[STAFF WORKING DRAFT]

AUGUST 6, 2001

107TH CONGRESS
1ST SESSION

S. _____

To provide for private sector development of workable security system standards and a certification protocol that could be implemented and enforced by Federal regulations, and for other purposes.

IN THE SENATE OF THE UNITED STATES

SEPTEMBER ——, 2001

Mr. HOLLINGS (for himself and Mr. STEVENS) introduced the following bill; which was read twice and referred to the Committee on

---

A BILL

To provide for private sector development of workable security system standards and a certification protocol that could be implemented and enforced by Federal regulations, 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; TABLE OF SECTIONS.

(a) SHORT TITLE.—This Act may be cited as the "Security Systems Standards and Certification Act".

(b) TABLE OF SECTIONS.—The table of sections for this Act is as follows:

Sec. 1. Short title; table of sections.
Sec. 2. Findings.
TITLE I—SECURITY SYSTEM STANDARDS AND CERTIFICATION
Sec. 101. Prohibition of certain devices.
Sec. 102. Preservation of the integrity of security.
Sec. 103. Prohibited acts.
Sec. 104. Adoption of security system standards.
Sec. 105. Certification of technologies.
Sec. 106. Federal Advisory Committee Act exemption.
Sec. 107. Antitrust exemption.
Sec. 108. Enforcement.
Sec. 109. Definitions.
Sec. 110. Effective date.
TITLE II—INTERNET SECURITY INITIATIVES
Sec. 201. Findings.
Sec. 202. Computer Security Partnership Council.
Sec. 203. Research and development.
Sec. 204. Computer security training programs.
Sec. 205. Government information security standards.
Sec. 206. Recognition of quality in computer security practices.
Sec. 207. Development of automated privacy controls.

SEC. 2. FINDINGS.

[TO BE SUPPLIED]

TITLE I—SECURITY SYSTEM STANDARDS

SEC. 101. PROHIBITION OF CERTAIN DEVICES.

(a) IN GENERAL.—It is unlawful to manufacture, import, offer to the public, provide or otherwise traffic in any interactive digital device that does not include and utilize certified security technologies that adhere to the security system standards adopted under section 104.

(b) EXCEPTION.—Subsection (a) does not apply to the offer for sale or provision of, or other trafficking in, any previously-owned interactive digital device, if such device was legally manufactured or imported, and sold, prior

to the effective date of regulations adopted under section 104 and not subsequently modified in violation of subsection (a) or 103(a).

SEC. 102. PRESERVATION OF THE INTEGRITY OF SECURITY.

An interactive computer service shall store and transmit with integrity any security measure associated with certified security technologies that is used in connection with copyrighted material or other protected content such service transmits or stores.

SEC. 103. PROHIBITED ACTS.

(a) REMOVAL OR ALTERATION OF SECURITY.—No person may—

(1) remove or alter any certified security technology in an interactive digital device; or

(2) transmit or make available to the public any copyrighted material or other protected content where the security measure associated with a certified security technology has been removed or altered.

(b) PERSONAL TIME-SHIFTING COPIES CANNOT BE BLOCKED.—No person may apply a security measure that uses a certified security technology to prevent a lawful recipient from making a personal copy for time-shifting purposes of programming at the time it is lawfully performed, on an over-the-air broadcast, non-premium cable channel,

or non-premium satellite channel, by a television broadcast station (as defined in section 122(j)(5)(A) of title 17, United States Code), a cable system (as defined in section 111(f) of such title), or a satellite carrier (as defined in section 119(d)(6) of such title).

SEC. 104. ADOPTION OF SECURITY SYSTEM STANDARDS.

(a) CRITERIA.—In achieving the goals of setting standards that will provide effective security for content and certifying as many conforming technologies as possible to develop a competitive and innovative marketplace, the following criteria shall be applied to the development of security system standards and certified security technologies:

(1) Reliability.

(2) Renewability.

(3) Resistance to attack.

(4) Ease of implementation.

(5) Modularity.

(6) Applicability to multiple technology platforms.

(b) PRIVATE SECTOR EFFORTS.—

(1) IN GENERAL.—The Secretary shall make a determination, not more than 12 months after the date of enactment of this Act, as to whether—

(A) representatives of interactive digital device manufacturers and representatives of copyright owners have reached agreement on security system standards for use in interactive digital devices; and

(B) the standards meet the criteria in subsection (a).

