AMENDMENT IN THE NATURE OF A SUBSTITUTE TO H.R. 3447 OFFERED BY MR. HUIZENGA OF MICHIGAN

Strike all after the enacting clause and insert the following:

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 illegal diversion to the People's Republic of China and the Russian Federation, is a significant and growing issue that undermines the United States' export controls and threatens the United States' national security;

(5) implementing chip security mechanisms will improve enforcement of 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) 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, including—

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

(B) periodic attestations 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, operation, repair (to the extent such repair is conducted by or under the direct super-

vision of the U.S.-headquartered entity or its subsidiaries), and disposal of the 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, or combinations of mechanisms, that the Secretary determines can verifiably demonstrate with significant confidence that the covered integrated circuit product has not been illegally diverted to a destination of concern.

(3) COVERED INTEGRATED CIRCUIT PRODUCT.—

(A) IN GENERAL.—The term ''covered integrated circuit product'' means a certain integrated circuit, computer, or other product classified under Export Control Classification Number 3A090, 4A090, 5A002.z, related .z Export Control Classification Numbers, or other functionally equivalent or substantially similar items.

(B) MODIFICATION.—The Secretary shall routinely modify the definition of the term

''covered integrated circuit product'' under subparagraph (A) for the purposes of this Act to ensure only integrated circuits, computers, electronic assembly, or components designed or marketed for datacenter use are subject to the requirements of this Act.

(C) EXCLUSION.—The term ''covered integrated circuit'' does not include—

(i) covered integrated circuits or products containing a covered integrated circuit that are not designed or marketed for use in a data center;

(ii) microprocessor microcircuits, such as central processing units, that are not graphics processing units or similar products; or

(iii) network switch integrated circuits whose dominant function is routing traffic over a computing network.

(4) DESTINATION OF CONCERN.—The term ''destination of concern'' means—

(A) a country subject to a U.S. arms embargo listed under Country Group D:5 in Supplement No. 1 to Part 740 of the Export Administration Regulations under parts 730

through 774 of title 15, Code of Federal Regulations; or

(B) any other country determined by the Secretary.

(5) EXPORT, IN-COUNTRY TRANSFER, AND REEXPORT.—The terms ''export'', ''in-country transfer'', and ''reexport'' have the meanings given those terms in section 1742 of the Export Control Reform Act of 2018 (50 U.S.C. 4801).

(6) SECRETARY.—The term ''Secretary'' means the Secretary of Commerce.

SEC. 4. RULES OF CONSTRUCTION.

Nothing in this Act may be construed to direct the Secretary 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 meaningfully undermine the cybersecurity of the covered integrated circuit product;

(2) mandate the incorporation of a location verification mechanism on a covered integrated circuit product that requires physical changes to hardware;

(3) consider any chip security mechanism requirements of this Act as applicable to a person that fabricates covered integrated circuit products, unless the 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 designed or marketed for artificial intelligence datacenter use;

(5) limit any other enforcement authority of the Secretary or the head of any other Federal department or agency under the Export Control Reform Act of 2018 (50 U.S.C. 4801 et seq.) or any other provision of law; or

(6) apply any requirements or regulations under this Act to any covered integrated circuit products in the United States.

SEC. 5. INITIAL REPORT TO CONGRESS ON CHIP SECURITY MECHANISMS.

(a) ASSESSMENT.—On the date of the enactment of this Act, the Secretary, in consultation with the Secretary of State, the Secretary of Defense, and the Secretary of Energy and in robust consultation with the public in a manner determined appropriate by the Secretary and in

consultation with the heads of other relevant Federal departments and agencies, shall initiate an assessment to—

(1) identify potential chip security mechanisms to enable reliable verification of whether a covered integrated circuit product has been illegally diverted or accessed;

(2) develop incentives for facilitating industry-wide incorporation of such chip security mechanisms;

(3) conduct an analysis of the potential costs associated with implementing such chip security mechanisms; and

(4) recommend a set of chip security mechanisms that would effectively detect diversion and smuggling and is technically feasible, cost-effective, and ensures the technology leadership of the United States.

(b) STAKEHOLDER ENGAGEMENT.—In carrying out the requirements under subsection (a), the Secretary shall undertake a robust stakeholder engagement process to inform the development and implementation of chip security mechanisms, which shall include—

(1) soliciting input from relevant stakeholders, including—

(A) private sector entities involved in the covered integrated circuit product supply chain;

(B) experts in software, firmware, hardware security, cybersecurity, privacy, export compliance, national security, and advanced artificial intelligence; and

(C) individuals from academic institutions, federally funded research and development centers, Federal departments and agencies, and other research organizations with relevant expertise; and

(2) incorporating stakeholder feedback to ensure that required chip security mechanisms are operationally effective, scalable, and aligned with best practices in security, privacy, and export compliance.

