

116TH CONGRESS  
1ST SESSION

# H. R. 739

To support United States international cyber diplomacy, and for other purposes.

---

IN THE HOUSE OF REPRESENTATIVES

JANUARY 24, 2019

Mr. McCAUL (for himself and Mr. ENGEL) introduced the following bill; which was referred to the Committee on Foreign Affairs

---

## A BILL

To support United States international cyber diplomacy, and for other purposes.

1 *Be it enacted by the Senate and House of Representa-*  
2 *tives of the United States of America in Congress assembled,*

3 **SECTION 1. SHORT TITLE; TABLE OF CONTENTS.**

4 (a) **SHORT TITLE.**—This Act may be cited as the  
5 “Cyber Diplomacy Act of 2019”.

6 (b) **TABLE OF CONTENTS.**—The table of contents for  
7 this Act is as follows:

- Sec. 1. Short title; table of contents.
- Sec. 2. Findings.
- Sec. 3. Definitions.
- Sec. 4. United States International Cyberspace Policy.
- Sec. 5. Department of State responsibilities.
- Sec. 6. International cyberspace executive arrangements.
- Sec. 7. International strategy for cyberspace.

Sec. 8. Annual country reports on human rights practices.

Sec. 9. GAO report on cyber threats and data misuse.

Sec. 10. Sense of Congress on cybersecurity sanctions against North Korea and cybersecurity legislation in Vietnam.

Sec. 11. Rule of construction.

1 **SEC. 2. FINDINGS.**

2 Congress makes the following findings:

3 (1) The stated goal of the United States Inter-  
4 national Strategy for Cyberspace, launched on May  
5 16, 2011, is to “work internationally to promote an  
6 open, interoperable, secure, and reliable information  
7 and communications infrastructure that supports  
8 international trade and commerce, strengthens inter-  
9 national security, and fosters free expression and in-  
10 novation . . . in which norms of responsible behav-  
11 ior guide states’ actions, sustain partnerships, and  
12 support the rule of law in cyberspace”.

13 (2) In its June 24, 2013 report, the Group of  
14 Governmental Experts on Developments in the Field  
15 of Information and Telecommunications in the Con-  
16 text of International Security (referred to in this  
17 section as “GGE”), established by the United Na-  
18 tions General Assembly, concluded that “State sov-  
19 ereignty and the international norms and principles  
20 that flow from it apply to States’ conduct of [infor-  
21 mation and communications technology] ICT-related  
22 activities and to their jurisdiction over ICT infra-  
23 structure with their territory”.

1           (3) In January 2015, China, Kazakhstan,  
2           Kyrgyzstan, Russia, Tajikistan, and Uzbekistan pro-  
3           posed a troubling international code of conduct for  
4           information security, which could be used as a pre-  
5           text for restricting political dissent, and includes  
6           “curbing the dissemination of information that in-  
7           cites terrorism, separatism or extremism or that in-  
8           flames hatred on ethnic, racial or religious grounds”.

9           (4) In its July 22, 2015 consensus report, GGE  
10          found that “norms of responsible State behavior can  
11          reduce risks to international peace, security and sta-  
12          bility”.

13          (5) On September 25, 2015, the United States  
14          and China announced a commitment that neither  
15          country’s government “will conduct or knowingly  
16          support cyber-enabled theft of intellectual property,  
17          including trade secrets or other confidential business  
18          information, with the intent of providing competitive  
19          advantages to companies or commercial sectors”.

20          (6) At the Antalya Summit on November 15  
21          and 16, 2015, the Group of 20 Leaders’  
22          communiqué—

23                  (A) affirmed the applicability of inter-  
24                  national law to state behavior in cyberspace;

1 (B) called on states to refrain from cyber-  
2 enabled theft of intellectual property for com-  
3 mercial gain; and

4 (C) endorsed the view that all states  
5 should abide by norms of responsible behavior.

