

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 maximum ex-
5 tent practicable, using techniques that are fea-
6 sible and appropriate on such date of enact-
7 ment.

8 (B) PROPOSED REGULATIONS.—

9 (i) IN GENERAL.—Not later than 270
10 days after the date of the enactment of
11 this Act, the Secretary shall promulgate
12 proposed regulations implementing the re-
13 quirements of subparagraph (A).

14 (ii) REQUIREMENTS.—In promul-
15 gating the proposed regulations under
16 clause (i), the Secretary shall—

17 (I) solicit public feedback on po-
18 tential guidance to clarify the cat-
19 egories of persons subject to this re-
20 quirement, how information should be
21 securely shared between entities, and
22 the procedures for submission of such
23 notifications, in order to ensure clarity
24 regarding compliance obligations and
25 implementation; and

1 (II) issue guidance to clarify how
2 the regulations can be applied in na-
3 tions with data localization laws or
4 data privacy laws, providing flexibility
5 if such laws require novel or flexible
6 approaches.

7 (C) FINAL RULE.—Not later than one year
8 after the date of the enactment of this Act, the
9 Secretary, in robust consultation with the public
10 in a manner determined appropriate by the Sec-
11 retary and in consultation with the heads of
12 other relevant Federal departments and agen-
13 cies, shall promulgate a final rule that includes
14 a reporting requirement to inform the Bureau
15 of Industry and Security of the Department of
16 Commerce whenever chip security mechanisms
17 fail to confirm that any covered integrated cir-
18 cuit product has not been illegally diverted to a
19 destination of concern, taking into account rea-
20 sonable time for persons to verify or repair the
21 chip security mechanism, identified in the final
22 rule, including instances in which there is evi-
23 dence that a product has been subjected to tam-
24 pering or an attempt at tampering, including
25 efforts to disable, spoof, falsify, manipulate,

1 mislead, or circumvent chip security mecha-
2 nisms.

3 (D) STAKEHOLDER ENGAGEMENT.—In
4 carrying out this paragraph, the Secretary shall
5 undertake a robust stakeholder engagement
6 process to inform the development and imple-
7 mentation of chip security mechanisms, which
8 shall include—

9 (i) soliciting input from relevant
10 stakeholders, including—

11 (I) private sector entities involved
12 in the covered integrated circuit prod-
13 uct supply chain;

14 (II) experts in software,
15 firmware, and hardware security, cy-
16 bersecurity, privacy, export compli-
17 ance, national security, and advanced
18 artificial intelligence; and

19 (III) individuals from academic
20 institutions, federally funded research
21 and development centers, Federal de-
22 partments and agencies, and other re-
23 search organizations with relevant ex-
24 pertise; and

1 (ii) incorporating stakeholder feedback
2 to ensure that required chip security mech-
3 anisms are operationally effective, scalable,
4 and aligned with best practices in security,
5 privacy, and export compliance.

6 (2) ENHANCEMENTS TO CHIP SECURITY MECH-
7 ANISMS.—

8 (A) ASSESSMENT.—

9 (i) IN GENERAL.—Not later than two
10 years after the date of the enactment of
11 this Act, and annually thereafter for three
12 years, the Secretary, in consultation with
13 the Secretary of State, the Secretary of
14 Defense, and the Secretary of Energy,
15 shall—

16 (I) conduct an assessment, in ro-
17 bust consultation with the public in a
18 manner determined appropriate by the
19 Secretary and in consultation with the
20 heads of other relevant Federal de-
21 partments and agencies, to identify
22 what enhancements, if any, should be
23 used to improve the chip security
24 mechanisms implemented under para-
25 graph (1)(A)—

