A BILL

To require the Secretary of Commerce to issue standards with respect to chip security mechanisms for integrated circuit products, 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 "Chip Security Act".

SEC. 2. SENSE OF CONGRESS.

It is the sense of Congress that—

(1) technology developed in the United States should serve as the foundation for the global ecosystem of artificial intelligence to advance the foreign policy and national security objectives of the United States and allies and partners of the United States;

(2) the United States can foster goodwill, strengthen relationships, and support innovative research around the world by providing allies and partners of the United States with advanced computing capabilities;

(3) advanced integrated circuits and computing hardware that is exported from the United States must be protected from diversion, theft, and other unauthorized use or exploitation in order to bolster the competitiveness of the United States and protect the national security of the United States;

(4) illegal diversion of advanced integrated circuits and computing hardware, particularly diversion to the People's Republic of China, is a significant and growing issue that undermines United States' export controls and threatens United States' national security;

(54) implementing chip security mechanisms will improve compliance with the export control laws of the United States, assist allies and partners with guarding computing hardware, and enhance protections from bad actors

looking to access, divert, or tamper with advanced integrated circuits and computing hardware; and

(6~~5~~) implementing chip security mechanisms may help with the detection of smuggling or exploitation of advanced integrated circuits and computing hardware, thereby allowing for increased flexibility in export controls and opening the door for more international partners to receive streamlined and larger shipments of advanced computing hardware.

SEC. 3. DEFINITIONS.

In this Act:

(1) APPROPRIATE CONGRESSIONAL COMMITTEES.—The term "appropriate congressional committees" means—

(A) the Committee on Banking, Housing, and Urban Affairs of the Senate; and

(B) the Committee on Foreign Affairs of the House of Representatives.

(2) CHIP SECURITY MECHANISM.—The term "chip security mechanism" means a software-, firmware-, or hardware-enabled security mechanism or a physical security mechanism, such as, but not limited to:~~.~~

(A) Periodic on-site audits or inventories at the end-user's approved destination for the covered integrated circuit product;

(B) Periodic certifications by a U.S.-headquartered entity, or its subsidiaries, confirming that all covered integrated circuit products are accounted for, provided the Secretary determines that the U.S.-headquartered entity or its subsidiaries verifiably certifies that the U.S.-headquartered entity or its subsidiaries maintain continuous and sufficiently secure control and operation of said covered integrated circuit products;

(C) Ping-based location verification through a trusted, landmark server utilizing secure software or firmware enabled mechanisms; or

(D) various other mechanisms that the Secretary determines can verifiably demonstrate that the covered integrated circuit product can achieve geolocation verification with significant confidence.

(3) COVERED INTEGRATED CIRCUIT PRODUCT.—The term "covered integrated circuit product" means—

(A) an integrated circuit classified under Export Control Classification Number 3A090 or 3A001.z;

(B) a computer or other product classified under Export Control Classification Number 4A090 or 4A003.z; or

(C) an integrated circuit or computer or a product containing an integrated circuit or computer that is classified under an Export Control Classification Number that is a successor or substantially similar to the numbers listed in subparagraphs (A) and (B).

(D) the Secretary is authorized to modify the covered integrated circuit product definition of this Act described in subparagraphs (A) through (C) to ensure only integrated circuits, computers, electronic assembly, or components marketed for artificial intelligence datacenter use are subject to the requirements of this Act.

(4) EXPORT.—The term "export" has the meaning given that term in section 1742(3) of the Export Control Reform Act of 2018 (50 U.S.C. 4801(3)).

(5) IN-COUNTRY TRANSFER.—The term "in-country transfer" has the meaning given that term in section 1742(6) of the Export Control Reform Act of 2018 (50 U.S.C. 4801(6)).

(6) REEXPORT.—The term "reexport" has the meaning given that term in section 1742(9) of the Export Control Reform Act of 2018 (50 U.S.C. 4801(9)).

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

SEC. 4. REQUIREMENTS FOR SECURITY MECHANISMS FOR EXPORT OF INTEGRATED CIRCUIT PRODUCTS.