6 (7) The March 2016 Department of State  
7 International Cyberspace Policy Strategy noted that  
8 “the Department of State anticipates a continued in-  
9 crease and expansion of our cyber-focused diplomatic  
10 efforts for the foreseeable future”.

11 (8) On December 1, 2016, the Commission on  
12 Enhancing National Cybersecurity, which was estab-  
13 lished within the Department of Commerce by Exec-  
14 utive Order 13718 (81 Fed. Reg. 7441), rec-  
15 ommended that “the President should appoint an  
16 Ambassador for Cybersecurity to lead U.S. engage-  
17 ment with the international community on cyberse-  
18 curity strategies, standards, and practices”.

19 (9) On April 11, 2017, the 2017 Group of 7  
20 Declaration on Responsible States Behavior in  
21 Cyberspace—

22 (A) recognized “the urgent necessity of in-  
23 creased international cooperation to promote se-  
24 curity and stability in cyberspace”;

1 (B) expressed commitment to “promoting  
2 a strategic framework for conflict prevention,  
3 cooperation and stability in cyberspace, con-  
4 sisting of the recognition of the applicability of  
5 existing international law to State behavior in  
6 cyberspace, the promotion of voluntary, non-  
7 binding norms of responsible State behavior  
8 during peacetime, and the development and the  
9 implementation of practical cyber confidence  
10 building measures (CBMs) between States”;  
11 and

12 (C) reaffirmed that “the same rights that  
13 people have offline must also be protected on-  
14 line”.

15 (10) In testimony before the Select Committee  
16 on Intelligence of the Senate on May 11, 2017, Di-  
17 rector of National Intelligence Daniel R. Coats iden-  
18 tified 6 cyber threat actors, including—

19 (A) Russia, for “efforts to influence the  
20 2016 US election”;

21 (B) China, for “actively targeting the US  
22 Government, its allies, and US companies for  
23 cyber espionage”;

24 (C) Iran, for “leverag[ing] cyber espionage,  
25 propaganda, and attacks to support its security

1 priorities, influence events and foreign percep-  
2 tions, and counter threats”;

3 (D) North Korea, for “previously  
4 conduct[ing] cyber-attacks against US commer-  
5 cial entities—specifically, Sony Pictures Enter-  
6 tainment in 2014”;

7 (E) terrorists, who “use the Internet to or-  
8 ganize, recruit, spread propaganda, raise funds,  
9 collect intelligence, inspire action by followers,  
10 and coordinate operations”; and

11 (F) criminals, who “are also developing  
12 and using sophisticated cyber tools for a variety  
13 of purposes including theft, extortion, and fa-  
14 cilitation of other criminal activities”.

15 (11) On May 11, 2017, President Donald J.  
16 Trump issued Executive Order 13800 (82 Fed. Reg.  
17 22391), entitled “Strengthening the Cybersecurity of  
18 Federal Networks and Infrastructure”, which—

19 (A) designates the Secretary of State to  
20 lead an interagency effort to develop an engage-  
21 ment strategy for international cooperation in  
22 cybersecurity; and

23 (B) notes that “the United States is espe-  
24 cially dependent on a globally secure and resil-  
25 ient internet and must work with allies and

1 other partners toward maintaining . . . the pol-  
2 icy of the executive branch to promote an open,  
3 interoperable, reliable, and secure internet that  
4 fosters efficiency, innovation, communication,  
5 and economic prosperity, while respecting pri-  
6 vacy and guarding against disruption, fraud,  
7 and theft”.

8 **SEC. 3. DEFINITIONS.**

9 In this Act:

10 (1) **APPROPRIATE CONGRESSIONAL COMMIT-**  
11 **TEES.**—The term “appropriate congressional com-  
12 mittees” means the Committee on Foreign Relations  
13 of the Senate and the Committee on Foreign Affairs  
14 of the House of Representatives.