(c) REPORT TO CONGRESS.—

(1) IN GENERAL.—Not later than 210 days 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 subsection (a), including—

(A) an identification of the chip security mechanisms the Secretary plans to propose pursuant to implementing section 6;

(B) an identification of future research and development directions that could be used to enhance robustness of chip security mechanisms and incentives to promote such research and development directions;

(C) a roadmap for the timely implementation of the chip security mechanisms; and

(D) any recommendations for potential 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.

(2) FORM.—The report required in this subsection shall be submitted in unclassified form but may include a classified annex.

SEC. 6. REQUIREMENTS FOR CHIP SECURITY MECHANISMS FOR EXPORT, RE-EXPORT, OR IN-COUNTRY TRANSFER OF COVERED INTEGRATED CIRCUIT PRODUCTS.

(a) PRIMARY REQUIREMENTS.—

(1) IN GENERAL.—Not later than one year after the date of the enactment of this Act, the Secretary, in consultation with the Secretary of State,

the Secretary of Defense, and the Secretary of Energy, shall require any covered integrated circuit product that is exported, reexported, or in-country-transferred to or within a foreign country to be secured by a chip security mechanism that enables reliable verification of whether the product has been illegally diverted to destinations of concern, to the maximum extent practicable, using techniques that are feasible and appropriate on such date of enactment.

(2) PROPOSED REGULATIONS.—

(A) IN GENERAL.—Not later than 270 days after the date of the enactment of this Act, the Secretary shall promulgate proposed regulations implementing the requirements of paragraph (1).

(B) REQUIREMENTS.—In promulgating the proposed regulations under subparagraph (A), the Secretary shall—

(i) solicit public feedback on potential guidance to clarify the categories of persons subject to this requirement, how information should be securely shared between entities, and the procedures for submission of such notifications, in order to

ensure clarity regarding compliance obligations and implementation; and

(ii) issue guidance to clarify how the regulations can be applied in nations with data localization laws or data privacy laws, providing flexibility if such laws require novel or flexible approaches.

(3) FINAL RULE.—Not later than one year after the date of the enactment of this Act, the Secretary, in robust consultation with the public in a manner determined appropriate by the Secretary and in consultation with the heads of other relevant Federal departments and agencies, shall promulgate a final rule that includes a reporting requirement to inform the Bureau of Industry and Security of the Department of Commerce whenever chip security mechanisms fail to confirm that any covered integrated circuit product has not been illegally diverted to a destination of concern, taking into account reasonable time for persons to verify or repair the chip security mechanism, identified in the final rule, including instances in which there is evidence that a product has been subjected to tampering or an attempt at tampering, including efforts to disable,

spoof, falsify, manipulate, mislead, or circumvent chip security mechanisms.

(4) STAKEHOLDER ENGAGEMENT.—In carrying out this subsection, the Secretary shall undertake a robust stakeholder engagement process to inform the development and implementation of chip security mechanisms, which shall include—

(A) soliciting input from relevant stakeholders, including—

(i) private sector entities involved in the covered integrated circuit product supply chain;

(ii) experts in software, firmware, and hardware security, cybersecurity, privacy, export compliance, national security, and advanced artificial intelligence; and

(iii) individuals from academic institutions, federally funded research and development centers, Federal departments and agencies, and other research organizations with relevant expertise; and

(B) incorporating stakeholder feedback to ensure that required chip security mechanisms are operationally effective, scalable, and aligned

with best practices in security, privacy, and export compliance.

