

Union Calendar No. 357

115TH CONGRESS
2D SESSION

H. R. 3776

[Report No. 115–483]

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

IN THE HOUSE OF REPRESENTATIVES

SEPTEMBER 14, 2017

Mr. ROYCE of California (for himself, Mr. ENGEL, Mr. McCAUL, Mr. TED LIEU of California, Mr. FITZPATRICK, Mrs. DINGELL, Mr. POE of Texas, Mr. RUPPERSBERGER, Mr. YOHIO, Mr. LANGEVIN, Mrs. WAGNER, and Mr. BRENDAN F. BOYLE of Pennsylvania) introduced the following bill; which was referred to the Committee on Foreign Affairs

JANUARY 3, 2018

Additional sponsors: Mr. CHABOT, Mr. CONNOLLY, Ms. ROSEN, Mr. HIMES, Mr. KINZINGER, Mr. SHERMAN, Mr. GRAVES of Georgia, Mr. MEADOWS, Mr. FRANCIS ROONEY of Florida, Mr. MARINO, Mr. CICILLINE, Ms. FRANKEL of Florida, Mr. WILSON of South Carolina, and Mrs. MURPHY of Florida

JANUARY 3, 2018

Reported with an amendment, committed to the Committee of the Whole House on the State of the Union, and ordered to be printed

[Strike out all after the enacting clause and insert the part printed in *italic*]

[For text of introduced bill, see copy of bill as introduced on September 14, 2017]

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.**

4 *This Act may be cited as the “Cyber Diplomacy Act*
5 *of 2017”.*

6 **SEC. 2. FINDINGS.**

7 *Congress finds the following:*

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

18 *(2) The Group of Governmental Experts (GGE)*
19 *on Developments in the Field of Information and*
20 *Telecommunications in the Context of International*
21 *Security, established by the United Nations General*
22 *Assembly, concluded in its June 24, 2013, report*
23 *“that State sovereignty and the international norms*
24 *and principles that flow from it apply to States’ con-*
25 *duct of [information and communications technology*

1 or ICT] related activities and to their jurisdiction
2 over ICT infrastructure with their territory.”.

3 (3) On January 13, 2015, China, Kazakhstan,
4 Kyrgyzstan, Russia, Tajikistan, and Uzbekistan pro-
5 posed a troubling international code of conduct for
6 information security which defines responsible State
7 behavior in cyberspace to include “curbing the dis-
8 semination of information” and the “right to inde-
9 pendent control of information and communications
10 technology” when a country’s political security is
11 threatened.

12 (4) The July 22, 2015, GGE consensus report
13 found that, “norms of responsible State behavior can
14 reduce risks to international peace, security and sta-
15 bility.”.

16 (5) On September 25, 2015, the United States
17 and China announced a commitment “that neither
18 country’s government will conduct or knowingly sup-
19 port cyber-enabled theft of intellectual property, in-
20 cluding trade secrets or other confidential business in-
21 formation, with the intent of providing competitive
22 advantages to companies or commercial sectors.”.

23 (6) At the Antalya Summit from November 15–
24 16, 2015, the Group of 20 (G20) Leaders’ Commu-
25 nique affirmed the applicability of international law

1 to State behavior in cyberspace, called on States to re-
2 frain from cyber-enabled theft of intellectual property
3 for commercial gain, and endorsed the view that all
4 States should abide by norms of responsible behavior.

5 (7) The March 2016 Department of State Inter-
6 national Cyberspace Policy Strategy noted that, “the
7 Department of State anticipates a continued increase
8 and expansion of our cyber-focused diplomatic efforts
9 for the foreseeable future.”.

10 (8) On December 1, 2016, the Commission on
11 Enhancing National Cybersecurity established within
12 the Department of Commerce recommended “the
13 President should appoint an Ambassador for Cyberse-
14 curity to lead U.S. engagement with the international
15 community on cybersecurity strategies, standards,
16 and practices.”.