- 1 (aa) to enhance compliance
2 with the requirements of the Ex-
3 port Control Reform Act of 2018
4 (50 U.S.C. 4801 et seq.);
- 5 (bb) to detect the illegal di-
6 version of covered integrated cir-
7 cuit products;
- 8 (cc) to identify and monitor
9 smuggling intermediaries;
- 10 (dd) to ensure United States
11 technology leadership;
- 12 (ee) to ensure the orderly
13 and effective implementation of
14 the chip security mechanism; and
- 15 (ff) to address industry feed-
16 back about the implementation of
17 the chip security mechanism;
- 18 (II) if the Secretary identifies
19 any such enhancements, develop in-
20 centives for facilitating industry-wide
21 incorporation of such enhancements
22 for covered integrated circuit prod-
23 ucts; and
- 24 (III) where necessary, to expedite
25 the implementation of such enhance-

1 ments and identify and support re-
2 search activities, such as—

3 (aa) updating and clarifying
4 relevant vulnerability and threat
5 models;

6 (bb) developing definitions,
7 assets, and other practices to
8 support traceability and prove-
9 nance of materials and data
10 across the product lifecycle;

11 (cc) developing updated
12 databases of existing trust and
13 assurance data practices; and

14 (dd) developing practices for
15 implementing chip security mech-
16 anisms and sharing relevant in-
17 formation across the product life
18 cycle while protecting confidential
19 intellectual property.

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

22 (I) an examination of the feasi-
23 bility, reliability, and effectiveness
24 of—

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25

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

(bb) 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—

(aa) the potential costs associated with implementing each method examined under subclause (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;

1 (bb) the potential benefits of
2 implementing the methods exam-
3 ined under subclause (I), includ-
4 ing an analysis of the potential
5 increase—

6 (AA) in compliance of
7 covered integrated circuit
8 products with the require-
9 ments of the Export Control
10 Reform Act of 2018 (50
11 U.S.C. 4801 et seq.);

12 (BB) in detecting and
13 deterring illegal diversion of
14 the covered integrated cir-
15 cuit products; and

16 (CC) in enhancing per-
17 sons' global inventory man-
18 agement; and

19 (cc) the susceptibility of the
20 methods examined under sub-
21 clause (I) to tampering, dis-
22 abling, or other forms of manipu-
23 lation; and

24 (III) an estimate of the expected
25 costs to implement at-scale methods

1 to tamper with, disable, or manipulate
2 a covered integrated circuit product,
3 or otherwise circumvent the methods
4 examined under subclause (I).

5 (B) REPORT TO CONGRESS.—

6 (i) IN GENERAL.—Not later than two
7 years after the date of the enactment of
8 this Act, and annually thereafter for three
9 years, the Secretary shall submit to the ap-
10 propriate congressional committees a re-
11 port on the results of the assessment re-
12 quired by subparagraph (A), including—

13 (I) an identification of the chip
14 security mechanisms, if any, to be in-
15 cluded in the requirements for en-
16 hanced chip security mechanisms;

17 (II) an identification of research
18 and development directions that could
19 be used to improve the robustness of
20 chip security mechanisms and incen-
21 tives to promote such research and
22 development directions;

23 (III) if applicable, a roadmap for
24 the timely implementation of the en-
25 hanced chip security mechanisms; and

1 (IV) any recommendations for
2 modifications to relevant export con-
3 trols to allow for more flexibility with
4 respect to the countries to or in which
5 covered integrated circuit products
6 may be exported, reexported, or in-
7 country-transferred if the products in-
8 clude enhanced chip security mecha-
9 nisms.

10 (ii) FORM.—The report required by
11 subparagraph (A) shall be submitted in
12 unclassified form, but may include a classi-
13 fied annex.

14 (C) IMPLEMENTATION.—

15 (i) IN GENERAL.—If any enhanced
16 chip security mechanisms identified pursu-
17 ant to subparagraph (A)(i) are determined
18 by the Secretary to be appropriate, the
19 Secretary may, not later than two years
20 after the date on which the Secretary com-
21 pletes the assessment required by subpara-
22 graph (A), require any covered integrated
23 circuit product to incorporate the enhanced
24 chip security mechanisms, or for additional
25 mechanisms to be otherwise implemented,

1 at the time the product is exported, reex-
2 ported, or in-country transferred to or in a
3 foreign country.

