[COMMITTEE PRINT]

111TH CONGRESS
1ST SESSION

H. R. _____

To authorize the Director of the National Institute of Standards and Technology to coordinate United States Government representation in international cybersecurity technical standards development, and for other purposes.

IN THE HOUSE OF REPRESENTATIVES

_____ introduced the following bill; which was referred to the Committee on _____

A BILL

To authorize the Director of the National Institute of Standards and Technology to coordinate United States Government representation in international cybersecurity technical standards development, 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 ''Cybersecurity Coordination and Awareness Act''.

SEC. 2. DEFINITIONS.

In this Act:

(1) DIRECTOR.—The term ''Director'' means the Director of the National Institute of Standards and Technology.

(2) INSTITUTE.—The term ''Institute'' means the National Institute of Standards and Technology.

SEC. 3. INTERNATIONAL CYBERSECURITY TECHNICAL STANDARDS.

The Director, in coordination with appropriate Federal authorities, shall—

(1) ensure coordination of United States Government representation in the international development of technical standards related to cybersecurity; and

(2) not later than 1 year after the date of enactment of this Act, develop and transmit to the Congress a proactive plan to engage international standards bodies with respect to the development of technical standards related to cybersecurity.

SEC. 4. PROMOTING CYBERSECURITY AWARENESS AND EDUCATION.

(a) PROGRAM.—The Director, in collaboration with relevant Federal agencies, industry, educational institutions, and other organizations, shall develop and implement a cybersecurity awareness and education program to

increase public awareness of cybersecurity risks, consequences, and best practices through—

(1) the widespread dissemination of cybersecurity technical standards and best practices identified by the Institute; and

(2) efforts to make cybersecurity technical standards and best practices usable by individuals, small to medium-sized businesses, State and local governments, and educational institutions.

(b) MANUFACTURING EXTENSION PARTNERSHIP.—The Director shall, to the extent appropriate, implement subsection (a) through the Manufacturing Extension Partnership program under section 25 of the National Institute of Standards and Technology Act (15 U.S.C. 278k).

(c) REPORT TO CONGRESS.—Not later than 90 days after the date of enactment of this Act, the Director shall transmit to the Congress a report containing a strategy for implementation of this section.

SEC. 5. IDENTITY MANAGEMENT RESEARCH AND DEVELOPMENT.

The Director shall establish a program to support the development of technical standards, metrology, testbeds, and conformance criteria, taking into account appropriate user concerns, to—

(1) improve interoperability among identity management technologies;

(2) strengthen authentication methods of identity management systems; and

(3) improve privacy protection in identity management systems through authentication and security protocols.

SEC. 6. AMENDMENT TO CYBERSECURITY RESEARCH AND DEVELOPMENT ACT.

(a) CHECKLISTS FOR GOVERNMENT SYSTEMS.—Section 8(c) of the Cybersecurity Research and Development Act (15 U.S.C. 7406(c)) is amended to read as follows:

''(c) CHECKLISTS FOR GOVERNMENT SYSTEMS.—

''(1) IN GENERAL.—The Director of the National Institute of Standards and Technology shall develop or identify and revise or adapt as necessary, checklists, configuration profiles, and deployment recommendations for products and protocols that minimize the security risks associated with each computer hardware or software system that is, or is likely to become, widely used within the Federal Government.

''(2) PRIORITIES FOR DEVELOPMENT.—The Director of the National Institute of Standards and Technology shall establish priorities for the develop-

ment of checklists under this subsection. Such priorities may be based on the security risks associated with the use of each system, the number of agencies that use a particular system, the usefulness of the checklist to Federal agencies that are users or potential users of the system, or such other factors as the Director determines to be appropriate.

''(3) EXCLUDED SYSTEMS.— The Director of the National Institute of Standards and Technology may exclude from the requirements of paragraph (1) any computer hardware or software system for which the Director determines that the development of a checklist is inappropriate because of the infrequency of use of the system, the obsolescence of the system, or the inutility or impracticability of developing a checklist for the system.

''(4) AUTOMATION SPECIFICATIONS.—The Director of the National Institute of Standards and Technology shall develop automated security specifications (such as the Security Content Automation Protocol) with respect to checklist content and associated security related data.

''(5) DISSEMINATION OF CHECKLISTS.—The Director of the National Institute of Standards and Technology shall ensure that any product developed

under the National Checklist Program for any information system, including the Security Content Automation Protocol and other automated security specifications, is made available to Federal agencies.

''(6) AGENCY USE REQUIREMENTS.—Federal agencies shall use checklists developed or identified under paragraph (1) to secure computer hardware and software systems. This paragraph does not—

''(A) require any Federal agency to select the specific settings or options recommended by the checklist for the system;

''(B) establish conditions or prerequisites for Federal agency procurement or deployment of any such system;

''(C) imply an endorsement of any such system by the Director of the National Institute of Standards and Technology; or

''(D) preclude any Federal agency from procuring or deploying other computer hardware or software systems for which no such checklist has been developed or identified under paragraph (1).''.

(b) INTRAMURAL SECURITY RESEARCH.—Section 20 of the National Institute of Standards and Technology Act (15 U.S.C. 278g–3) is amended by redesignating sub-

section (e) as subsection (f), and by inserting after subsection (d) the following:

''(e) INTRAMURAL SECURITY RESEARCH.—As part of the research activities conducted in accordance with subsection (d)(3), the Institute shall—

''(1) conduct a research program to develop a unifying and standardized identity, privilege, and access control management framework for the enforcement of a wide variety of resource protection policies and that is amenable to implementation within a wide variety of existing and emerging computing environments;

''(2) carry out research associated with improving the security of information systems and networks;

''(3) carry out research associated with improving the testing, measurement, usability, and assurance of information systems and networks; and

''(4) carry out research associated with improving security of industrial control systems.''.