

AMENDMENT TO RULES COMM. PRINT 119–33
OFFERED BY MR. HUIZENGA OF MICHIGAN

Add at the end of subtitle A of title XVII the following:

1 **SEC. 17 ____ . CHIP SECURITY.**

2 (a) INITIAL REPORT TO CONGRESS ON CHIP SECURITY MECHANISMS.—

3 (1) 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—

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

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

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

4 (D) recommend a set of chip security
5 mechanisms that would effectively detect diver-
6 sion and smuggling and is technically feasible,
7 cost-effective, and ensures the technology lead-
8 ership of the United States.

9 (2) STAKEHOLDER ENGAGEMENT.—In carrying
10 out the requirements under paragraph (1), the Sec-
11 retary shall undertake a robust stakeholder engage-
12 ment process to inform the development and imple-
13 mentation of chip security mechanisms, which shall
14 include—

15 (A) soliciting input from relevant stake-
16 holders, including—

17 (i) private sector entities involved in
18 the covered integrated circuit product sup-
19 ply chain;

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

24 (iii) individuals from academic institu-
25 tions, federally funded research and devel-

1 opment centers, Federal departments and
2 agencies, and other research organizations
3 with relevant expertise; and

4 (B) incorporating stakeholder feedback to
5 ensure that required chip security mechanisms
6 are operationally effective, scalable, and aligned
7 with best practices in security, privacy, and ex-
8 port compliance.

9 (3) REPORT TO CONGRESS.—

10 (A) IN GENERAL.—Not later than 210
11 days after the date of the enactment of this
12 Act, the Secretary shall submit to the appro-
13 priate congressional committees a report on the
14 results of the assessment required by paragraph
15 (1), including—

16 (i) an identification of the chip secu-
17 rity mechanisms the Secretary plans to
18 propose pursuant to implementing sub-
19 section (b);

20 (ii) an identification of future re-
21 search and development directions that
22 could be used to enhance robustness of
23 chip security mechanisms and incentives to
24 promote such research and development di-
25 rections;

1 (iii) a roadmap for the timely imple-
2 mentation of the chip security mechanisms;
3 and

4 (iv) any recommendations for poten-
5 tial modifications to relevant export con-
6 trols to allow for more flexibility with re-
7 spect to the countries to or in which cov-
8 ered integrated circuit products may be ex-
9 ported, reexported, or in-country-trans-
10 ferred if the products include chip security
11 mechanisms.

12 (B) FORM.—The report required in this
13 paragraph shall be submitted in unclassified
14 form but may include a classified annex.

15 (b) REQUIREMENTS FOR CHIP SECURITY MECHA-
16 NISMS FOR EXPORT, RE-EXPORT, OR IN-COUNTRY TRANS-
17 FER OF COVERED INTEGRATED CIRCUIT PRODUCTS.—

18 (1) PRIMARY REQUIREMENTS.—

19 (A) IN GENERAL.—Not later than one year
20 after the date of the enactment of this Act, the
21 Secretary, in consultation with the Secretary of
22 State, the Secretary of Defense, and the Sec-
23 retary of Energy, shall require any covered inte-
24 grated circuit product that is exported, reex-
25 ported, or in-country-transferred to or within a

1 foreign country to be secured by a chip security
2 mechanism that enables reliable verification of
3 whether the product has been illegally diverted
4 to destinations of concern, to the extent con-
5 sistent with the recommendations submitted
6 pursuant to section (a)(3), using techniques
7 that are feasible and appropriate on such date
8 of enactment.

9 (B) VARYING MECHANISMS PERMITTED.—
10 In implementing the requirements of subpara-
11 graph (A), the Secretary may require chip secu-
12 rity mechanisms that vary by geographical re-
13 gion and by party, as the Secretary deems ap-
14 propriate in light of national security interests,
15 foreign policy objectives, and the assessment of
16 the Secretary of the risk of diversion.

17 (C) PROPOSED REGULATIONS.—

18 (i) IN GENERAL.—Not later than 270
19 days after the date of the enactment of
20 this Act, the Secretary shall promulgate
21 proposed regulations implementing the re-
22 quirements of subparagraph (A).

