

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

SECTION 1. SHORT TITLE.

This Act may be cited as the ''National Cyber Security Leadership Act of 2003''.

SEC. 2. FINDINGS.

Congress makes the following findings:

(1) Federal agencies rely on networked computer systems to deliver critical services and information to the American people, including operations

related to national defense, emergency services, tax collection, and the payment of benefits.

(2) There has been an astonishing increase in cyber threats to government and industry in recent years. The number of cyber attacks on Federal Government systems in 2001 was 71 percent greater than the number of such attacks on such systems in 2000.

(3) Cyber attacks can cause irreparable harm in network systems, including the loss or dissemination of sensitive and important data. Cyber attacks can also reduce the confidence of the American people in the integrity and security of the Internet.

(4) There is mounting evidence to suggest that terrorists view the Internet as a tool to achieve their goals. Government investigators found that al Qaeda operatives browsed Internet sites that offered software describing the digital switches that control power, water, transport, and communications grids.

(5) The Bush Administration has recognized in its draft National Strategy to Secure Cyberspace ''the pressing need to make federal cyberspace security a model for the nation''.

(6) All but a few Federal agencies continue to receive failing grades for their cyber security programs.

(7) Federal agencies must take significant steps to better protect themselves against cyber attacks, including—

(A) identifying significant vulnerabilities in their computer networks and the tools needed to detect such vulnerabilities;

(B) monitoring for new vulnerabilities in their computer networks, and assessing risks of cyber attacks;

(C) testing computers against identified vulnerabilities; and

(D) ensuring that computers and networks are adequately protected against such vulnerabilities.

SEC. 3. DEFINITIONS.

In this Act:

(1) CHIEF INFORMATION OFFICER.—The term ''Chief Information Officer'', with respect to an agency, means the official designated as the Chief Information Officer of the agency pursuant to section 3506(a)(2) of title 44, United States Code.

(2) VULNERABILITY.—The term ''vulnerability'', in the case of information technology, means an error or defect in coding, configuration, or installation of such information technology that increases its susceptibility to a cyber threat.

(3) OTHER DEFINITIONS.—Except as otherwise provided in this section, any term used in this Act which is defined in section 3502 of title 44, United States Code, shall have the meaning given that term in such section 3502.

SEC. 4. ELIMINATION OF SIGNIFICANT VULNERABILITIES OF FEDERAL GOVERNMENT INFORMATION TECHNOLOGY.

(a) IN GENERAL.—The Chief Information Officer of each agency shall—

(1) identify the significant vulnerabilities of the information technology of such agency, including—

(A) vulnerabilities of such classes of information technology of such agency as the Chief Information Officer shall designate for purposes of this section; and

(B) vulnerabilities of the information technology of such agency as a whole;

(2) establish performance goals for eliminating the significant vulnerabilities of the information

technology of such agency identified under paragraph (1), with such performance goals—

(A) to be established utilizing the current state of the information technology of such agency as a baseline;

(B) to be stated both for particular classes of information technology of such agency (as determined under paragraph (1)(A)) and for the information technology of such agency as a whole; and

(C) to be expressed as target ratios of vulnerabilities per information technology;

(3) procure or develop tools to identify and eliminate the vulnerabilities identified under paragraph (1) in order to achieve the performance goals established under paragraph (2);

(4) train personnel of such agency in the utilization of tools procured or developed under paragraph (3);

(5) not less often than once each quarter, test the information technology of such agency to determine the extent of the compliance of the information technology with the performance goals established under paragraph (3); and

(6) to the extent that the information technology of such agency does not comply with the performance goals established under paragraph (3), promptly develop and implement a plan to eliminate significant vulnerabilities in the information technology in order to achieve compliance with such performance goals.

(b) ANNUAL REPORT ON ACTIVITIES.—

(1) REQUIREMENT.—The Chief Information Officer of each agency shall include information on its activities under subsection (a) in each annual report submitted to the Director of the Office of Management and Budget under section 3545(e) of title 44, United States Code (as amended by section 301(b) of the Federal Information Security Management Act of 2002 (title III of Public Law 107–347)).

(2) FORM.—The form of information submitted under paragraph (1) shall be specified by the Director of the Office of Management and Budget.

(c) GOVERNMENTWIDE STANDARDS.—

(1) REVIEW BY NIST.—The Director of the Office of Management and Budget shall ensure the review by the Director of the National Institute of Standards and Technology of the annual reports

submitted under subsection (b) in the first year after the date of the enactment of this Act.

(2) GUIDELINES.—Not later than 180 days after receiving annual reports for review under paragraph (1), the Director of the National Institute of Standards and Technology shall develop and make available to the Chief Information Officers of the agencies governmentwide guidelines for use in complying with subsection (a). The guidelines shall—

(A) identify vulnerabilities of information technology common to the agencies; and

(B) describe means of eliminating such vulnerabilities, including the use of checklists pursuant to section 8(c) of the Cyber Security Research and Development Act (Public Law 107–305).

(3) MANDATORY USE.—

(A) DESIGNATION OF VULNERABILITIES.—The Director of the National Institute of Standards and Technology shall designate as a result of the review under paragraph (1) any significant vulnerabilities of information technology of such broad applicability and severity so as to warrant the mandatory use of the

guidelines developed under paragraph (2) with respect to such vulnerabilities.

(B) MANDATORY USE.—The Secretary of Commerce shall, using the authority available to the Secretary under section 11331(b) of title 40, United States Code, mandate the use by the agencies of guidelines developed under paragraph (2) with respect to vulnerabilities designated under subparagraph (A).

(C) USE AND EXCEPTION.—Each agency shall use a standard mandated under subparagraph (B) unless the Chief Information Officer of such agency determines, with the concurrence of the Director of the National Institute of Standards and Technology, that the use of such guideline by such agency would not increase the security of the information technology covered by such standard.

SEC. 5. AUTHORIZATION OF APPROPRIATIONS.

(a) AUTHORIZATION OF APPROPRIATIONS.—There is authorized to be appropriated to carry out the provisions of this Act amounts as follows:

(1) For the Department of Commerce for the National Institute of Standards and Technology,

$1,000,000 for fiscal year 2004 to develop the guidelines required by section 4(c).

(2) For each agency, such sums as may be necessary for such agency for fiscal years 2004 through 2008 to carry out the provisions of this Act.

(b) AVAILABILITY.—The amount authorized to be appropriated by subsection (a)(1) shall remain available until expended.

SEC. 6. EFFECTIVE DATE.

This Act shall take effect 180 days after the date of the enactment of this Act.

○