(b) ENHANCEMENTS TO CHIP SECURITY MECHANISMS.—

(1) ASSESSMENT.—

(A) IN GENERAL.—Not later than two years after the date of the enactment of this Act, and annually thereafter for three years, the Secretary, in consultation with the Secretary of State, the Secretary of Defense, and the Secretary of Energy, shall—

(i) conduct an assessment, in robust consultation with the public in a manner determined appropriate by the Secretary and in consultation with the heads of other relevant Federal departments and agencies, to identify what enhancements, if any, should be used to improve the chip security mechanisms implemented under subsection (a)(1)—

(I) to enhance compliance with the requirements of the Export Control Reform Act of 2018 (50 U.S.C. 4801 et seq.);

(II) to detect the illegal diversion of covered integrated circuit products;

(III) to identify and monitor smuggling intermediaries;

(IV) to ensure United States technology leadership;

(V) to ensure the orderly and effective implementation of the chip security mechanism; and

(VI) to address industry feedback about the implementation of the chip security mechanism;

(ii) if the Secretary identifies any such enhancements, develop incentives for facilitating industry-wide incorporation of such enhancements for covered integrated circuit products; and

(iii) where necessary, to expedite the implementation of such enhancements and identify and support research activities, such as—

(I) updating and clarifying relevant vulnerability and threat models;

(II) developing definitions, assets, and other practices to support

traceability and provenance of materials and data across the product lifecycle;

(III) developing updated databases of existing trust and assurance data practices; and

(IV) developing practices for implementing chip security mechanisms and sharing relevant information across the product life cycle while protecting confidential intellectual property.

(B) ELEMENTS.—The assessment required by subparagraph (A) shall include—

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

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

(II) 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 (50 U.S.C. 4801 et seq.);

(bb) in detecting and deterring illegal diversion of the covered integrated circuit products; and

(cc) in enhancing persons' global inventory management; 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 two years after the date of the enactment of this Act, and annually thereafter for three years, 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 enhanced chip security mechanisms;

(ii) an identification of research and development directions that could be used to improve the robustness of chip security mechanisms and incentives to promote such research and development directions;

(iii) if applicable, a roadmap for the timely implementation of the enhanced chip security mechanisms; and

(iv) 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 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 enhanced chip security mechanisms identified pursuant to paragraph (1)(A) are determined by the Secretary to be appropriate, the Secretary may, not later than two years after the date on which the

Secretary completes the assessment required by paragraph (1), require any covered integrated circuit product to incorporate the enhanced chip security mechanisms, or for additional mechanisms to be otherwise implemented, at the time the product is exported, reexported, or in-country transferred to or in a foreign country.

(B) PRIVACY AND CYBERSECURITY.—In assessing and developing requirements for enhanced chip security mechanisms under this subsection, the Secretary shall prioritize mitigation of confidentiality and cybersecurity risk.

(c) ENFORCEMENT AUTHORITY.—In addition to the penalty and enforcement authorities granted to the Secretary under the Export Control Reform Act of 2018 (50 U.S.C. 4801 et seq.) or otherwise provided by law, 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 involved in the design, manufacture, sale, physical security, oversight, distribution, export, or licensed transfer of a covered integrated circuit product being exported, re-exported, or in-country-transferred to a foreign country to provide the information needed to maintain the record (such as essential information relating to the chip security mechanisms, or the end-user of covered integrated circuit products located outside of the United States).

(d) FOREIGN COMPETITIVENESS ASSESSMENT AND RELATED AUTHORITIES.—

(1) IN GENERAL.—The Secretary shall annually assess the competitiveness of foreign covered integrated circuit products in relation to United States covered integrated circuit products.

(2) WAIVER.—The Secretary, in consultation with the Secretary of State, the Secretary of Defense, and the Secretary of Energy, is authorized to waive any requirements of this Act if the Secretary, in consultation with such Secretaries, determines that the implementation of chip security mechanisms poses an undue burden on United States competitiveness, is inconsistent with the national security interests of the United States, and that exercising any

and all authorities under the Export Control Reform Act of 2018 (50 U.S.C. 4801 et seq.) insufficiently addressed issues arising from the presence of sufficient volume of foreign covered integrated circuit products not covered by the requirements of this Act.

(3) CONGRESSIONAL NOTIFICATION.—At least 30 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 the rationale for the waiver and that exercising any and all authorities under the Export Control Reform Act of 2018 (50 U.S.C. 4801 et seq.) insufficiently addressed issues arising from the presence of sufficient volume of foreign covered integrated circuit products not covered by the requirements of this Act.

(e) ENFORCEMENT.—A violation of any provision of this Act, or of any regulation, order, license, or other authorization issued pursuant to this Act shall be deemed a violation of the Export Control Reform Act of 2018 (50 U.S.C. 4801 et seq.).

(f) ADMINISTRATIVE PROCEDURES.—The provisions of section 1762 of the Export Control Reform Act of 2018

(50 U.S.C. 4821) shall apply to this Act in the same manner and to the same extent as such provisions apply to the Export Control Reform Act of 2018.