

AMENDMENT TO RULES COMM. PRINT 116–57

OFFERED BY MR. YOHO OF FLORIDA

At the end of title XII, add the following:

1 **Subtitle H—Cyber Deterrence and**
2 **Response Act of 2020**

3 **SEC. 1281. SHORT TITLE.**

4 This subtitle may be cited as the “Cyber Deterrence
5 and Response Act of 2020”.

6 **SEC. 1282. FINDINGS.**

7 Congress finds the following:

8 (1) On February 13, 2018, the Director of Na-
9 tional Intelligence stated in his testimony before the
10 Senate Select Committee on Intelligence that “Rus-
11 sia, China, Iran, and North Korea will pose the
12 greatest cyber threats to the United States during
13 the next year” through the use of cyber operations
14 as low-cost tools of statecraft, and assessed that
15 these states would “work to use cyber operations to
16 achieve strategic objectives unless they face clear re-
17 percussions for their cyber operations”.

18 (2) The 2017 Worldwide Threat Assessment of
19 the United States Intelligence Community stated
20 that “The potential for surprise in the cyber realm

1 will increase in the next year and beyond as billions
2 more digital devices are connected—with relatively
3 little built-in security—and both nation states and
4 malign actors become more emboldened and better
5 equipped in the use of increasingly widespread cyber
6 toolkits. The risk is growing that some adversaries
7 will conduct cyber attacks—such as data deletion or
8 localized and temporary disruptions of critical infra-
9 structure—against the United States in a crisis
10 short of war.”.

11 (3) On March 29, 2017, President Donald J.
12 Trump deemed it necessary to continue the national
13 emergency declared in Executive Order No. 13694
14 as “Significant malicious cyber-enabled activities
15 originating from, or directed by persons located, in
16 whole or in substantial part, outside the United
17 States, continue to pose an unusual and extraor-
18 dinary threat to the national security, foreign policy,
19 and economy of the United States.”.

20 (4) On January 5, 2017, former Director of
21 National Intelligence, James Clapper, former Under-
22 secretary of Defense for Intelligence, Marcel Lettre,
23 and the Commander of the United States Cyber
24 Command, Admiral Michael Rogers, submitted joint
25 testimony to the Committee on Armed Services of

1 the Senate that stated “As of late 2016 more than
2 30 nations are developing offensive cyber attack ca-
3 pabilities” and that “Protecting critical infrastruc-
4 ture, such as crucial energy, financial, manufac-
5 turing, transportation, communication, and health
6 systems, will become an increasingly complex na-
7 tional security challenge.”.

8 (5) There is significant evidence that hackers
9 affiliated with foreign governments have conducted
10 cyber operations targeting companies and critical in-
11 frastructure sectors in the United States as the De-
12 partment of Justice and the Department of the
13 Treasury have announced that—

14 (A) on March 15, 2018, five Russian enti-
15 ties and 19 Russian individuals were designated
16 under the Countering America’s Adversaries
17 Through Sanctions Act, as well as pursuant to
18 Executive Order No. 13694, for interference in
19 the 2016 United States elections and other ma-
20 licious cyber-enabled activities;

21 (B) on March 24, 2016, seven Iranians
22 working for Iran’s Revolutionary Guard Corps-
23 affiliated entities were indicted for conducting
24 distributed denial of service attacks against the

1 financial sector in the United States from 2012
2 to 2013; and

3 (C) on May 19, 2014, five Chinese military
4 hackers were charged for hacking United States
5 companies in the nuclear power, metals, and
6 solar products industries, and engaging in eco-
7 nomic espionage.

8 (6) In May 2017, North Korea released
9 “WannaCry” pseudo-ransomware, which posed a sig-
10 nificant risk to the economy, national security, and
11 the citizens of the United States and the world, as
12 it resulted in the infection of over 300,000 computer
13 systems in more than 150 countries, including in the
14 healthcare sector of the United Kingdom, dem-
15 onstrating the global reach and cost of cyber-enabled
16 malicious activity.

17 (7) In June 2017, Russia carried out the most
18 destructive cyber-enabled operation in history, re-
19 leasing the NotPetya malware that caused billions of
20 dollars’ worth of damage within Ukraine and across
21 Europe, Asia, and the Americas.