23 (ii) REQUIREMENTS.—In promul-
24 gating the proposed regulations under
25 clause (i), the Secretary shall—

1 (I) solicit public feedback on po-
2 tential guidance to clarify the cat-
3 egories of persons subject to this re-
4 quirement, how information should be
5 securely shared between entities, and
6 the procedures for submission of such
7 notifications, in order to ensure clarity
8 regarding compliance obligations and
9 implementation; and

10 (II) propose and clarify how the
11 regulations can be applied in nations
12 with data localization laws or data
13 privacy laws, providing flexibility if
14 such laws require novel or flexible ap-
15 proaches.

16 (D) FINAL RULE.—Not later than one
17 year after the date of the enactment of this Act,
18 the Secretary, in robust consultation with the
19 public in a manner determined appropriate by
20 the Secretary and in consultation with the
21 heads of other relevant Federal departments
22 and agencies, shall promulgate a final rule that
23 may include a reporting requirement to inform
24 the Bureau of Industry and Security of the De-
25 partment of Commerce whenever chip security

1 mechanisms fail to confirm that any covered in-
2 tegrated circuit product has not been illegally
3 diverted to a destination of concern, taking into
4 account reasonable time for persons to verify or
5 repair the chip security mechanism, identified
6 in the final rule, including instances in which
7 there is evidence that a product has been sub-
8 jected to tampering or an attempt at tam-
9 pering, including efforts to disable, spoof, fal-
10 sify, manipulate, mislead, or circumvent chip
11 security mechanisms.

12 (E) STAKEHOLDER ENGAGEMENT.—In
13 carrying out this paragraph, the Secretary
14 should undertake a robust stakeholder engage-
15 ment process to inform the development and
16 implementation of chip security mechanisms,
17 which shall include—

18 (i) soliciting input from relevant
19 stakeholders, including—

20 (I) private sector entities involved
21 in the covered integrated circuit prod-
22 uct supply chain;

23 (II) experts in software,
24 firmware, and hardware security, cy-
25 bersecurity, privacy, export compli-

1 ance, national security, and advanced
2 artificial intelligence; and

3 (III) individuals from academic
4 institutions, federally funded research
5 and development centers, Federal de-
6 partments and agencies, and other re-
7 search organizations with relevant ex-
8 pertise; and

9 (ii) incorporating stakeholder feedback
10 to ensure that required chip security mech-
11 anisms are operationally effective, scalable,
12 and aligned with best practices in security,
13 privacy, and export compliance.

14 (2) ENHANCEMENTS TO CHIP SECURITY MECH-
15 ANISMS.—

16 (A) ASSESSMENT.—

17 (i) IN GENERAL.—Not later than two
18 years after the date of the enactment of
19 this Act, and annually thereafter for three
20 years, the Secretary, in consultation with
21 the Secretary of State, the Secretary of
22 Defense, and the Secretary of Energy,
23 shall—

24 (I) conduct an assessment, in ro-
25 bust consultation with the public in a

1 manner determined appropriate by the
2 Secretary and in consultation with the
3 heads of other relevant Federal de-
4 partments and agencies, to identify
5 what enhancements, if any, should be
6 used to improve the chip security
7 mechanisms implemented under para-
8 graph (1)(A)—

9 (aa) to enhance compliance
10 with the requirements of the Ex-
11 port Control Reform Act of 2018
12 (50 U.S.C. 4801 et seq.);

13 (bb) to detect the illegal di-
14 version of covered integrated cir-
15 cuit products;

16 (cc) to identify and monitor
17 smuggling intermediaries;

18 (dd) to ensure United States
19 technology leadership;

20 (ee) to ensure the orderly
21 and effective implementation of
22 the chip security mechanism; and

23 (ff) to address industry feed-
24 back about the implementation of
25 the chip security mechanism;

1 (II) if the Secretary identifies
2 any such enhancements, develop in-
3 centives for facilitating industry-wide
4 incorporation of such enhancements
5 for covered integrated circuit prod-
6 ucts; and

7 (III) where necessary, to expedite
8 the implementation of such enhance-
9 ments and identify and support re-
10 search activities, such as—

11 (aa) updating and clarifying
12 relevant vulnerability and threat
13 models;

14 (bb) developing definitions,
15 assets, and other practices to
16 support traceability and prove-
17 nance of materials and data
18 across the product lifecycle;

19 (cc) developing updated
20 databases of existing trust and
21 assurance data practices; and

22 (dd) developing practices for
23 implementing chip security mech-
24 anisms and sharing relevant in-
25 formation across the product life

1 cycle while protecting confidential
2 intellectual property.