15 (2) **INFORMATION AND COMMUNICATIONS**  
16 **TECHNOLOGY; ICT.**—The terms “information and  
17 communications technology” and “ICT” include  
18 hardware, software, and other products or services  
19 primarily intended to fulfill or enable the function of  
20 information processing and communication by elec-  
21 tronic means, including transmission and display, in-  
22 cluding via the Internet.

23 (3) **EXECUTIVE AGENCY.**—The term “Executive  
24 agency” has the meaning given the term in section  
25 105 of title 5, United States Code.

1 **SEC. 4. UNITED STATES INTERNATIONAL CYBERSPACE**  
2 **POLICY.**

3 (a) **IN GENERAL.**—It is the policy of the United  
4 States to work internationally to promote an open, inter-  
5 operable, reliable, unfettered, and secure Internet gov-  
6 erned by the multi-stakeholder model, which—

7 (1) promotes human rights, democracy, and  
8 rule of law, including freedom of expression, innova-  
9 tion, communication, and economic prosperity; and

10 (2) respects privacy and guards against decep-  
11 tion, fraud, and theft.

12 (b) **IMPLEMENTATION.**—In implementing the policy  
13 described in subsection (a), the President, in consultation  
14 with outside actors, including private sector companies,  
15 nongovernmental organizations, security researchers, and  
16 other relevant stakeholders, in the conduct of bilateral and  
17 multilateral relations, shall pursue the following objectives:

18 (1) Clarifying the applicability of international  
19 laws and norms to the use of ICT.

20 (2) Reducing and limiting the risk of escalation  
21 and retaliation in cyberspace, damage to critical in-  
22 frastructure, and other malicious cyber activity that  
23 impairs the use and operation of critical infrastruc-  
24 ture that provides services to the public.

25 (3) Cooperating with like-minded democratic  
26 countries that share common values and cyberspace

1 policies with the United States, including respect for  
2 human rights, democracy, and the rule of law, to ad-  
3 vance such values and policies internationally.

4 (4) Encouraging the responsible development of  
5 new, innovative technologies and ICT products that  
6 strengthen a secure Internet architecture that is ac-  
7 cessible to all.

8 (5) Securing and implementing commitments  
9 on responsible country behavior in cyberspace based  
10 upon accepted norms, including the following:

11 (A) Countries should not conduct, or  
12 knowingly support, cyber-enabled theft of intel-  
13 lectual property, including trade secrets or  
14 other confidential business information, with  
15 the intent of providing competitive advantages  
16 to companies or commercial sectors.

17 (B) Countries should take all appropriate  
18 and reasonable efforts to keep their territories  
19 clear of intentionally wrongful acts using ICTs  
20 in violation of international commitments.

21 (C) Countries should not conduct or know-  
22 ingly support ICT activity that, contrary to  
23 international law, intentionally damages or oth-  
24 erwise impairs the use and operation of critical  
25 infrastructure providing services to the public,

1 and should take appropriate measures to pro-  
2 tect their critical infrastructure from ICT  
3 threats.

4 (D) Countries should not conduct or know-  
5 ingly support malicious international activity  
6 that, contrary to international law, harms the  
7 information systems of authorized emergency  
8 response teams (also known as “computer  
9 emergency response teams” or “cybersecurity  
10 incident response teams”) of another country or  
11 authorize emergency response teams to engage  
12 in malicious international activity.

13 (E) Countries should respond to appro-  
14 priate requests for assistance to mitigate mali-  
15 cious ICT activity emanating from their terri-  
16 tory and aimed at the critical infrastructure of  
17 another country.

18 (F) Countries should not restrict cross-bor-  
19 der data flows or require local storage or proc-  
20 essing of data.

21 (G) Countries should protect the exercise  
22 of human rights and fundamental freedoms on  
23 the Internet and commit to the principle that  
24 the human rights that people have offline  
25 should also be protected online.

1           (6) Advancing, encouraging, and supporting the  
2           development and adoption of internationally recog-  
3           nized technical standards and best practices.

