4.1 Establish a National Cybersecurity Certification and Labeling Authority

This proposal implements the Commission's recommendation to create a National Cybersecurity Certification and Labeling Authority to establish and manage a voluntary cybersecurity certification and labeling program for information and communication technologies. The certification scheme is aimed at enabling critical infrastructure providers to more easily price cybersecurity into equipment procurement decisions, facilitating decision-making that enhances the overall cybersecurity and resilience of technologies purchased in the United States.

A BILL

To establish a National Cybersecurity Certification and Labeling Authority, and for other purposes.

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

SEC. 1. ESTABLISH A NATIONAL CYBERSECURITY CERTIFICATION AND LABELING AUTHORITY.

(a) Definitions.—In this section:

(1) ACCREDITED CERTIFYING AGENT.—The term "accredited certifying agent" means any organization that is accredited by the Authority as a certifying agent for the purposes of certifying a specific class of critical information and communications technology.

(2) AUTHORITY.—The term "Authority" means the National Cybersecurity Certification and Labeling Authority established under subsection (b)(1).

(3) CERTIFICATION.—The term "certification" means an attestation by an accredited certifying agent that identified products, processes, systems, or persons comply with established and identified requirements as performed and confirmed by an accredited certifying agent.

(4) CERTIFICATE.—The term "certificate" means a document issued by an accredited certifying agent affirming that identified products, processes, systems, or persons comply with established and identified requirements as performed and confirmed by accredited certifying agents.

(5) CERTIFYING MARK.—The term "certifying mark" means a seal or symbol provided by an accredited certifying agent, upon completion of a successful certification which is applied to the product, process, system, or person, and establishes the extent to which a particular design and implementation meets a set of specified security standards.

(6) CRITICAL INFORMATION AND COMMUNICATIONS TECHNOLOGY.—The term "critical information and communications technology" means information and communications technology that is in use in critical infrastructure sectors and that underpins the resilience of national critical functions, as determined by the Secretary.

(7) CRITICAL INFRASTRUCTURE.—The term "critical infrastructure" has the meaning given that term in section 1016(e) of the Critical Infrastructure Protection Act of 2001 (42 U.S.C. 5195c(e)).

(8) LABEL.—The term "label" means a clear, visual, and easy to understand symbol or list that conveys specific information about a product's security attributes, characteristics, functionality, components, or other features.

(9) PROGRAM.—The term "Program" means the program administered under subsection (b)(1).

(10) SECRETARY.—The term "Secretary" means the Secretary of Homeland Security.

(b) National Cybersecurity Certification and Labeling Authority.—

(1) ESTABLISHMENT.—There is established a National Cybersecurity Certification and Labeling Authority for the purpose of establishing and administering a voluntary national cybersecurity certification and labeling program for critical information and communications technology in order to bolster the resilience of the networks and critical infrastructure of the United States.

(2) PROGRAMS.—

(A) ACCREDITATION OF CERTIFYING AGENTS.—As part of the Program, the Authority shall define and publish a process whereby governmental and nongovernmental entities may apply to become accredited certifying agents for the certification of specific critical information and communications technology, including—

(i) smartphones;

(ii) tablets;

(iii) laptop computers;

(iv) operating systems;

(v) routers;

(vi) software-as-a-service;

(vii) infrastructure-as-a-service;

(viii) platform-as-a-service;

(ix) programmable logic controllers;

(x) intelligent electronic devices; and

(xi) programmable automation controllers.

(B) IDENTIFICATION OF STANDARDS, FRAMEWORKS, AND BENCHMARKS.—As part of the Program, the Authority shall work in coordination with accredited certifying agents, the Secretary, and subject matter experts from the Federal Government, academia, nongovernmental organizations, and the private sector, including with the International Organization for Standardization and other international standards bodies, to—

(i) identify and harmonize common security standards, frameworks, and benchmarks against which the security of critical information and

communications technologies may be measured; and

(ii) identify cybersecurity certification programs that are available and accepted by industry and consumers.

(C) PRODUCT CERTIFICATION.—As part of the Program, the Authority, in consultation with the Secretary and other experts from the Federal Government, academia, nongovernmental organizations, and the private sector, shall—

(i) develop, and disseminate to accredited certifying agents, guidelines to standardize the presentation and issuance of certifications and certifying marks to communicate the level of security, as specified in applicable voluntary standards, for critical information and communications technologies;

(ii) develop, or permit accredited certifying agents to develop, certification criteria for critical information and communications technologies based on identified security standards, frameworks, and benchmarks, through the work conducted under subparagraph (B);

(iii) permit accredited certifying agents to issue certifications and certifying marks for critical information and communications technology that meet and comply with security standards, frameworks, and benchmarks identified through the work conducted under subparagraph (B);

(iv) permit a manufacturer or distributor of critical information and communications technology to display a certificate reflecting the extent to which the critical information and communications technology meets security standards, frameworks, and benchmarks identified through the work conducted under subparagraph (B);

(v) develop a post-market surveillance program to support the monitoring of participants in the Program and removal of the certification of a critical information and communications technology as a critical information and communications technology certified under the Program if the manufacturer of the certified critical information and communications technology falls out of conformity with the benchmarks security standards, frameworks, or benchmarks identified through the work conducted under subparagraph (B) for the critical information and communications technology;

(vi) work to enhance public awareness of the certification and labeling efforts of the Authority and accredited certifying agents, including through public outreach, education, research and development, and other means; and

(vii) publicly display a list of labels and certified critical information and communications technology, along with their respective certification information.