3 (ii) ELEMENTS.—The assessment re-
4 quired by clause (i) shall include—

5 (I) an examination of the feasi-
6 bility, reliability, and effectiveness
7 of—

8 (aa) methods and strategies
9 that prevent the tampering, dis-
10 abling, or other manipulating of
11 covered integrated circuit prod-
12 ucts; and

13 (bb) any other method the
14 Secretary determines appropriate
15 for the prevention of unauthor-
16 ized use, access, or exploitation
17 of covered integrated circuit
18 products;

19 (II) an analysis of—

20 (aa) the potential costs asso-
21 ciated with implementing each
22 method examined under sub-
23 clause (I), including an analysis
24 of—

1 (AA) the potential im-
2 pact of the method on the
3 performance of covered inte-
4 grated circuit products; and
5 (BB) the potential for
6 the introduction of new
7 vulnerabilities into the prod-
8 ucts;
9 (bb) the potential benefits of
10 implementing the methods exam-
11 ined under subclause (I), includ-
12 ing an analysis of the potential
13 increase—
14 (AA) in compliance of
15 covered integrated circuit
16 products with the require-
17 ments of the Export Control
18 Reform Act of 2018 (50
19 U.S.C. 4801 et seq.);
20 (BB) in detecting and
21 deterring illegal diversion of
22 the covered integrated cir-
23 cuit products; and

1 (CC) in enhancing per-
2 sons' global inventory man-
3 agement; and

4 (cc) the susceptibility of the
5 methods examined under sub-
6 clause (I) to tampering, dis-
7 abling, or other forms of manipu-
8 lation; and

9 (III) an estimate of the expected
10 costs to implement at-scale methods
11 to tamper with, disable, or manipulate
12 a covered integrated circuit product,
13 or otherwise circumvent the methods
14 examined under subclause (I).

15 (B) REPORT TO CONGRESS.—

16 (i) IN GENERAL.—Not later than two
17 years after the date of the enactment of
18 this Act, and annually thereafter for three
19 years, the Secretary shall submit to the ap-
20 propriate congressional committees a re-
21 port on the results of the assessment re-
22 quired by subparagraph (A), including—

23 (I) an identification of the chip
24 security mechanisms, if any, to be in-

1 included in the requirements for en-
2 hanced chip security mechanisms;

3 (II) an identification of research
4 and development directions that could
5 be used to improve the robustness of
6 chip security mechanisms and incen-
7 tives to promote such research and
8 development directions;

9 (III) if applicable, a roadmap for
10 the timely implementation of the en-
11 hanced chip security mechanisms; and

12 (IV) any recommendations for
13 modifications to relevant export con-
14 trols to allow for more flexibility with
15 respect to the countries to or in which
16 covered integrated circuit products
17 may be exported, reexported, or in-
18 country-transferred if the products in-
19 clude enhanced chip security mecha-
20 nisms.

21 (ii) FORM.—The report required by
22 subparagraph (A) shall be submitted in
23 unclassified form, but may include a classi-
24 fied annex.

25 (C) IMPLEMENTATION.—

1 (i) IN GENERAL.—If any enhanced
2 chip security mechanisms identified pursu-
3 ant to subparagraph (A)(i) are determined
4 by the Secretary to be appropriate, the
5 Secretary may, not later than two years
6 after the date on which the Secretary com-
7 pletes the assessment required by subpara-
8 graph (A), require any covered integrated
9 circuit product to incorporate the enhanced
10 chip security mechanisms, or for additional
11 mechanisms to be otherwise implemented,
12 at the time the product is exported, reex-
13 ported, or in-country transferred to or in a
14 foreign country.

15 (ii) PRIVACY AND CYBERSECURITY.—
16 In assessing and developing requirements
17 for enhanced chip security mechanisms
18 under this paragraph, the Secretary shall
19 prioritize mitigation of confidentiality and
20 cybersecurity risk.