4 **SEC. 5. DEPARTMENT OF STATE RESPONSIBILITIES.**

5           (a) IN GENERAL.—Section 1 of the State Depart-  
6           ment Basic Authorities Act of 1956 (22 U.S.C. 2651a)  
7           is amended—

8           (1) by redesignating subsection (g) as sub-  
9           section (h); and

10           (2) by inserting after subsection (f) the fol-  
11           lowing:

12           “(g) OFFICE OF INTERNATIONAL CYBERSPACE POL-  
13           ICY.—

14           “(1) IN GENERAL.—There is established, within  
15           the Department of State, an Office of International  
16           Cyberspace Policy (referred to in this subsection as  
17           the ‘Office’). The head of the Office shall have the  
18           rank and status of ambassador and shall be ap-  
19           pointed by the President, by and with the advice and  
20           consent of the Senate.

21           “(2) DUTIES.—

22           “(A) IN GENERAL.—The head of the Of-  
23           fice shall perform such duties and exercise such  
24           powers as the Secretary of State shall prescribe,  
25           including implementing the policy of the United

1 States described in section 4 of the Cyber Di-  
2 plomacy Act of 2019.

3 “(B) DUTIES DESCRIBED.—The principal  
4 duties and responsibilities of the head of the  
5 Office shall be—

6 “(i) to serve as the principal cyber-  
7 space policy official within the senior man-  
8 agement of the Department of State and  
9 as the advisor to the Secretary of State for  
10 cyberspace issues;

11 “(ii) to lead the Department of  
12 State’s diplomatic cyberspace efforts, in-  
13 cluding efforts relating to international cy-  
14 bersecurity, Internet access, Internet free-  
15 dom, digital economy, cybercrime, deter-  
16 rence and international responses to cyber  
17 threats, and other issues that the Sec-  
18 retary assigns to the Office;

19 “(iii) to promote an open, interoper-  
20 able, reliable, unfettered, and secure infor-  
21 mation and communications technology in-  
22 frastructure globally;

23 “(iv) to represent the Secretary of  
24 State in interagency efforts to develop and

1 advance the policy described in section 4 of  
2 the Cyber Diplomacy Act of 2019;

3 “(v) to coordinate cyberspace efforts  
4 and other relevant functions, including  
5 countering terrorists’ use of cyberspace,  
6 within the Department of State and with  
7 other components of the United States  
8 Government;

9 “(vi) to act as a liaison to public and  
10 private sector entities on relevant inter-  
11 national cyberspace issues;

12 “(vii) to lead United States Govern-  
13 ment efforts to establish a global deter-  
14 rence framework for malicious cyber activ-  
15 ity;

16 “(viii) to develop and execute adver-  
17 sary-specific strategies to influence adver-  
18 sary decisionmaking through the imposi-  
19 tion of costs and deterrence strategies, in  
20 coordination with other relevant Executive  
21 agencies;

22 “(ix) to advise the Secretary and co-  
23 ordinate with foreign governments on ex-  
24 ternal responses to national-security-level  
25 cyber incidents, including coordination on

1 diplomatic response efforts to support al-  
2 lies threatened by malicious cyber activity,  
3 in conjunction with members of the North  
4 Atlantic Treaty Organization and other  
5 like-minded countries;

6 “(x) to promote the adoption of na-  
7 tional processes and programs that enable  
8 threat detection, prevention, and response  
9 to malicious cyber activity emanating from  
10 the territory of a foreign country, including  
11 as such activity relates to the United  
12 States’ European allies, as appropriate;

13 “(xi) to promote the building of for-  
14 eign capacity to protect the global network  
15 with the goal of enabling like-minded par-  
16 ticipation in deterrence frameworks;

17 “(xii) to promote the maintenance of  
18 an open and interoperable Internet gov-  
19 erned by the multi-stakeholder model, in-  
20 stead of by centralized government control;

21 “(xiii) to promote an international  
22 regulatory environment for technology in-  
23 vestments and the Internet that benefits  
24 United States economic and national secu-  
25 rity interests;