(2) EXTENSION OF 12-MONTH PERIOD.—The Secretary may, for good cause shown, extend the 12-month period in paragraph (1) for a period of not more than 6 months if the Secretary determines that—

(A) substantial progress has been made by those representatives toward development of security system standards that will meet those criteria;

(B) those representatives are continuing to negotiate in good faith; and

(C) there is a reasonable expectation that final agreement will be reached by those representatives before the expiration of the extended period of time.

(c) AFFIRMATIVE DETERMINATION.—If the Secretary makes a determination under subsection (b)(1) that an agreement on security system standards that meet the

criteria in subsection (a) has been reached by those representatives, then the Secretary shall—

(1) initiate a rulemaking within 30 days after the date on which the determination is made to adopt those standards; and

(2) publish a final rule pursuant to that rulemaking not later than 90 days after initiating the rulemaking that will take effect 1 year after its publication.

(d) NEGATIVE DETERMINATION.—If the Secretary makes a determination under subsection (b)(1) that an agreement on security system standards that meet the criteria in subsection (a) has not been reached by those representatives, then the Secretary—

(1) in consultation with representatives described in subsection (b)(1)(A), the National Institute of Standards and Technology and the Register of Copyrights, shall initiate a rulemaking within 30 days after the date on which the determination is made to adopt security system standards that meet those criteria to provide effective security for copyrighted material and other protected content; and

(2) publish a final rule pursuant to that rulemaking not later than 1 year after initiating the

rulemaking that will take effect 1 year after its publication.

(c) MEANS OF IMPLEMENTING STANDARDS.—The security system standards adopted under subsection (c) or (d) shall provide for secure technical means of implementing directions of copyright owners, for copyrighted material, and rights holders, for other protected content, with regard to the reproduction, performance, display, storage, and transmission of such material or content.

(f) SUBSEQUENT MODIFICATION; NEW STANDARDS.—The Secretary may conduct subsequent rulemakings to modify any standards established under subsection (c) or (d) or to adopt new security system standards that meet the criteria in subsection (a). In conducting any such subsequent rulemaking, the Secretary shall consult with representatives of interactive digital device manufacturers, representatives of copyright owners, the National Institute of Standards and Technology, and the Register of Copyrights. Any final rule published in such a subsequent rulemaking shall—

(1) apply prospectively only; and

(2) take into consideration the effect of adoption of the modified or new security system standards on consumers' ability to utilize interactive dig-

tal devices manufactured before the modified or new standards take effect.

SEC. 105. CERTIFICATION OF TECHNOLOGIES.

The Secretary shall certify technologies that adhere to the security system standards adopted under section 104. The Secretary shall certify only those conforming technologies that are available for licensing on reasonable and nondiscriminatory terms.

SEC. 106. FEDERAL ADVISORY COMMITTEE ACT EXEMPTION.

The Federal Advisory Committee Act (5 U.S.C. App.) does not apply to any committee, board, commission, council, conference, panel, task force, or other similar group of representatives of interactive digital devices and representatives of copyright owners convened for the purpose of developing the security system standards described in section 104.

SEC. 107. ANTITRUST EXEMPTION.

(a) IN GENERAL.—Any person described in section 104(b)(1)(A) may file with the Secretary of Commerce a request for authority for a group of 2 or more such persons to meet and enter into discussions, if the sole purpose of the discussions is to discuss the development of security system standards under section 104. The Secretary shall

grant or deny the request within 10 days after it is received.

(b) PROCEDURE.—The Secretary shall establish procedures within 30 days after the date of enactment of this Act for filing requests for an authorization under subsection (a).

(c) EXEMPTION AUTHORIZED.—When the Secretary finds that it is required by the public interest, the Secretary shall exempt a person participating in a meeting or discussion described in subsection (a) from the antitrust laws to the extent necessary to allow the person to proceed with the activities approved in the order.

(d) ANTITRUST LAWS DEFINED.—In this section, the term "antitrust laws" has the meaning given that term in the first section of the Clayton Act (15 U.S.C. 12).

SEC. 105. ENFORCEMENT.

The provisions of section 1203 and 1204 of title 17, United States Code, shall apply to any violation of this title as if—

(1) a violation of section 101 or 103(a)(1) of this Act were a violation of section 1201 of title 17, United States Code; and

(2) a violation of section 102 or section 103(a)(2) of this Act were a violation of section 1202 of that title.