17 (9) The 2017 Group of 7 (G7) Declaration on
18 Responsible States Behavior in Cyberspace recognized
19 on April 11, 2017, “the urgent necessity of increased
20 international cooperation to promote security and
21 stability in cyberspace . . . consisting of the applica-
22 bility of existing international law to State behavior
23 in cyberspace, the promotion of voluntary, non-bind-
24 ing norms of responsible State behavior during peace-

1 *time” and reaffirmed “that the same rights that peo-*
2 *ple have offline must also be protected online.”.*

3 *(10) In testimony before the Select Committee on*
4 *Intelligence of the Senate on May 11, 2017, the Direc-*
5 *tor of National Intelligence identified six cyber threat*
6 *actors, including Russia for “efforts to influence the*
7 *2016 US election”; China, for “actively targeting the*
8 *US Government, its allies, and US companies for*
9 *cyber espionage”; Iran for “leverage[ing] cyber espio-*
10 *nage, propaganda, and attacks to support its security*
11 *priorities, influence events and foreign perceptions,*
12 *and counter threats”; North Korea for “previously*
13 *conduct[ing] cyber-attacks against US commercial en-*
14 *tities—specifically, Sony Pictures Entertainment in*
15 *2014”; terrorists, who “use the Internet to organize,*
16 *recruit, spread propaganda, raise funds, collect intel-*
17 *ligence, inspire action by followers, and coordinate*
18 *operations”; and criminals who “are also developing*
19 *and using sophisticated cyber tools for a variety of*
20 *purposes including theft, extortion, and facilitation of*
21 *other criminal activities”.*

22 *(11) On May 11, 2017, President Trump issued*
23 *Presidential Executive Order 13800 on Strengthening*
24 *the Cybersecurity of Federal Networks and Infrastruc-*
25 *ture which designated the Secretary of State to lead*

1 *an interagency effort to develop strategic options for*
2 *the President to deter adversaries from cyber threats*
3 *and an engagement strategy for international co-*
4 *operation in cybersecurity, noting that “the United*
5 *States is especially dependent on a globally secure*
6 *and resilient internet and must work with allies and*
7 *other partners” toward maintaining “the policy of*
8 *the executive branch to promote an open, interoper-*
9 *able, reliable, and secure internet that fosters effi-*
10 *ciency, innovation, communication, and economic*
11 *prosperity, while respecting privacy and guarding*
12 *against deception, fraud, and theft.”.*

13 **SEC. 3. UNITED STATES INTERNATIONAL CYBERSPACE POL-**
14 **ICY.**

15 *(a) IN GENERAL.—Congress declares that it is the pol-*
16 *icy of the United States to work internationally with allies*
17 *and other partners to promote an open, interoperable, reli-*
18 *able, unfettered, and secure internet governed by the multi-*
19 *stakeholder model which promotes human rights, democ-*
20 *racy, and rule of law, including freedom of expression, in-*
21 *novation, communication, and economic prosperity, while*
22 *respecting privacy and guarding against deception, fraud,*
23 *and theft.*

24 *(b) IMPLEMENTATION.—In implementing the policy*
25 *described in subsection (a), the President, in consultation*

1 *with outside actors, including technology companies, non-*
2 *governmental organizations, security researchers, and other*
3 *relevant stakeholders, shall pursue the following objectives*
4 *in the conduct of bilateral and multilateral relations:*

5 (1) *Clarifying the applicability of international*
6 *laws and norms, including the law of armed conflict,*
7 *to the use of ICT.*

8 (2) *Clarifying that countries that fall victim to*
9 *malicious cyber activities have the right to take pro-*
10 *portionate countermeasures under international law,*
11 *provided such measures do not violate a fundamental*
12 *human right or peremptory norm.*

13 (3) *Reducing and limiting the risk of escalation*
14 *and retaliation in cyberspace, such as massive denial-*
15 *of-service attacks, damage to critical infrastructure,*
16 *or other malicious cyber activity that impairs the use*
17 *and operation of critical infrastructure that provides*
18 *services to the public.*