22 (8) In May 2018, the Department of State,
23 pursuant to section 3(b) of Executive Order No.
24 13800, prepared recommendations to the President
25 on Deterring Adversaries and Better Protecting the

1 American People From Cyber Threats, which stated
2 “With respect to activities below the threshold of the
3 use of force, the United States should, working with
4 likeminded partners when possible, adopt an ap-
5 proach of imposing swift, costly, and transparent
6 consequences on foreign governments responsible for
7 significant malicious cyber activities aimed at harm-
8 ing U.S. national interests.”.

9 **SEC. 1283. ACTIONS TO ADDRESS STATE-SPONSORED**
10 **CYBER ACTIVITIES AGAINST THE UNITED**
11 **STATES.**

12 (a) DESIGNATION AS A CRITICAL CYBER THREAT
13 ACTOR.—

14 (1) IN GENERAL.—The President, acting
15 through the Secretary of State and the Secretary of
16 Defense, and in coordination with other relevant
17 Federal agency heads, shall designate as a critical
18 cyber threat actor—

19 (A) each foreign person and each agency
20 or instrumentality of a foreign state that the
21 President determines to be knowingly respon-
22 sible for or complicit in, or have engaged in, di-
23 rectly or indirectly, state-sponsored cyber activi-
24 ties that are reasonably likely to result in, or
25 have contributed to, a significant threat to the

1 national security, foreign policy, or economic
2 health or financial stability of the United States
3 and that have the purpose or effect of—

4 (i) causing a significant disruption to
5 the availability of a computer or network
6 of computers;

7 (ii) harming, or otherwise significantly
8 compromising the provision of service by, a
9 computer or network of computers that
10 support one or more entities in a critical
11 infrastructure sector;

12 (iii) significantly compromising the
13 provision of services by one or more enti-
14 ties in a critical infrastructure sector;

15 (iv) causing a significant misappro-
16 priation of funds or economic resources,
17 trade secrets, personal identifiers, or finan-
18 cial information for commercial or competi-
19 tive advantage or private financial gain;

20 (v) destabilizing the financial sector of
21 the United States by tampering with, alter-
22 ing, or causing a misappropriation of data;
23 or

24 (vi) interfering with or undermining
25 election processes or institutions by tam-

1 pering with, altering, or causing misappro-
2 piation of data;

3 (B) each foreign person that the President
4 has determined to have knowingly, significantly,
5 and materially assisted, sponsored, or provided
6 financial, material, or technological support for,
7 or goods or services to or in support of, any ac-
8 tivities described in subparagraph (A) by a for-
9 eign person or agency or instrumentality of a
10 foreign state designated as a critical cyber
11 threat actor under subparagraph (A); and

12 (C) each agency or instrumentality of a
13 foreign state that the President has determined
14 to have significantly and materially assisted,
15 sponsored, or provided financial, material, or
16 technological support for, or goods or services
17 to or in support of, any activities described in
18 subparagraph (A) by a foreign person or agency
19 or instrumentality of a foreign state designated
20 as a critical cyber threat actor under subpara-
21 graph (A).

22 (2) TRANSMISSION TO CONGRESS.—Not later
23 than 7 days after designating a foreign person or
24 agency or instrumentality of a foreign state as a
25 critical cyber threat actor, the President shall trans-

1 mit to the appropriate congressional committees in
2 classified or unclassified form a report identifying
3 the designee.

4 (b) NON-TRAVEL-RELATED SANCTIONS.—

5 (1) IN GENERAL.—The President shall impose
6 one or more of the applicable sanctions described in
7 paragraph (2) with respect to each foreign person
8 and each agency or instrumentality of a foreign
9 state designated as a critical cyber threat actor
10 under subsection (a).

11 (2) SANCTIONS DESCRIBED.—The sanctions de-
12 scribed in this paragraph are the following:

13 (A) The President may provide for the
14 withdrawal, limitation, or suspension of non-hu-
15 manitarian United States development assist-
16 ance under chapter 1 of part I of the Foreign
17 Assistance Act of 1961.

18 (B) The President may provide for the
19 withdrawal, limitation, or suspension of United
20 States security assistance under part II of the
21 Foreign Assistance Act of 1961.

22 (C) The President may direct the United
23 States executive director to each international
24 financial institution to use the voice and vote of
25 the United States to oppose any loan from the

1 international financial institution that would
2 benefit the designated foreign person or the
3 designated agency or instrumentality of a for-
4 eign state.