4 (ii) PRIVACY AND CYBERSECURITY.—
5 In assessing and developing requirements
6 for enhanced chip security mechanisms
7 under this paragraph, the Secretary shall
8 prioritize mitigation of confidentiality and
9 cybersecurity risk.

10 (3) ENFORCEMENT AUTHORITY.—In addition to
11 the penalty and enforcement authorities granted to
12 the Secretary under the Export Control Reform Act
13 of 2018 (50 U.S.C. 4801 et seq.) or otherwise pro-
14 vided by law, in carrying out this subsection, the
15 Secretary may—

16 (A) verify, in a manner the Secretary de-
17 termines appropriate, the ownership and loca-
18 tion of a covered integrated circuit product that
19 has been exported, reexported, or in-country
20 transferred to or in a foreign country;

21 (B) maintain a record of covered inte-
22 grated circuit products and include in the
23 record the location and current end-user of each
24 such product; and

1 (C) require any person involved in the de-
2 sign, manufacture, sale, physical security, over-
3 sight, distribution, export, or licensed transfer
4 of a covered integrated circuit product being ex-
5 ported, re-exported, or in-country-transferred to
6 a foreign country to provide the information
7 needed to maintain the record (such as essential
8 information relating to the chip security mecha-
9 nisms, or the end-user of covered integrated cir-
10 cuit products located outside of the United
11 States).

12 (4) FOREIGN COMPETITIVENESS ASSESSMENT
13 AND RELATED AUTHORITIES.—

14 (A) IN GENERAL.—The Secretary shall an-
15 nually assess the competitiveness of foreign cov-
16 ered integrated circuit products in relation to
17 United States covered integrated circuit prod-
18 ucts.

19 (B) WAIVER.—The Secretary, in consulta-
20 tion with the Secretary of State, the Secretary
21 of Defense, and the Secretary of Energy, is au-
22 thorized to waive any requirements of this sec-
23 tion if the Secretary, in consultation with such
24 Secretaries, determines that the implementation
25 of chip security mechanisms poses an undue

1 burden on United States competitiveness, is in-
2 consistent with the national security interests of
3 the United States, and that exercising any and
4 all authorities under the Export Control Reform
5 Act of 2018 (50 U.S.C. 4801 et seq.) insuffi-
6 ciently addressed issues arising from the pres-
7 ence of sufficient volume of foreign covered in-
8 tegrated circuit products not covered by the re-
9 quirements of this section.

10 (C) CONGRESSIONAL NOTIFICATION.—At
11 least 30 days prior to exercising the waiver de-
12 scribed in subparagraph (B), the Secretary
13 shall provide a written notification to the appro-
14 priate congressional committees containing de-
15 tailed quantitative analysis demonstrating the
16 rationale for the waiver and that exercising any
17 and all authorities under the Export Control
18 Reform Act of 2018 (50 U.S.C. 4801 et seq.)
19 insufficiently addressed issues arising from the
20 presence of sufficient volume of foreign covered
21 integrated circuit products not covered by the
22 requirements of this section.

23 (5) ENFORCEMENT.—A violation of any provi-
24 sion of this section, or of any regulation, order, li-
25 cense, or other authorization issued pursuant to this

1 section shall be deemed a violation of the Export
2 Control Reform Act of 2018 (50 U.S.C. 4801 et
3 seq.).

4 (6) ADMINISTRATIVE PROCEDURES.—The pro-
5 visions of section 1762 of the Export Control Re-
6 form Act of 2018 (50 U.S.C. 4821) shall apply to
7 this section in the same manner and to the same ex-
8 tent as such provisions apply to the Export Control
9 Reform Act of 2018.