19 (4) *Cooperating with like-minded democratic*
20 *countries that share common values and cyberspace*
21 *policies with the United States, including respect for*
22 *human rights, democracy, and rule of law, to advance*
23 *such values and policies internationally.*

1 (5) *Securing and implementing commitments on*
2 *responsible country behavior in cyberspace based*
3 *upon accepted norms, including the following:*

4 (A) *Countries should not conduct or know-*
5 *ingly support cyber-enabled theft of intellectual*
6 *property, including trade secrets or other con-*
7 *fidential business information, with the intent of*
8 *providing competitive advantages to companies*
9 *or commercial sectors.*

10 (B) *Countries should cooperate in devel-*
11 *oping and applying measures to increase sta-*
12 *bility and security in the use of ICTs and to pre-*
13 *vent ICT practices that are acknowledged to be*
14 *harmful or that may pose threats to inter-*
15 *national peace and security.*

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

20 (D) *Countries should not conduct or know-*
21 *ingly support ICT activity that, contrary to*
22 *international law, intentionally damages or oth-*
23 *erwise impairs the use and operation of critical*
24 *infrastructure, and should take appropriate*

1 *measures to protect their critical infrastructure*
2 *from ICT threats.*

3 *(E) Countries should not conduct or know-*
4 *ingly support malicious international activity*
5 *that, contrary to international law, harms the*
6 *information systems of authorized emergency re-*
7 *sponse teams (sometimes known as “computer*
8 *emergency response teams” or “cybersecurity in-*
9 *cident response teams”)* *or related private sector*
10 *companies of another country.*

11 *(F) Countries should identify economic*
12 *drivers and incentives to promote securely-de-*
13 *signed ICT products and to develop policy and*
14 *legal frameworks to promote the development of*
15 *secure internet architecture.*

16 *(G) Countries should respond to appro-*
17 *priate requests for assistance to mitigate mali-*
18 *cious ICT activity aimed at the critical infra-*
19 *structure of another country emanating from*
20 *their territory.*

21 *(H) Countries should not restrict cross-bor-*
22 *der data flows or require local storage or proc-*
23 *essing of data.*

24 *(I) Countries should protect the exercise of*
25 *human rights and fundamental freedoms on the*

1 *Internet and commit to the principle that the*
 2 *human rights that people have offline enjoy the*
 3 *same protections online.*

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

5 (a) *OFFICE OF CYBER ISSUES.*—*Section 1 of the State*
 6 *Department Basic Authorities Act of 1956 (22 U.S.C.*
 7 *2651a) is amended—*

8 (1) *by redesignating subsection (g) as subsection*
 9 (h); *and*

10 (2) *by inserting after subsection (f) the following*
 11 *new subsection:*

12 “(g) *OFFICE OF CYBER ISSUES.*—

13 “(1) *IN GENERAL.*—*There is established an Of-*
 14 *fice of Cyber Issues (in this subsection referred to as*
 15 *the ‘Office’). The head of the Office shall have the rank*
 16 *and status of ambassador and be appointed by the*
 17 *President, by and with the advice and consent of the*
 18 *Senate.*

19 “(2) *DUTIES.*—

20 “(A) *IN GENERAL.*—*The head of the Office*
 21 *shall perform such duties and exercise such pow-*
 22 *ers as the Secretary of State shall prescribe, in-*
 23 *cluding implementing the policy of the United*
 24 *States described in section 3 of the Cyber Diplo-*
 25 *macy Act of 2017.*

1 “(B) *DUTIES DESCRIBED.*—*The principal*
2 *duties of the head of the Office shall be to—*

3 “(i) *serve as the principal cyber-policy*
4 *official within the senior management of the*
5 *Department of State and advisor to the Sec-*
6 *retary of State for cyber issues;*

7 “(ii) *lead the Department of State’s*
8 *diplomatic cyberspace efforts generally, in-*
9 *cluding relating to international cybersecu-*
10 *rity, internet access, internet freedom, dig-*
11 *ital economy, cybercrime, deterrence and*
12 *international responses to cyber threats;*