5 (D) The President may direct the United
6 States International Development Finance Cor-
7 poration or any other United States Govern-
8 ment agency not to approve the issuance of any
9 (or a specified number of) guarantees, insur-
10 ance, extensions of credit, or participations in
11 the extension of credit.

12 (E) The President may, pursuant to such
13 regulations or guidelines as the President may
14 prescribe, prohibit any United States person
15 from investing in or purchasing significant
16 amounts of equity or debt instruments of the
17 designated foreign person.

18 (F) The President may, pursuant to proce-
19 dures the President shall prescribe, which shall
20 include the opportunity to appeal actions under
21 this subparagraph, prohibit any United States
22 agency or instrumentality from procuring, or
23 entering into any contract for the procurement
24 of, any goods, technology, or services, or classes
25 of goods, technology, or services, from the des-

1 ignated foreign person or the designated agency
2 or instrumentality of a foreign state.

3 (G) The President may order the heads of
4 the appropriate United States agencies to not
5 issue any (or a specified number of) specific li-
6 censes, and to not grant any other specific au-
7 thority (or a specified number of authorities), to
8 export any goods or technology to the des-
9 ignated foreign person or the designated agency
10 or instrumentality of a foreign state under—

11 (i) the Export Control Reform Act of
12 2018;

13 (ii) the Arms Export Control Act;

14 (iii) the Atomic Energy Act of 1954;

15 or

16 (iv) any other statute that requires
17 the prior review and approval of the
18 United States Government as a condition
19 for the export or re-export of goods or
20 services.

21 (H)(i) The President may exercise all of
22 the powers granted to the President under the
23 International Emergency Economic Powers Act
24 (50 U.S.C. 1701 et seq.) (except that the re-
25 quirements of section 202 of such Act (50

1 U.S.C. 1701) shall not apply) to the extent nec-
2 essary to block and prohibit all transactions in
3 property and interests in property of the des-
4 ignated foreign person if such property and in-
5 terests in property are in the United States,
6 come within the United States, or are or come
7 within the possession or control of a United
8 States person.

9 (ii) The penalties provided for in sub-
10 sections (b) and (c) of section 206 of the Inter-
11 national Emergency Economic Powers Act (50
12 U.S.C. 1705) shall apply to a person that vio-
13 lates, attempts to violate, conspires to violate,
14 or causes a violation of regulations prescribed
15 under clause (i) to the same extent that such
16 penalties apply to a person that commits an un-
17 lawful act described in subsection (a) of such
18 section 206.

19 (I) The President may, pursuant to such
20 regulations as the President may prescribe, pro-
21 hibit any transfers of credit or payments be-
22 tween one or more financial institutions or by,
23 through, or to any financial institution, to the
24 extent that such transfers or payments are sub-
25 ject to the jurisdiction of the United States and

1 involve any interest of the designated foreign
2 person.

3 (c) TRAVEL-RELATED SANCTIONS.—

4 (1) ALIENS INELIGIBLE FOR VISAS, ADMISSION,
5 OR PAROLE.—An alien who is designated as a crit-
6 ical cyber threat actor under subsection (a) is—

7 (A) inadmissible to the United States;

8 (B) ineligible to receive a visa or other doc-
9 umentation to enter the United States; and

10 (C) otherwise ineligible to be admitted or
11 paroled into the United States or to receive any
12 other benefit under the Immigration and Na-
13 tionality Act (8 U.S.C. 1101 et seq.).

14 (2) CURRENT VISAS REVOKED.—The issuing
15 consular officer, the Secretary of State, or the Sec-
16 retary of Homeland Security (or a designee of either
17 such Secretaries) shall revoke any visa or other
18 entry documentation issued to the foreign person
19 designated as a critical cyber threat actor under sub-
20 section (a) regardless of when issued. A revocation
21 under this clause shall take effect immediately and
22 shall automatically cancel any other valid visa or
23 entry documentation that is in the possession of
24 such foreign person.

1 (d) ADDITIONAL SANCTIONS WITH RESPECT TO
2 FOREIGN STATES.—

3 (1) IN GENERAL.—The President may impose
4 any of the sanctions described in paragraph (2) with
5 respect to the government of each foreign state that
6 the President has determined aided, abetted, or di-
7 rected a foreign person or agency or instrumentality
8 of a foreign state designated as a critical cyber
9 threat actor under subsection (a).