SEC. 109. DEFINITIONS.

In this title:

(1) CERTIFIED SECURITY TECHNOLOGY.—The term "certified security technology" means a security technology certified by the Secretary of Commerce under section 105.

(2) INTERACTIVE COMPUTER SERVICE.—The term "interactive computer service" has the meaning given that term in section 230(f) of the Communications Act of 1934 (47 U.S.C. 230(f)).

(3) INTERACTIVE DIGITAL DEVICE.—The term "interactive digital device" means any machine, device, product, software, or technology, whether or not included with or as part of some other machine, device, product, software, or technology, that is designed, marketed or used for the primary purpose of, and that is capable of, storing, retrieving, processing, performing, transmitting, receiving, or copying information in digital form.

(4) SECRETARY.—The term "Secretary" means the Secretary of Commerce.

SEC. 110. EFFECTIVE DATE.

This title shall take effect on the date of enactment of this Act, except that sections 101, 102, and 108 shall take effect on the day on which the final rule published under section 104(c) or (d) takes effect.

TITLE II—INTERNET SECURITY INITIATIVES

SEC. 201. FINDINGS.

The Congress finds the following:

(1) Good computer security practices are an underpinning of any privacy protection. The operator of a computer system should protect that system from unauthorized use and secure any sensitive information.

(2) The Federal Government should be a role model in securing its computer systems and should ensure the protection of sensitive information controlled by Federal agencies.

(3) The National Institute of Standards and Technology has the responsibility for developing standards and guidelines needed to ensure the cost-effective security and privacy of sensitive information in Federal computer systems.

(4) This Nation faces a shortage of trained, qualified information technology workers, including computer security professionals. As the demand for information technology workers grows, the Federal government will have an increasingly difficult time attracting such workers into the Federal workforce.

(5) Some commercial off-the-shelf hardware and off-the-shelf software components to protect computer systems are widely available. There is still a need for long-term computer security research, particularly in the area of infrastructure protection.

(6) The Nation's information infrastructures are owned, for the most part, by the private sector, and partnerships and cooperation will be needed for the security of these infrastructures.

(7) There is little financial incentive for private companies to enhance the security of the Internet and other infrastructures as a whole. The Federal government will need to make investments in this area to address issues and concerns not addressed by the private sector.

SEC. 202. COMPUTER SECURITY PARTNERSHIP COUNCIL.

(a) ESTABLISHMENT.—The Secretary of Commerce, in consultation with the President's Information Technology Advisory Committee established by Executive Order No. 13035 of February 11, 1997 (62 F.R. 7231), shall establish a 25-member Computer Security Partnership Council the membership of which shall be drawn from Federal, State, and local governments, universities, and businesses.

(b) PURPOSE.—The purpose of the Council is to collect and share information about, and to increase public awareness of, information security practices and programs, threats to information security, and responses to those threats.

(c) STUDY.—Within 12 months after the date of enactment of this Act, the Council shall publish a report which evaluates and describes areas of computer security research and development that are not adequately developed or funded.

SEC. 203. RESEARCH AND DEVELOPMENT.

Section 20 of the National Institute of Standards and Technology Act (15 U.S.C. 278g-3) is amended—

(1) by redesignating subsections (c) and (d) as subsections (d) and (e), respectively; and

(2) by inserting after subsection (b) the following:

"(c) RESEARCH AND DEVELOPMENT OF PROTECTION TECHNOLOGIES.—

"(1) IN GENERAL.—The Institute shall establish a program at the National Institute of Standards and Technology to conduct, or to fund the conduct of, research and development of technology and techniques to provide security for advanced communications and computing systems and networks in-

cluding the Next Generation Internet, the underlying structure of the Internet, and networked computers.

"(2) PURPOSE.—A purpose of the program established under paragraph (1) is to address issues or problems that are not addressed by market-driven, private-sector information security research. This may include research—

"(A) to identify internet security problems which are not adequately addressed by current security technologies;

"(B) to develop interactive tools to analyze security risks in an easy-to-understand manner;

"(C) to enhance the security and reliability of the underlying Internet infrastructure while minimizing other operational impacts such as speed; and

"(D) to allow networks to become self-healing and provide for better analysis of the state of Internet and infrastructure operations and security.

"(3) MATCHING GRANTS.—A grant awarded by the Institute under the program established under paragraph (1) to a commercial enterprise may not exceed 50 percent of the cost of the project to be funded by the grant.