(D) CERTIFICATIONS.—

(i) IN GENERAL.—A certification shall remain valid for not less than 1 year from the date of issuance and not more than 5 years from the date of issuance, as determined by the accredited certifying agent.

(ii) CLASSES OF CONFORMITY ASSESSMENT.—In developing the guidelines and

criteria required under subparagraph (C)(i), the Authority shall designate at least 3 classes of conformity assessment, including the following:

(I) For critical information and communications technology which the product manufacturer or service provider attests meets the criteria for a certification, self-declaration of conformity.

(II) For critical information and communications technology products and services that have undergone conformity assessment, including a security evaluation and testing by an accredited certifying agent, third-party certification of conformity.

(III) For critical information and communications technology that has undergone testing by a third-party testing laboratory, as approved by the Authority, test-based confirmation of conformity.

(E) PRODUCT LABELING.—The Authority, in consultation with the Secretary and other experts from the Federal Government, academia, nongovernmental organizations, and the private sector, shall—

(i) collaborate with the private sector to standardize language and define a labeling schema, that may developed by accredited certifying agents, to provide transparent information on the security characteristics and constituent components of a software or hardware product; and

(ii) establish a mechanism by which product developers can provide this information for both product labeling and public posting.

(3) ENFORCEMENT.—

(A) IN GENERAL.—It shall be unlawful for a product manufacturer, distributor, or seller to—

(i) falsely attest to, or falsify an audit or test for, a security standard, framework, or benchmark for certification;

(ii) intentionally mislabel a product; or

(iii) fail to maintain the security standard, framework, or benchmark to which the manufacturer, distributor, or seller attested.

(B) ENFORCEMENT BY FEDERAL TRADE COMMISSION.—

(i) UNFAIR OR DECEPTIVE ACTS OR PRACTICES.—A violation of subparagraph (A) shall be treated as an unfair and deceptive act or practice in violation of a regulation under section 18(a)(1)(B) of the Federal Trade Commission Act (15 U.S.C. 57a(a)(1)(B)) regarding unfair or deceptive acts or practices.

(ii) POWERS OF COMMISSION.—

(I) IN GENERAL.—The Federal Trade Commission shall enforce this paragraph in the same manner, by the same means, and with the same jurisdiction, powers, and duties as though all applicable terms and provisions of the Federal Trade Commission Act (15 U.S.C. 41 et seq.) were incorporated into and made a part of this paragraph.

(II) PRIVILEGES AND IMMUNITIES.—Any person who violates this paragraph shall be subject to the penalties and entitled to the privileges and immunities provided in the Federal Trade Commission Act (15 U.S.C. 41 et seq.).

(c) Selection of the Authority.—

(1) SELECTION.—The Secretary shall issue a notice of funding opportunity and select, on a competitive basis, a nonprofit, nongovernmental organization to serve as the Authority for a period of 5 years.

(2) ELIGIBILITY FOR SELECTION.—The Secretary may only select an organization to serve as the Authority if such organization—

(A) is a nongovernmental, nonprofit organization that is—

(i) exempt from taxation under section 501(a) of the Internal Revenue Code of 1986; and

(ii) described in sections 501(c)(3) and 170(b)(1)(A)(vi) of that Code;

(B) has a demonstrable track record of development and oversight of accreditation programs and work on cybersecurity and information security standards, frameworks, and benchmarks; and

(C) possesses requisite staffing and expertise, with demonstrable prior experience in the development and oversight of accreditation programs, as well as technology security or safety standards, frameworks, and benchmarks, as well as certification.

(3) APPLICATION.—The Secretary shall establish a process by which a nonprofit, nongovernmental organization that seeks to be selected as the Authority may apply for consideration.

(4) PROGRAM EVALUATION.—Not later than the date that is 4 years after the initial selection pursuant paragraph (1), and every 4 years thereafter, the Secretary shall—

(A) assess the effectiveness of the labels and certificates produced by the Authority, including—

(i) assessing the costs to businesses that manufacture critical information and communications technology participating in the Program;

(ii) evaluating the level of participation in the Program by businesses that manufacture critical information and communications technology; and

(iii) assessing the level of public awareness and consumer awareness of the label;

(B) audit the impartiality and fairness of the Authority's activities conducted under this section;

(C) issue a public report on the assessment most recently carried out under subparagraph (A) and the audit most recently carried out under subparagraph (B); and

(D) brief Congress on the findings of the Secretary with respect to the most recent assessment under subparagraph (A) and the most recent audit under subparagraph (B).

(5) RENEWAL.—After the initial selection pursuant to paragraph (1), the Secretary shall,

every 5 years—

(A) accept applications from nonprofit, nongovernmental organizations seeking selection as the Authority; and

(B) following competitive consideration of all applications—

(i) renew the selection of the organization serving as the Authority; or

(ii) select another applicant organization to serve as the Authority.

(d) Authorization of Appropriations.—There are authorized to be appropriated to carry out this section $25,000,000 for each of fiscal years 2022 through 2026.