(a) PRIMARY REQUIREMENTS FOR CHIP SECURITY MECHANISMS.—

(1) IN GENERAL.—Not later than ~~180 days~~one year after the date of the enactment of this Act, the Secretary shall require any covered integrated circuit product ~~to be outfitted with~~be secured by chip security mechanisms that implement location verification, using techniques that are feasible and appropriate on such date of enactment, before it is exported, reexported, or in-country transferred to or in a foreign country.

(2) NOTIFICATION REQUIREMENT.—Not later than ~~180 days~~one year after the date of the enactment of this Act, the Secretary shall require any person that has received a license or other authorization under the Export Control Reform Act of 2018 (50 U.S.C. 4811 et seq.) ~~-~~to export, reexport, or in-country transfer a covered integrated circuit product to promptly report to the Under Secretary of Industry and Security, if the person obtains credible information that the product—

(A) is in a location other than the location specified in the application for the license or other authorization;

(B) has been diverted to a user other than the user specified in the application; or

(C) has been subjected to tampering or an attempt at tampering, including efforts to disable, spoof, falsify, manipulate, mislead, or circumvent location verification mechanisms or other chip security mechanisms.

(b) DEVELOPMENT OF ~~SECONDARY REQUIREMENTS~~ENHANCEMENTS FOR CHIP SECURITY MECHANISMS.—

(1) ASSESSMENT.—

(A) IN GENERAL.—Not later than two~~one~~ years after the date of the enactment of this Act, the Secretary shall—

(i) conduct an assessment, in robust consultation with the public in a manner determined appropriate by the Secretary and in consultation with any additional relevant Federal agencies or offices the Secretary determines, to identify what ~~additional~~

~~mechanisms~~enhancement, if any, ~~should be added to the primary~~should be used to improve the chip security mechanisms required under subsection (a)(1)—

(I) to enhance compliance with the requirements of the Export Control Reform Act of 2018;

(II) to ~~prevent, hinder, and~~ detect the ~~unauthorized use, access, or exploitation of~~diversion of covered integrated circuit products;

(III) to identify and monitor smuggling intermediaries; and

(IV) to achieve any national security or foreign policy objective of the United States that the Secretary considers appropriate; and

(ii) if the Secretary identifies any such enhanced chip security mechanism, develop ~~requirements~~ incentives for facilitating industry-wide incorporation of said enhanced chip security mechanism for ~~outfitting~~ covered integrated circuit products,~~.~~ including by potentially developing expedited license processing procedures for covered integrated circuit products that utilize ~~with that mechanism~~the enhanced chip security mechanisms. ~~.~~

(B) ELEMENTS.—The assessment required by paragraph (1) shall include—

(i) an examination of the feasibility, scalability, reliability, and effectiveness of —

~~(I)~~ methods and strategies that prevent the tampering, disabling, or other manipulating of covered integrated circuit products; or

~~(II) workload verification methods;~~

~~(III) methods to modify the functionality of covered integrated circuit products that have been illicitly acquired; and~~

~~(IV~~

(I) ~~)~~any other method the Secretary determines appropriate for the prevention of unauthorized use, access, or exploitation of covered integrated circuit products;

(ii) an analysis of—

(I) the potential costs associated with implementing each method examined under clause (i), including an analysis of—

(aa) the potential impact of the method on the performance of covered integrated circuit products; and

(bb) the potential for the introduction of new vulnerabilities into the products;

(II) the potential benefits of implementing the methods examined under clause (i), including an analysis of the potential increase—

(aa) in compliance of covered integrated circuit products with the requirements of the Export Control Reform Act of 2018; and

(bb) in ~~detecting, hindering, and preventing unauthorized use, access, or exploitation~~detecting and deterring illegal diversion of the covered integrated circuit products; and

(III) the susceptibility of the methods examined under clause (i) to tampering, disabling, or other forms of manipulation; and

(iii) an estimate of the expected costs to implement at-scale methods to tamper with, disable, or manipulate a covered integrated circuit product, or otherwise circumvent the methods examined under clause (i).

(2) REPORT TO CONGRESS.—

(A) IN GENERAL.—Not later than one year after the date of the enactment of this Act, the Secretary shall submit to the appropriate congressional committees a report on the results of the assessment required by paragraph (1), including—

(i) an identification of the chip security mechanisms, if any, to be included in the requirements for ~~secondary~~ enhanced chip security mechanisms; ~~and~~

(i~~i~~i) if applicable, a roadmap for the timely implementation of the ~~secondary~~ enhanced chip security mechanisms.