"(4) AUTHORIZATION OF APPROPRIATIONS.—There are authorized to be appropriated to the Institute to carry out this subsection—

"(A) $50,000,000 for fiscal year 2001;

"(B) $60,000,000 for fiscal year 2002;

"(C) $70,000,000 for fiscal year 2003;

"(D) $80,000,000 for fiscal year 2004;

"(E) $90,000,000 for fiscal year 2005; and

"(F) $100,000,000 for fiscal year 2006.".

SEC. 204. COMPUTER SECURITY TRAINING PROGRAMS.

(a) IN GENERAL.—The Secretary of Commerce, in consultation with appropriate Federal agencies, shall establish a program to support the training of individuals in computer security, Internet security, and related fields at institutions of higher education located in the United States.

(b) SUPPORT AUTHORIZED.—Under the program established under subsection (a), the Secretary may provide scholarships, loans, and other forms of financial aid to students at institutions of higher education. The Secretary shall require a recipient of a scholarship under this program to provide a reasonable period of service as an employee of the United States government after graduation as a condition of the scholarship, and may authorize full or partial forgiveness of indebtedness for loans made

under this program in exchange for periods of employment by the United States government.

(c) AUTHORIZATION OF APPROPRIATIONS.—There are authorized to be appropriated to the Secretary such sums as may be necessary to carry out this section—

(A) $15,000,000 for fiscal year 2001;

(B) $17,000,000 for fiscal year 2002;

(C) $20,000,000 for fiscal year 2003;

(D) $25,000,000 for fiscal year 2004;

(E) $30,000,000 for fiscal year 2005; and

(F) $35,000,000 for fiscal year 2006.

SEC. 205. GOVERNMENT INFORMATION SECURITY STANDARDS.

(a) IN GENERAL.—Section 20(b) of the National Institute of Standards and Technology Act (15 U.S.C. 278g-3(b)) is amended—

(1) by striking "and" after the semicolon in paragraph (4);

(2) by redesignating paragraph (5) as paragraph (6); and

(3) by inserting after paragraph (4) the following:

"(5) to provide guidance and assistance to Federal agencies in the protection of interconnected computer systems and to coordinate Federal re-

sponse efforts related to unauthorized access to Federal computer systems; and".

(b) FEDERAL COMPUTER SYSTEM SECURITY TRAINING.—Section 5(b) of the Computer Security Act of 1987 (49 U.S.C. 759 note) is amended—

(1) by striking "and" at the end of paragraph (1);

(2) by striking the period at the end of paragraph (2) and inserting in lieu thereof "; and"; and

(3) by adding at the end the following new paragraph:

"(3) to include emphasis on protecting the availability of Federal electronic citizen services and protecting sensitive information in Federal databases and Federal computer sites that are accessible through public networks.".

SEC. 206. RECOGNITION OF QUALITY IN COMPUTER SECURITY PRACTICES.

Section 20 of the National Institute of Standards and Technology Act (15 U.S.C. 278g-3), as amended by section 203, is further amended—

(1) by redesignating subsections (d) and (e) as subsections (e) and (f), respectively; and

(2) by inserting after subsection (c), the following:

"(d) AWARD PROGRAM.—The Institute may establish a program for the recognition of excellence in Federal computer system security practices, including the development of a seal, symbol, mark, or logo that could be displayed on the website maintained by the operator of such a system recognized under the program. In order to be recognized under the program, the operator—

"(1) shall have implemented exemplary processes for the protection of its systems and the information stored on that system;

"(2) shall have met any standard established under subsection (a);

"(3) shall have a process in place for updating the system security procedures; and

"(4) shall meet such other criteria as the Institute may require.".

SEC. 207. DEVELOPMENT OF AUTOMATED PRIVACY CONTROLS.

Section 20 of the National Institute of Standards and Technology Act (15 U.S.C. 278g-3), as amended by section 206, is further amended—

(1) by redesignating subsection (f) as subsection (g); and

(2) by inserting after subsection (e) the following:

"(f) DEVELOPMENT OF INTERNET PRIVACY PROGRAM.—The Institute shall encourage and support the development of one or more computer programs, protocols, or other software, such as the World Wide Web Consortium's P3P program, capable of being installed on computers, or computer networks, with Internet access that would reflect the user's preferences for protecting personally-identifiable or other sensitive, privacy-related information, and automatically execute the program, once activated, without requiring user intervention.".

O