21 (3) ENFORCEMENT AUTHORITY.—In addition to
22 the penalty and enforcement authorities granted to
23 the Secretary under the Export Control Reform Act
24 of 2018 (50 U.S.C. 4801 et seq.) or otherwise pro-

1 vided by law, in carrying out this subsection, the
2 Secretary may—

3 (A) verify, in a manner the Secretary de-
4 termines appropriate, the ownership and loca-
5 tion of a covered integrated circuit product that
6 has been exported, reexported, or in-country
7 transferred to or in a foreign country;

8 (B) maintain a record of covered inte-
9 grated circuit products and include in the
10 record the location and current end-user of each
11 such product; and

12 (C) require any person involved in the de-
13 sign, manufacture, sale, physical security, over-
14 sight, distribution, export, or licensed transfer
15 of a covered integrated circuit product being ex-
16 ported, re-exported, or in-country-transferred to
17 a foreign country to provide the information
18 needed to maintain the record (such as essential
19 information relating to the chip security mecha-
20 nisms, or the end-user of covered integrated cir-
21 cuit products located outside of the United
22 States).

23 (4) FOREIGN COMPETITIVENESS ASSESSMENT
24 AND RELATED AUTHORITIES.—

1 (A) IN GENERAL.—The Secretary shall an-
2 nually assess the competitiveness of foreign cov-
3 ered integrated circuit products in relation to
4 United States covered integrated circuit prod-
5 ucts.

6 (B) WAIVER.—The Secretary, in consulta-
7 tion with the Secretary of State, the Secretary
8 of Defense, and the Secretary of Energy, is au-
9 thorized to waive any requirements of this sec-
10 tion if the Secretary, in consultation with such
11 Secretaries, determines that the implementation
12 of chip security mechanisms poses an undue
13 burden on United States competitiveness, is in-
14 consistent with the national security interests of
15 the United States, and that exercising any and
16 all authorities under the Export Control Reform
17 Act of 2018 (50 U.S.C. 4801 et seq.) insuffi-
18 ciently addressed issues arising from the pres-
19 ence of sufficient volume of foreign covered in-
20 tegrated circuit products not covered by the re-
21 quirements of this section.

22 (C) CONGRESSIONAL NOTIFICATION.—At
23 least 30 days prior to exercising the waiver de-
24 scribed in subparagraph (B), the Secretary
25 shall provide a written notification to the appro-

1 appropriate congressional committees containing de-
2 tailed quantitative analysis demonstrating the
3 rationale for the waiver and that exercising any
4 and all authorities under the Export Control
5 Reform Act of 2018 (50 U.S.C. 4801 et seq.)
6 insufficiently addressed issues arising from the
7 presence of sufficient volume of foreign covered
8 integrated circuit products not covered by the
9 requirements of this section.

10 (5) ENFORCEMENT.—A violation of any provi-
11 sion of this section, or of any regulation, order, li-
12 cense, or other authorization issued pursuant to this
13 section shall be deemed a violation of the Export
14 Control Reform Act of 2018 (50 U.S.C. 4801 et
15 seq.).

16 (6) ADMINISTRATIVE PROCEDURES.—The pro-
17 visions of section 1761(h) and section 1762 of the
18 Export Control Reform Act of 2018 (50 U.S.C.
19 4801 et seq.) shall apply to this section in the same
20 manner and to the same extent as such provisions
21 apply to the Export Control Reform Act of 2018.

22 (c) RULES OF CONSTRUCTION.—Nothing in this sec-
23 tion may be construed to direct the Secretary to—

24 (1) require any chip security mechanisms that
25 may hinder the capability or functionality of a cov-

1 ered integrated circuit product, such as a kill switch
2 or geofencing mechanism, or meaningfully under-
3 mine the cybersecurity of the covered integrated cir-
4 cuit product;

5 (2) mandate the incorporation of a location
6 verification mechanism on a covered integrated cir-
7 cuit product that requires physical changes to hard-
8 ware;

9 (3) consider any chip security mechanism re-
10 quirements of this section as applicable to a person
11 that fabricates covered integrated circuit products,
12 unless the person also designs the respective covered
13 integrated circuit products;

14 (4) require chip security mechanisms for ex-
15 ports of integrated circuits, computers, electronic as-
16 semblies, or components that are not designed or
17 marketed for artificial intelligence datacenter use;

18 (5) limit any other enforcement authority of the
19 Secretary or the head of any other Federal depart-
20 ment or agency under the Export Control Reform
21 Act of 2018 (50 U.S.C. 4801 et seq.) or any other
22 provision of law; or

23 (6) apply any requirements or regulations under
24 this section to any covered integrated circuit prod-
25 ucts in the United States.