1 “(xiv) to promote cross-border flow of  
2 data and combat international initiatives  
3 seeking to impose unreasonable require-  
4 ments on United States businesses;

5 “(xv) to promote international policies  
6 to protect the integrity of United States  
7 and international telecommunications in-  
8 frastructure from foreign-based, cyber-en-  
9 abled threats;

10 “(xvi) to lead engagement, in coordi-  
11 nation with Executive agencies, with for-  
12 eign governments on cyberspace and digital  
13 economy issues as described in the Cyber  
14 Diplomacy Act of 2019;

15 “(xvii) to promote international poli-  
16 cies to secure radio frequency spectrum for  
17 United States businesses and national se-  
18 curity needs;

19 “(xviii) to promote and protect the ex-  
20 ercise of human rights, including freedom  
21 of speech and religion, through the Inter-  
22 net;

23 “(xix) to build capacity of United  
24 States diplomatic officials to engage on  
25 cyber issues;

1           “(xx) to encourage the development  
2           and adoption by foreign countries of inter-  
3           nationally recognized standards, policies,  
4           and best practices; and

5           “(xxi) to consult, as appropriate, with  
6           other Executive agencies with related func-  
7           tions vested in such Executive agencies by  
8           law.

9           “(3) QUALIFICATIONS.—The head of the Office  
10          should be an individual of demonstrated competency  
11          in the fields of—

12                 “(A) cybersecurity and other relevant cyber  
13                 issues; and

14                 “(B) international diplomacy.

15          “(4) ORGANIZATIONAL PLACEMENT.—During  
16          the 4-year period beginning on the date of the enact-  
17          ment of the Cyber Diplomacy Act of 2019, the head  
18          of the Office shall report to the Under Secretary for  
19          Political Affairs or to an official holding a higher po-  
20          sition than the Under Secretary for Political Affairs  
21          in the Department of State. After the conclusion of  
22          such period, the head of the Office shall report to  
23          an appropriate Under Secretary or to an official  
24          holding a higher position than Under Secretary.

1           “(5) RULE OF CONSTRUCTION.—Nothing in  
2 this subsection may be construed to preclude—

3           “(A) the Office from being elevated to a  
4 Bureau within the Department of State; or

5           “(B) the head of the Office from being ele-  
6 vated to an Assistant Secretary, if such an As-  
7 sistant Secretary position does not increase the  
8 number of Assistant Secretary positions at the  
9 Department above the number authorized under  
10 subsection (c)(1).”.

11       (b) SENSE OF CONGRESS.—It is the sense of Con-  
12 gress that the Office of International Cyberspace Policy  
13 established under section 1(g) of the State Department  
14 Basic Authorities Act of 1956, as added by subsection (a),  
15 should be a Bureau of the Department of State and the  
16 head of such Office should report directly to the Secretary  
17 of State or Deputy Secretary of State.

18       (c) UNITED NATIONS.—The Permanent Representa-  
19 tive of the United States to the United Nations should  
20 use the voice, vote, and influence of the United States to  
21 oppose any measure that is inconsistent with the policy  
22 described in section 4.

1 **SEC. 6. INTERNATIONAL CYBERSPACE EXECUTIVE AR-**  
2 **RANGEMENTS.**

3 (a) IN GENERAL.—The President is encouraged to  
4 enter into executive arrangements with foreign govern-  
5 ments that support the policy described in section 4.

