SUBTITLE H—CYBER DETERRENCE AND RESPONSE ACT OF 2020

SEC. 1281. SHORT TITLE.
This subtitle may be cited as the “Cyber Deterrence and Response Act of 2020”.

SEC. 1282. FINDINGS.
Congress finds the following:

(1) On February 13, 2018, the Director of National Intelligence stated in his testimony before the Senate Select Committee on Intelligence that “Russia, China, Iran, and North Korea will pose the greatest cyber threats to the United States during the next year” through the use of cyber operations as low-cost tools of statecraft, and assessed that these states would “work to use cyber operations to achieve strategic objectives unless they face clear repercussions for their cyber operations”.

(2) The 2017 Worldwide Threat Assessment of the United States Intelligence Community stated that “The potential for surprise in the cyber realm
will increase in the next year and beyond as billions
more digital devices are connected—with relatively
little built-in security—and both nation states and
malign actors become more emboldened and better
equipped in the use of increasingly widespread cyber
toolkits. The risk is growing that some adversaries
will conduct cyber attacks—such as data deletion or
localized and temporary disruptions of critical infra-
structure—against the United States in a crisis
short of war.”.

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

(4) On January 5, 2017, former Director of
National Intelligence, James Clapper, former Under-
secretary of Defense for Intelligence, Marcel Lettre,
and the Commander of the United States Cyber
Command, Admiral Michael Rogers, submitted joint
testimony to the Committee on Armed Services of
the Senate that stated “As of late 2016 more than
30 nations are developing offensive cyber attack ca-
pabilities” and that “Protecting critical infrastruc-
ture, such as crucial energy, financial, manufac-
turing, transportation, communication, and health
systems, will become an increasingly complex na-
tional security challenge.”.

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

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

(B) on March 24, 2016, seven Iranians
working for Iran’s Revolutionary Guard Corps-
affiliated entities were indicted for conducting
distributed denial of service attacks against the
financial sector in the United States from 2012 to 2013; and

(C) on May 19, 2014, five Chinese military hackers were charged for hacking United States companies in the nuclear power, metals, and solar products industries, and engaging in economic espionage.

(6) In May 2017, North Korea released “WannaCry” pseudo-ransomware, which posed a significant risk to the economy, national security, and the citizens of the United States and the world, as it resulted in the infection of over 300,000 computer systems in more than 150 countries, including in the healthcare sector of the United Kingdom, demonstrating the global reach and cost of cyber-enabled malicious activity.

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

(8) In May 2018, the Department of State, pursuant to section 3(b) of Executive Order No. 13800, prepared recommendations to the President on Deterring Adversaries and Better Protecting the
American People From Cyber Threats, which stated
“With respect to activities below the threshold of the
use of force, the United States should, working with
likeminded partners when possible, adopt an ap-
proach of imposing swift, costly, and transparent
consequences on foreign governments responsible for
significant malicious cyber activities aimed at harm-
ing U.S. national interests.”

SEC. 1283. ACTIONS TO ADDRESS STATE-SPONSORED
CYBER ACTIVITIES AGAINST THE UNITED
STATES.

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

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

(A) each foreign person and each agency
or instrumentality of a foreign state that the
President determines to be knowingly respon-
sible for or complicit in, or have engaged in, di-
rectly or indirectly, state-sponsored cyber activi-
ties that are reasonably likely to result in, or
have contributed to, a significant threat to the
national security, foreign policy, or economic health or financial stability of the United States and that have the purpose or effect of—

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

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

(iii) significantly compromising the provision of services by one or more entities in a critical infrastructure sector;

(iv) causing a significant misappropriation of funds or economic resources, trade secrets, personal identifiers, or financial information for commercial or competitive advantage or private financial gain;

(v) destabilizing the financial sector of the United States by tampering with, altering, or causing a misappropriation of data; or

(vi) interfering with or undermining election processes or institutions by tam-
7

pering with, altering, or causing misappropriation of data;

(B) each foreign person that the President has determined to have knowingly, significantly, and materially assisted, sponsored, or provided financial, material, or technological support for, or goods or services to or in support of, any activities described in subparagraph (A) by a foreign person or agency or instrumentality of a foreign state designated as a critical cyber threat actor under subparagraph (A); and

(C) each agency or instrumentality of a foreign state that the President has determined to have significantly and materially assisted, sponsored, or provided financial, material, or technological support for, or goods or services to or in support of, any activities described in subparagraph (A) by a foreign person or agency or instrumentality of a foreign state designated as a critical cyber threat actor under subparagraph (A).