10 (2) SANCTIONS DESCRIBED.—The sanctions re-
11 ferred to in paragraph (1) are the following:

12 (A) The President may provide for the
13 withdrawal, limitation, or suspension of non-hu-
14 manitarian or non-trade-related assistance
15 United States development assistance under
16 chapter 1 of part I of the Foreign Assistance
17 Act of 1961.

18 (B) The President may provide for the
19 withdrawal, limitation, or suspension of United
20 States security assistance under part II of the
21 Foreign Assistance Act of 1961.

22 (C) The President may instruct the United
23 States Executive Director to each appropriate
24 international financial institution to oppose, and
25 vote against the extension by such institution of

1 any loan or financial assistance to the govern-
2 ment of the foreign state.

3 (D) No item on the United States Muni-
4 tions List (established pursuant to section 38 of
5 the Arms Export Control Act (22 U.S.C.
6 2778)) or the Commerce Control List set forth
7 in Supplement No. 1 to part 774 of title 15,
8 Code of Federal Regulations, may be exported
9 to the government of the foreign state.

10 (e) IMPLEMENTATION.—The President may exercise
11 all authorities provided under sections 203 and 205 of the
12 International Emergency Economic Powers Act (50
13 U.S.C. 1702 and 1704) to carry out this section.

14 (f) COORDINATION.—To the extent practicable—

15 (1) actions taken by the President pursuant to
16 this section should be coordinated with United
17 States allies and partners;

18 (2) the Secretary of State should work with
19 United States allies and partners, on a voluntary
20 basis, to lead an international diplomatic initiative
21 to—

22 (A) deter critical cyber threat actors and
23 state-sponsored cyber activities; and

24 (B) provide mutual support to such allies
25 and partners participating in such initiative to

1 respond to such state-sponsored cyber activities;
2 and

3 (3) the Secretary of Defense should work within
4 existing partnerships with United States allies and
5 partners, on a voluntary basis, to—

6 (A) deter critical cyber threat actors and
7 state-sponsored cyber activities; and

8 (B) provide mutual support to such allies
9 and partners participating in such initiative to
10 respond to such state-sponsored cyber activities.

11 (g) EXEMPTIONS, WAIVERS, AND REMOVALS OF
12 SANCTIONS AND DESIGNATIONS.—

13 (1) MANDATORY EXEMPTIONS.—The following
14 activities shall be exempt from sanctions under sub-
15 sections (b), (c), and (d):

16 (A) Activities subject to the reporting re-
17 quirements of title V of the National Security
18 Act of 1947 (50 U.S.C. 413 et seq.), or to any
19 authorized intelligence activities of the United
20 States.

21 (B) Any transaction necessary to comply
22 with United States obligations under the Agree-
23 ment between the United Nations and the
24 United States of America regarding the Head-
25 quarters of the United Nations, signed June

1 26, 1947, and entered into force on November
2 21, 1947, or under the Vienna Convention on
3 Consular Relations, signed April 24, 1963, and
4 entered into force on March 19, 1967, or under
5 other international obligations.

6 (2) WAIVER.—The President may waive the im-
7 position of sanctions described in this section for a
8 period of not more than 1 year, and may renew such
9 waiver for additional periods of not more than 1
10 year, if the President transmits to the appropriate
11 congressional committees a written determination
12 that such waiver meets one or more of the following
13 requirements:

14 (A) Such waiver is in the national interests
15 of the United States.

16 (B) Such waiver will further the enforce-
17 ment of this subtitle or is for an important law
18 enforcement purpose.

19 (C) Such waiver is for an important hu-
20 manitarian purpose.

21 (3) REMOVALS OF SANCTIONS AND DESIGNA-
22 TIONS.—The President may prescribe rules and reg-
23 ulations for the removal of sanctions under sub-
24 sections (b), (c), and (d) and the removal of designa-
25 tions under subsection (a) if the President deter-

1 mines that a foreign person, agency or instrumen-
2 tality of a foreign state, or government of a foreign
3 state subject to such sanctions or such designations,
4 as the case may be, has verifiably ceased its partici-
5 pation in any of the conduct with respect to which
6 such foreign person, agency or instrumentality of a
7 foreign state, or government of a foreign state was
8 subject to such sanctions or designation, as the case
9 may be, under this section, and has given assurances
10 that such foreign person, agency or instrumentality
11 of a foreign state, or government of a foreign state,
12 as the case may be, will no longer participate in such
13 conduct.