6 (b) TRANSMISSION TO CONGRESS.—Section 112b of  
7 title 1, United States Code, is amended—

8 (1) in subsection (a) by striking “International  
9 Relations” and inserting “Foreign Affairs”;

10 (2) in subsection (e)(2)(B), by adding at the  
11 end the following:

12 “(iii) A bilateral or multilateral cyberspace  
13 agreement.”;

14 (3) by redesignating subsection (f) as sub-  
15 section (g); and

16 (4) by inserting after subsection (e) the fol-  
17 lowing:

18 “(f) With respect to any bilateral or multilateral  
19 cyberspace agreement under subsection (e)(2)(B)(iii) and  
20 the information required to be transmitted to Congress  
21 under subsection (a), or with respect to any arrangement  
22 that seeks to secure commitments on responsible country  
23 behavior in cyberspace consistent with section 4(b)(5) of  
24 the Cyber Diplomacy Act of 2019, the Secretary of State  
25 shall provide an explanation of such arrangement, includ-  
26 ing—

1           “(1) the purpose of such arrangement;

2           “(2) how such arrangement is consistent with  
3 the policy described in section 4 of such Act; and

4           “(3) how such arrangement will be imple-  
5 mented.”.

6       (c) STATUS REPORT.—During the 5-year period im-  
7 mediately following the transmittal to Congress of an  
8 agreement described in section 112b(e)(2)(B)(iii) of title  
9 1, United States Code, as added by subsection (b)(2), or  
10 until such agreement has been discontinued, if discon-  
11 tinued within 5 years, the President shall—

12           (1) notify the appropriate congressional com-  
13 mittees if another country fails to adhere to signifi-  
14 cant commitments contained in such agreement; and

15           (2) describe the steps that the United States  
16 has taken or plans to take to ensure that all such  
17 commitments are fulfilled.

18       (d) EXISTING EXECUTIVE ARRANGEMENTS.—Not  
19 later than 180 days after the date of the enactment of  
20 this Act, the Secretary of State shall brief the appropriate  
21 congressional committees regarding any executive bilateral  
22 or multilateral cyberspace arrangement in effect before the  
23 date of enactment of this Act, including—

24           (1) the arrangement announced between the  
25 United States and Japan on April 25, 2014;

1           (2) the arrangement announced between the  
2 United States and the United Kingdom on January  
3 16, 2015;

4           (3) the arrangement announced between the  
5 United States and China on September 25, 2015;

6           (4) the arrangement announced between the  
7 United States and Korea on October 16, 2015;

8           (5) the arrangement announced between the  
9 United States and Australia on January 19, 2016;

10          (6) the arrangement announced between the  
11 United States and India on June 7, 2016;

12          (7) the arrangement announced between the  
13 United States and Argentina on April 27, 2017;

14          (8) the arrangement announced between the  
15 United States and Kenya on June 22, 2017;

16          (9) the arrangement announced between the  
17 United States and Israel on June 26, 2017;

18          (10) the arrangement announced between the  
19 United States and France on February 9, 2018;

20          (11) the arrangement announced between the  
21 United States and Brazil on May 14, 2018; and

22          (12) any other similar bilateral or multilateral  
23 arrangement announced before such date of enact-  
24 ment.

1 **SEC. 7. INTERNATIONAL STRATEGY FOR CYBERSPACE.**

2 (a) STRATEGY REQUIRED.—Not later than 1 year  
3 after the date of the enactment of this Act, the President,  
4 acting through the Secretary of State, and in coordination  
5 with the heads of other relevant Federal departments and  
6 agencies, shall develop a strategy relating to United States  
7 engagement with foreign governments on international  
8 norms with respect to responsible state behavior in cyber-  
9 space.

10 (b) ELEMENTS.—The strategy required under sub-  
11 section (a) shall include the following:

12 (1) A review of actions and activities under-  
13 taken to support the policy described in section 4.

14 (2) A plan of action to guide the diplomacy of  
15 the Department of State with regard to foreign  
16 countries, including—

17 (A) conducting bilateral and multilateral  
18 activities to develop norms of responsible coun-  
19 try behavior in cyberspace consistent with the  
20 objectives under section 4(b)(5); and

21 (B) reviewing the status of existing efforts  
22 in relevant multilateral fora, as appropriate, to  
23 obtain commitments on international norms in  
24 cyberspace.

1           (3) A review of alternative concepts with regard  
2 to international norms in cyberspace offered by for-  
3 eign countries.