(2) TRANSMISSION TO CONGRESS.—Not later than 7 days after designating a foreign person or agency or instrumentality of a foreign state as a critical cyber threat actor, the President shall trans-
mit to the appropriate congressional committees in
classified or unclassified form a report identifying
the designee.

(b) NON-TRAVEL-RELATED SANCTIONS.—
(1) IN GENERAL.—The President shall impose
one or more of the applicable sanctions described in
paragraph (2) with respect to each foreign person
and each agency or instrumentality of a foreign
state designated as a critical cyber threat actor
under subsection (a).

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

(A) The President may provide for the
withdrawal, limitation, or suspension of non-hu-
manitarian United States development assist-
ance under chapter 1 of part I of the Foreign

(B) The President may provide for the
withdrawal, limitation, or suspension of United
States security assistance under part II of the

(C) The President may direct the United
States executive director to each international
financial institution to use the voice and vote of
the United States to oppose any loan from the
international financial institution that would
benefit the designated foreign person or the
designated agency or instrumentality of a for-

ey state.

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

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

(F) The President may, pursuant to proce-
dures the President shall prescribe, which shall
include the opportunity to appeal actions under
this subparagraph, prohibit any United States
agency or instrumentality from procuring, or
entering into any contract for the procurement
of, any goods, technology, or services, or classes
of goods, technology, or services, from the des-
ignated foreign person or the designated agency
or instrumentality of a foreign state.

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

(i) the Export Control Reform Act of
2018;

(ii) the Arms Export Control Act;

(iii) the Atomic Energy Act of 1954;

or

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

(H)(i) The President may exercise all of
the powers granted to the President under the
International Emergency Economic Powers Act
(50 U.S.C. 1701 et seq.) (except that the re-
requirements of section 202 of such Act (50
11

U.S.C. 1701) shall not apply) to the extent nec-

essary to block and prohibit all transactions in

property and interests in property of the des-

ignated foreign person if such property and in-

terests in property are in the United States,

come within the United States, or are or come

within the possession or control of a United

States person.

(ii) The penalties provided for in sub-

sections (b) and (c) of section 206 of the Inter-

national Emergency Economic Powers Act (50

U.S.C. 1705) shall apply to a person that vio-

lates, attempts to violate, conspires to violate,

or causes a violation of regulations prescribed

under clause (i) to the same extent that such

penalties apply to a person that commits an un-

lawful act described in subsection (a) of such

section 206.

(I) The President may, pursuant to such

regulations as the President may prescribe, pro-

hibit any transfers of credit or payments be-

tween one or more financial institutions or by,

through, or to any financial institution, to the

extent that such transfers or payments are sub-

ject to the jurisdiction of the United States and
involve any interest of the designated foreign person.

(c) **Travel-Related Sanctions.**—

(1) **Aliens Ineligible for Visas, Admission,** or Parole.—An alien who is designated as a critical cyber threat actor under subsection (a) is—

(A) inadmissible to the United States;

(B) ineligible to receive a visa or other documentation to enter the United States; and

(C) otherwise ineligible to be admitted or paroled into the United States or to receive any other benefit under the Immigration and Nationality Act (8 U.S.C. 1101 et seq.).

(2) **Current Visas Revoked.**—The issuing consular officer, the Secretary of State, or the Secretary of Homeland Security (or a designee of either such Secretaries) shall revoke any visa or other entry documentation issued to the foreign person designated as a critical cyber threat actor under subsection (a) regardless of when issued. A revocation under this clause shall take effect immediately and shall automatically cancel any other valid visa or entry documentation that is in the possession of such foreign person.
(d) ADDITIONAL SANCTIONS WITH RESPECT TO FOREIGN STATES.—

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

(2) SANCTIONS DESCRIBED.—The sanctions referred to in paragraph (1) are the following:

(A) The President may provide for the withdrawal, limitation, or suspension of non-humanitarian or non-trade-related assistance United States development assistance under chapter 1 of part I of the Foreign Assistance Act of 1961.

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

(C) The President may instruct the United States Executive Director to each appropriate international financial institution to oppose, and vote against the extension by such institution of
any loan or financial assistance to the government of the foreign state.