(B) FORM.—The report required by paragraph (1) shall be submitted in unclassified form, but may include a classified annex.

(3) IMPLEMENTATION.—

(A) IN GENERAL.—If any mechanisms are determined by the Secretary to be appropriate, the Secretary shall, not later than 2 years after the date on which the Secretary completes the assessment required by paragraph (1), require any covered integrated circuit product to ~~be outfitted~~ incorporate~~with~~ the enhanced~~secondary~~ chip security mechanisms identified pursuant to paragraph (1)(A) before the product is exported, reexported, or in-country transferred to or in a foreign country.

(B) PRIVACY & ~~.~~ CYBERSECURITY. —In implementing requirements for ~~secondary~~ enhanced chip security mechanisms under subparagraph (A), the Secretary shall prioritize mitigation of confidentiality and cybersecurity risk.~~.~~

(c) ENFORCEMENT AUTHORITY.—In carrying out this section, the Secretary may—

(1) verify, in a manner the Secretary determines appropriate, the ownership and location of a covered integrated circuit product that has been exported, reexported, or in-country transferred to or in a foreign country;

(2) maintain a record of covered integrated circuit products and include in the record the location and current end-user of each such product; and

(3) require any person who has been granted a license or other authorization under the Export Control Reform Act of 2018 to export, reexport, or in-country transfer a covered integrated circuit product to provide the information needed to maintain the record.

(d) ANNUAL ASSESSMENT AND REPORT ON NEW CHIP SECURITY MECHANISMS.—Not later than 2 years after the date of the enactment of this Act, and annually thereafter for 3 years, the Secretary shall—

(1) conduct an assessment of new chip security mechanisms that have been developed in the year preceding the date of the assessment; and

(2) submit to the appropriate congressional committees a report that includes—

(A) a summary of the results of the assessment required by paragraph (1);

(B) an evaluation of whether any of the new mechanisms assessed under paragraph (1) should be added to or replace any of the existing requirements for ~~secondary~~ enhanced chip security mechanisms developed under subsection (b)(1); and

(C) any recommendations for modifications to relevant export controls to allow for more flexibility with respect to the countries to or in which covered integrated circuit products may be exported, reexported, or in-country transferred if the products include chip security mechanisms that meet the requirements developed under subsection (b)(1).

(e) Foreign Competitiveness Assessment.

(1) The Secretary shall annually assess the competitiveness of foreign covered integrated circuit products in relation to U.S. covered integrated circuit products.

(2) The Secretary is authorized to issue a Foreign Direct Product Rule for the covered integrated circuit products if the Secretary determines that it is necessary to prevent covered integrated circuit product diversion, ensure

global competitiveness of U.S. covered integrated circuit products, or otherwise achieve the goals of this Act.

(3) The Secretary is authorized to waive any requirements of this Act after issuing a Foreign Direct Product Rule if the Secretary determines the Foreign Direct Product Rule insufficiently addressed issues arising from the presence of sufficient volume of foreign covered integrated circuit products that undermined the goals of this Act.

(A) Congressional Notification.—At least seven days prior to exercising the waiver described in subparagraph (3), the Secretary shall provide a written notification to the appropriate congressional committees containing detailed quantitative analysis demonstrating that the Foreign Direct Product Rule insufficiently addressed issues arising from the presence of sufficient volume of foreign covered integrated circuit products.

(f~~e~~) RULE OF CONSTRUCTION.—Nothing in this Act shall be construed as directing the Secretary of Commerce to

(1) require any chip security mechanisms that may hinder the capability or functionality of a covered integrated circuit product, such as a kill switch or geofencing mechanism, or undermine the cybersecurity of the covered integrated circuit product;

(2) mandate the incorporation of a hardware-based location verification mechanism on a covered integrated circuit product;~~.~~

(3) consider any requirements of this Act as applicable to a person that fabricates covered integrated circuit products, unless said person also designs the respective covered integrated circuit products;

(4) require chip security mechanisms for exports of integrated circuits, computers, electronic assemblies, or components that are not marketed for artificial intelligence datacenter use.