4           (4) A detailed description of new and evolving  
5 threats in cyberspace from foreign adversaries, state-  
6 sponsored actors, and private actors to—

7                   (A) United States national security;

8                   (B) Federal and private sector cyberspace  
9 infrastructure of the United States;

10                  (C) intellectual property in the United  
11 States; and

12                  (D) the privacy of citizens of the United  
13 States.

14           (5) A review of policy tools available to the  
15 President to deter and de-escalate tensions with for-  
16 eign countries, state-sponsored actors, and private  
17 actors regarding threats in cyberspace, the degree to  
18 which such tools have been used, and whether such  
19 tools have been effective deterrents.

20           (6) A review of resources required to conduct  
21 activities to build responsible norms of international  
22 cyber behavior.

23           (7) A plan of action, developed in consultation  
24 with relevant Federal departments and agencies as  
25 the President may direct, to guide the diplomacy of

1 the Department of State with regard to inclusion of  
2 cyber issues in mutual defense agreements.

3 (c) FORM OF STRATEGY.—

4 (1) PUBLIC AVAILABILITY.—The strategy re-  
5 quired under subsection (a) shall be available to the  
6 public in unclassified form, including through publi-  
7 cation in the Federal Register.

8 (2) CLASSIFIED ANNEX.—The strategy required  
9 under subsection (a) may include a classified annex,  
10 consistent with United States national security inter-  
11 ests, if the Secretary of State determines that such  
12 annex is appropriate.

13 (d) BRIEFING.—Not later than 30 days after the  
14 completion of the strategy required under subsection (a),  
15 the Secretary of State shall brief the appropriate congres-  
16 sional committees on the strategy, including any material  
17 contained in a classified annex.

18 (e) UPDATES.—The strategy required under sub-  
19 section (a) shall be updated—

20 (1) not later than 90 days after any material  
21 change to United States policy described in such  
22 strategy; and

23 (2) not later than 1 year after the inauguration  
24 of each new President.

1 (f) PREEXISTING REQUIREMENT.—The Rec-  
2 ommendations to the President on Protecting American  
3 Cyber Interests through International Engagement, pre-  
4 pared by the Office of the Coordinator for Cyber Issues  
5 on May 31, 2018, pursuant to section 3(c) of Executive  
6 Order 13800 (82 Fed. Reg. 22391), shall be deemed to  
7 satisfy the requirement under subsection (a).

8 **SEC. 8. ANNUAL COUNTRY REPORTS ON HUMAN RIGHTS**  
9 **PRACTICES.**

10 Section 116 of the Foreign Assistance Act of 1961  
11 (22 U.S.C. 2151n) is amended by adding at the end the  
12 following:

13 “(h)(1) The report required under subsection (d)  
14 shall include an assessment of freedom of expression with  
15 respect to electronic information in each foreign country  
16 that includes the following:

17 “(A) An assessment of the extent to which gov-  
18 ernment authorities in the country inappropriately  
19 attempt to filter, censor, or otherwise block or re-  
20 move nonviolent expression of political or religious  
21 opinion or belief through the Internet, including  
22 electronic mail, and a description of the means by  
23 which such authorities attempt to inappropriately  
24 block or remove such expression.

1           “(B) An assessment of the extent to which gov-  
2           ernment authorities in the country have persecuted  
3           or otherwise punished, arbitrarily and without due  
4           process, an individual or group for the nonviolent ex-  
5           pression of political, religious, or ideological opinion  
6           or belief through the Internet, including electronic  
7           mail.

8           “(C) An assessment of the extent to which gov-  
9           ernment authorities in the country have sought, in-  
10          appropriately and with malicious intent, to collect,  
11          request, obtain, or disclose without due process per-  
12          sonally identifiable information of a person in con-  
13          nection with that person’s nonviolent expression of  
14          political, religious, or ideological opinion or belief, in-  
15          cluding expression that would be protected by the  
16          International Covenant on Civil and Political Rights,  
17          adopted at New York December 16, 1966, and en-  
18          tered into force March 23, 1976, as interpreted by  
19          the United States.