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

12 (1) require any chip security mechanisms that
13 may hinder the capability or functionality of a cov-
14 ered integrated circuit product, such as a kill switch
15 or geofencing mechanism, or meaningfully under-
16 mine the cybersecurity of the covered integrated cir-
17 cuit product;

18 (2) mandate the incorporation of a location
19 verification mechanism on a covered integrated cir-
20 cuit product that requires physical changes to hard-
21 ware;

22 (3) consider any chip security mechanism re-
23 quirements of this section as applicable to a person
24 that fabricates covered integrated circuit products,

1 unless the person also designs the respective covered
2 integrated circuit products;

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

7 (5) limit any other enforcement authority of the
8 Secretary or the head of any other Federal depart-
9 ment or agency under the Export Control Reform
10 Act of 2018 (50 U.S.C. 4801 et seq.) or any other
11 provision of law; or

12 (6) apply any requirements or regulations under
13 this section to any covered integrated circuit prod-
14 ucts in the United States.

15 (d) DEFINITIONS.—In this section:

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

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

20 (B) the Committee on Energy and Com-
21 merce of the House of Representatives; and

22 (C) the Committee on Foreign Affairs of
23 the House of Representatives.

24 (2) The term “chip security mechanism” means
25 a software-, firmware-, or hardware-enabled security

1 mechanism or a physical security mechanism, includ-
2 ing—

3 (A) periodic on-site audits or inventories at
4 the end-user's approved destination for the cov-
5 ered integrated circuit product;

6 (B) periodic attestations by a United
7 States-headquartered entity, or its subsidiaries,
8 confirming that all covered integrated circuit
9 products are accounted for, provided the Sec-
10 retary determines that the United States-
11 headquartered entity or its subsidiaries
12 verifiably certifies that the United States-
13 headquartered entity or its subsidiaries main-
14 tain continuous and sufficiently secure control,
15 operation, repair (to the extent such repair is
16 conducted by or under the direct supervision of
17 the United States-headquartered entity or its
18 subsidiaries), and disposal of the covered inte-
19 grated circuit products;

20 (C) ping-based location verification
21 through a trusted landmark server utilizing se-
22 cure software- or firmware-enabled mechanisms;
23 or

24 (D) various other mechanisms, or combina-
25 tions of mechanisms, that the Secretary deter-

1 mines can verifiably demonstrate with signifi-
2 cant confidence that the covered integrated cir-
3 cuit product has not been illegally diverted to a
4 destination of concern.

5 (3)(A) The term “covered integrated circuit
6 product” means a certain integrated circuit, com-
7 puter, or other product classified under Export Con-
8 trol Classification Number 3A090, 4A090, 5A002.z,
9 related .z Export Control Classification Numbers, or
10 other functionally equivalent or substantially similar
11 items.

12 (B) The Secretary shall routinely modify the
13 definition of the term “covered integrated circuit
14 product” under subparagraph (A) for the purposes
15 of this section to ensure only integrated circuits,
16 computers, electronic assembly, or components de-
17 signed or marketed for datacenter use are subject to
18 the requirements of this section.

19 (C) The term “covered integrated circuit” does
20 not include—

21 (i) covered integrated circuits or products
22 containing a covered integrated circuit that are
23 not designed or marketed for use in a data cen-
24 ter;

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

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

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

8 (A) a country subject to a United States
9 arms embargo listed under Country Group D:5
10 in Supplement No. 1 to Part 740 of the Export
11 Administration Regulations under parts 730
12 through 774 of title 15, Code of Federal Regu-
13 lations; or

14 (B) any other country determined by the
15 Secretary.

16 (5) The terms “export”, “in-country transfer”,
17 and “reexport” have the meanings given those terms
18 in section 1742 of the Export Control Reform Act
19 of 2018 (50 U.S.C. 4801).

20 (6) The term “Secretary” means the Secretary
21 of Commerce.