1 (d) ASSESSMENT OF THE PEOPLE'S REPUBLIC OF
2 CHINA'S MILITARY USE OF ARTIFICIAL INTELLIGENCE.—

3 (1) IN GENERAL.—Not later than 180 days
4 after the date of the enactment of this Act, and an-
5 nually thereafter, the Secretary of Defense shall sub-
6 mit to the Committee on Armed Services and the
7 Committee on Foreign Affairs of the House of Rep-
8 resentatives and the Committee on Armed Services
9 and the Committee on Foreign Relations of the Sen-
10 ate a report on the People's Liberation Army Rocket
11 Force use of artificial intelligence, including—

12 (2) REPORT CONTENTS.—The report required
13 in paragraph (1) shall include a detailed explanation
14 of how the People's Liberation Army Rocket Force
15 is using artificial intelligence for its modernization
16 efforts and force posture in the Western Pacific, in-
17 cluding how the People's Liberation Army Rocket
18 Force is exploiting access to United States and allied
19 advanced semiconductor technologies and artificial
20 intelligence.

21 (3) FORM.—The report required in paragraph
22 (1) shall be submitted in unclassified but may in-
23 clude a classified annex.

24 (e) DEFINITIONS.—In this section:

1 (1) The term “appropriate congressional com-
2 mittees” means—

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

5 (B) the Committee on Energy and Com-
6 merce of the House of Representatives; and

7 (C) the Committee on Foreign Affairs of
8 the House of Representatives.

9 (2) The term “chip security mechanism” means
10 a software-, firmware-, or hardware-enabled security
11 mechanism or a physical security mechanism, includ-
12 ing—

13 (A) periodic on-site audits or inventories at
14 the end-user’s approved destination for the cov-
15 ered integrated circuit product;

16 (B) periodic attestations by a United
17 States-headquartered entity, a subsidiary of a
18 United States-headquartered entity, or an enti-
19 ty determined by the Secretary to be reliable,
20 confirming that all covered integrated circuit
21 products are accounted for, provided the Sec-
22 retary determines that the United States-
23 headquartered entity or its subsidiaries
24 verifiably certifies that the United States-
25 headquartered entity or its subsidiaries main-

1 tain continuous and sufficiently secure control,
2 operation, repair (to the extent such repair is
3 conducted by or under the direct supervision of
4 the United States-headquartered entity or its
5 subsidiaries), and disposal of the covered inte-
6 grated circuit products;

7 (C) ping-based location verification
8 through a trusted landmark server utilizing se-
9 cure software- or firmware-enabled mechanisms;
10 or

11 (D) various other mechanisms, or combina-
12 tions of mechanisms, that the Secretary deter-
13 mines can verifiably demonstrate with signifi-
14 cant confidence that the covered integrated cir-
15 cuit product has not been illegally diverted to a
16 destination of concern.

17 (3)(A) The term “covered integrated circuit
18 product” means a certain integrated circuit, com-
19 puter, or other product classified under Export Con-
20 trol Classification Number 3A090, 4A090, 5A002.z,
21 related .z Export Control Classification Numbers, or
22 other functionally equivalent or substantially similar
23 items.

24 (B) The Secretary shall routinely modify the
25 definition of the term “covered integrated circuit

1 product” under subparagraph (A) for the purposes
2 of this section to ensure only integrated circuits,
3 computers, electronic assembly, or components de-
4 signed or marketed for datacenter use are subject to
5 the requirements of this section.

6 (C) The term “covered integrated circuit” does
7 not include—

8 (i) covered integrated circuits or products
9 containing a covered integrated circuit that are
10 not designed or marketed for use in a data cen-
11 ter;

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

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

18 (4) The term “destination of concern” means—

19 (A) a country subject to a United States
20 arms embargo pursuant to section 126.1 of title
21 22, Code of Federal Regulations; or

22 (B) any other country determined by the
23 Secretary.

24 (5) The terms “export”, “in-country transfer”,
25 and “reexport” have the meanings given those terms

1 in section 1742 of the Export Control Reform Act
2 of 2018 (50 U.S.C. 4801).

3 (6) The term “Secretary” means the Secretary
4 of Commerce.