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

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

(f) COORDINATION.—To the extent practicable—

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

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

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

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

and

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

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

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

(g) Exemptions, Waivers, and Removals of
Sanctions and Designations.—

(1) Mandatory Exemptions.—The following
activities shall be exempt from sanctions under sub-
sections (b), (c), and (d):

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

(B) Any transaction necessary to comply
with United States obligations under the Agree-
ment between the United Nations and the
United States of America regarding the Head-
quarters of the United Nations, signed June
26, 1947, and entered into force on November 21, 1947, or under the Vienna Convention on Consular Relations, signed April 24, 1963, and entered into force on March 19, 1967, or under other international obligations.

(2) WAIVER.—The President may waive the imposition of sanctions described in this section for a period of not more than 1 year, and may renew such waiver for additional periods of not more than 1 year, if the President transmits to the appropriate congressional committees a written determination that such waiver meets one or more of the following requirements:

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

(B) Such waiver will further the enforcement of this subtitle or is for an important law enforcement purpose.

(C) Such waiver is for an important humanitarian purpose.

(3) REMOVALS OF SANCTIONS AND DESIGNATIONS.—The President may prescribe rules and regulations for the removal of sanctions under subsections (b), (c), and (d) and the removal of designations under subsection (a) if the President deter-
mines that a foreign person, agency or instrumentality of a foreign state, or government of a foreign state subject to such sanctions or such designations, as the case may be, has verifiably ceased its participation in any of the conduct with respect to which such foreign person, agency or instrumentality of a foreign state, or government of a foreign state was subject to such sanctions or designation, as the case may be, under this section, and has given assurances that such foreign person, agency or instrumentality of a foreign state, or government of a foreign state, as the case may be, will no longer participate in such conduct.

(4) Exception to Comply with United Nations Headquarters Agreement.—Sanctions under subsection (c) shall not apply to a foreign person if admitting such foreign person into the United States is necessary to permit the United States to comply with the Agreement regarding the Headquarters of the United Nations, signed at Lake Success June 26, 1947, and entered into force November 21, 1947, between the United Nations and the United States, or other applicable international obligations.
(h) Rule of Construction.—Nothing in this section may be construed to limit the authority of the President under the International Emergency Economic Powers Act (50 U.S.C. 1701 et seq.) or any other provision of law to impose sanctions to address critical cyber threat actors and malicious state-sponsored cyber activities.

(i) Definitions.—In this section:

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

(2) Appropriate Congressional Committees.—The term “appropriate congressional committees” means—

(A) the Committee on Foreign Affairs, the Committee on Financial Services, the Committee on the Judiciary, the Committee on Oversight and Reform, and the Committee on Homeland Security of the House of Representatives; and

(B) the Committee on Foreign Relations, the Committee on Banking, Housing, and Urban Affairs, the Committee on the Judiciary, and the Committee on Homeland Security and Governmental Affairs of the Senate.
(3) AGENCY OR INSTRUMENTALITY OF A FOREIGN STATE.—The term “agency or instrumentality of a foreign state” has the meaning given such term in section 1603(b) of title 28, United States Code.


(5) FOREIGN PERSON.—The term “foreign person” means a person that is not a United States person.

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

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

(8) MISAPPROPRIATION.—The term “misappropriation” means taking or obtaining by improper means, without permission or consent, or under false pretenses.
(9) **State-sponsored cyber activities.**—
The term “state-sponsored cyber activities” means any malicious cyber-enabled activities that—  
(A) are carried out by a government of a foreign state or an agency or instrumentality of a foreign state; or  
(B) are carried out by a foreign person that is aided, abetted, or directed by a government of a foreign state or an agency or instrumentality of a foreign state.

(10) **United States person.**—The term “United States person” means—  
(A) a United States citizen or an alien lawfully admitted for permanent residence to the United States; or  
(B) an entity organized under the laws of the United States or of any jurisdiction within the United States, including a foreign branch of such an entity.

**SEC. 1284. CYBERSECURITY COOPERATION UNDER ASIA REASSURANCE INITIATIVE ACT OF 2018.**
The Administration is encouraged to fully implement section 215 of the Asia Reassurance Initiative Act of 2018 (Public Law 115–409) with regard to robust cybersecurity
cooperation between the United States and nations in the Indo-Pacific region.