20          “(D) An assessment of the extent to which wire  
21          communications and electronic communications are  
22          monitored without due process and in contravention  
23          to United States policy with respect to the principles  
24          of privacy, human rights, democracy, and rule of  
25          law.

1       “(2) In compiling data and making assessments  
2 under paragraph (1), United States diplomatic personnel  
3 should consult with relevant entities, including human  
4 rights organizations, the private sector, the governments  
5 of like-minded countries, technology and Internet compa-  
6 nies, and other appropriate nongovernmental organiza-  
7 tions or entities.

8       “(3) In this subsection—

9           “(A) the term ‘electronic communication’ has  
10 the meaning given the term in section 2510 of title  
11 18, United States Code;

12           “(B) the term ‘Internet’ has the meaning given  
13 the term in section 231(e)(3) of the Communications  
14 Act of 1934 (47 U.S.C. 231(e)(3));

15           “(C) the term ‘personally identifiable informa-  
16 tion’ means data in a form that identifies a par-  
17 ticular person; and

18           “(D) the term ‘wire communication’ has the  
19 meaning given the term in section 2510 of title 18,  
20 United States Code.”.

21 **SEC. 9. GAO REPORT ON CYBER THREATS AND DATA MIS-**  
22 **USE.**

23       Not later than 1 year after the date of the enactment  
24 of this Act, the Comptroller General of the United States

1 shall submit a report and provide a briefing to the appro-  
2 priate congressional committees that includes—

3 (1) a description of the primary threats to the  
4 personal information of United States citizens from  
5 international actors within the cyberspace domain;

6 (2) an assessment of the extent to which United  
7 States diplomatic processes and other efforts with  
8 foreign countries, including through multilateral  
9 fora, bilateral engagements, and negotiated cyber-  
10 space agreements, strengthen the protections of  
11 United States citizens' personal information;

12 (3) an assessment of the Department of State's  
13 report in response to Executive Order 13800 (82  
14 Fed. Reg. 22391), which documents an engagement  
15 strategy for international cooperation in cybersecu-  
16 rity and the extent to which this strategy addresses  
17 protections of United States citizens' personal infor-  
18 mation;

19 (4) recommendations for United States policy-  
20 makers on methods to properly address and  
21 strengthen the protections of United States citizens'  
22 personal information from misuse by international  
23 actors; and

24 (5) any other matters deemed relevant by the  
25 Comptroller General.

1 **SEC. 10. SENSE OF CONGRESS ON CYBERSECURITY SANC-**  
2 **TIONS AGAINST NORTH KOREA AND CYBER-**  
3 **SECURITY LEGISLATION IN VIETNAM.**

4 It is the sense of Congress that—

5 (1) the President should designate all entities  
6 that knowingly engage in significant activities under-  
7 mining cybersecurity through the use of computer  
8 networks or systems against foreign persons, govern-  
9 ments, or other entities on behalf of the Government  
10 of North Korea, consistent with section 209(b) of  
11 the North Korea Sanctions and Policy Enhancement  
12 Act of 2016 (22 U.S.C. 9229(b));

13 (2) the cybersecurity law approved by the Na-  
14 tional Assembly of Vietnam on June 12, 2018—

15 (A) may not be consistent with inter-  
16 national trade standards; and

17 (B) may endanger the privacy of citizens  
18 of Vietnam; and

19 (3) the Government of Vietnam should work  
20 with the United States and other countries to ensure  
21 that such law meets all relevant international stand-  
22 ards.

23 **SEC. 11. RULE OF CONSTRUCTION.**

24 (a) **RULE OF CONSTRUCTION.**—Nothing in this Act  
25 may be construed to infringe upon the related functions

- 1 of any Executive agency vested in such agency under any
- 2 provision of law.