14 (4) EXCEPTION TO COMPLY WITH UNITED NA-
15 TIONS HEADQUARTERS AGREEMENT.—Sanctions
16 under subsection (c) shall not apply to a foreign per-
17 son if admitting such foreign person into the United
18 States is necessary to permit the United States to
19 comply with the Agreement regarding the Head-
20 quarters of the United Nations, signed at Lake Suc-
21 cess June 26, 1947, and entered into force Novem-
22 ber 21, 1947, between the United Nations and the
23 United States, or other applicable international obli-
24 gations.

1 (h) RULE OF CONSTRUCTION.—Nothing in this sec-
2 tion may be construed to limit the authority of the Presi-
3 dent under the International Emergency Economic Powers
4 Act (50 U.S.C. 1701 et seq.) or any other provision of
5 law to impose sanctions to address critical cyber threat
6 actors and malicious state-sponsored cyber activities.

7 (i) DEFINITIONS.—In this section:

8 (1) ADMITTED; ALIEN.—The terms “admitted”
9 and “alien” have the meanings given such terms in
10 section 101 of the Immigration and Nationality Act
11 (8 U.S.C. 1101).

12 (2) APPROPRIATE CONGRESSIONAL COMMIT-
13 TEES.—The term “appropriate congressional com-
14 mittees” means—

15 (A) the Committee on Foreign Affairs, the
16 Committee on Financial Services, the Com-
17 mittee on the Judiciary, the Committee on
18 Oversight and Reform, and the Committee on
19 Homeland Security of the House of Representa-
20 tives; and

21 (B) the Committee on Foreign Relations,
22 the Committee on Banking, Housing, and
23 Urban Affairs, the Committee on the Judiciary,
24 and the Committee on Homeland Security and
25 Governmental Affairs of the Senate.

1 (3) AGENCY OR INSTRUMENTALITY OF A FOR-
2 EIGN STATE.—The term “agency or instrumentality
3 of a foreign state” has the meaning given such term
4 in section 1603(b) of title 28, United States Code.

5 (4) CRITICAL INFRASTRUCTURE SECTOR.—The
6 term “critical infrastructure sector” means any of
7 the designated critical infrastructure sectors identi-
8 fied in the Presidential Policy Directive entitled
9 “Critical Infrastructure Security and Resilience”,
10 numbered 21, and dated February 12, 2013.

11 (5) FOREIGN PERSON.—The term “foreign per-
12 son” means a person that is not a United States
13 person.

14 (6) FOREIGN STATE.—The term “foreign state”
15 has the meaning given such term in section 1603(a)
16 of title 28, United States Code.

17 (7) KNOWINGLY.—The term “knowingly”, with
18 respect to conduct, a circumstance, or a result,
19 means that a person has actual knowledge, or should
20 have known, of the conduct, the circumstance, or the
21 result.

22 (8) MISAPPROPRIATION.—The term “misappro-
23 priation” means taking or obtaining by improper
24 means, without permission or consent, or under false
25 pretenses.

1 (9) STATE-SPONSORED CYBER ACTIVITIES.—

2 The term “state-sponsored cyber activities” means
3 any malicious cyber-enabled activities that—

4 (A) are carried out by a government of a
5 foreign state or an agency or instrumentality of
6 a foreign state; or

7 (B) are carried out by a foreign person
8 that is aided, abetted, or directed by a govern-
9 ment of a foreign state or an agency or instru-
10 mentality of a foreign state.

11 (10) UNITED STATES PERSON.—The term
12 “United States person” means—

13 (A) a United States citizen or an alien law-
14 fully admitted for permanent residence to the
15 United States; or

16 (B) an entity organized under the laws of
17 the United States or of any jurisdiction within
18 the United States, including a foreign branch of
19 such an entity.

20 **SEC. 1284. CYBERSECURITY COOPERATION UNDER ASIA**
21 **REASSURANCE INITIATIVE ACT OF 2018.**

22 The Administration is encouraged to fully implement
23 section 215 of the Asia Reassurance Initiative Act of 2018
24 (Public Law 115–409) with regard to robust cybersecurity

- 1 cooperation between the United States and nations in the
- 2 Indo-Pacific region.