13 “(iii) *promote an open, interoperable,*
14 *reliable, unfettered, and secure information*
15 *and communications technology infrastruc-*
16 *ture globally;*

17 “(iv) *represent the Secretary of State*
18 *in interagency efforts to develop and ad-*
19 *vance the United States international cyber-*
20 *space policy;*

21 “(v) *coordinate within the Department*
22 *of State and with other components of the*
23 *United States Government cyberspace efforts*
24 *and other relevant functions, including*
25 *countering terrorists’ use of cyberspace; and*

1 “(vi) act as liaison to public and pri-
 2 vate sector entities on relevant cyberspace
 3 issues.

4 “(3) QUALIFICATIONS.—The head of the Office
 5 should be an individual of demonstrated competency
 6 in the field of—

7 “(A) cybersecurity and other relevant cyber
 8 issues; and

9 “(B) international diplomacy.

10 “(4) ORGANIZATIONAL PLACEMENT.—The head of
 11 the Office shall report to the Under Secretary for Po-
 12 litical Affairs or official holding a higher position in
 13 the Department of State.

14 “(5) RULE OF CONSTRUCTION.—Nothing in this
 15 subsection may be construed as precluding—

16 “(A) the Office from being elevated to a Bu-
 17 reau of the Department of State; and

18 “(B) the head of the Office from being ele-
 19 vated to an Assistant Secretary, if such an As-
 20 sistant Secretary position does not increase the
 21 number of Assistant Secretary positions at the
 22 Department above the number authorized under
 23 subsection (c)(1).”.

24 (b) SENSE OF CONGRESS.—It is the sense of Congress
 25 that the Office of Cyber Issues established under section 1(g)

1 *of the State Department Basic Authorities Act of 1956 (as*
 2 *amended by subsection (a) of this section) should be a Bu-*
 3 *reau of the Department of State headed by an Assistant*
 4 *Secretary, subject to the rule of construction specified in*
 5 *paragraph (5)(B) of such section 1(g).*

6 (c) *UNITED NATIONS.—The Permanent Representative*
 7 *of the United States to the United Nations shall use the*
 8 *voice, vote, and influence of the United States to oppose any*
 9 *measure that is inconsistent with the United States inter-*
 10 *national cyberspace policy described in section 3.*

11 **SEC. 5. INTERNATIONAL CYBERSPACE EXECUTIVE AR-**
 12 **RANGEMENTS.**

13 (a) *IN GENERAL.—The President is encouraged to*
 14 *enter into executive arrangements with foreign governments*
 15 *that support the United States international cyberspace*
 16 *policy described in section 3.*

17 (b) *TRANSMISSION TO CONGRESS.—The text of any ex-*
 18 *ecutive arrangement (including the text of any oral ar-*
 19 *rangement, which shall be reduced to writing) entered into*
 20 *by the United States under subsection (a) shall be trans-*
 21 *mitted to the Committee on Foreign Affairs of the House*
 22 *of Representatives and the Committee on Foreign Relations*
 23 *of the Senate not later than five days after such arrange-*
 24 *ment is signed or otherwise agreed to, together with an ex-*
 25 *planation of such arrangement, its purpose, how such ar-*

1 *rangement is consistent with the United States inter-*
2 *national cyberspace policy described in section 3, and how*
3 *such arrangement will be implemented.*

4 (c) *STATUS REPORT.*—*Not later than one year after*
5 *the text of an executive arrangement is transmitted to Con-*
6 *gress pursuant to subsection (b) and annually thereafter for*
7 *seven years, or until such an arrangement has been discon-*
8 *tinued, the President shall report to the Committee on For-*
9 *ign Affairs of the House of Representatives and the Com-*
10 *mittee on Foreign Relations of the Senate on the status of*
11 *such arrangement, including an evidence-based assessment*
12 *of whether all parties to such arrangement have fulfilled*
13 *their commitments under such arrangement and if not,*
14 *what steps the United States has taken or plans to take*
15 *to ensure all such commitments are fulfilled, whether the*
16 *stated purpose of such arrangement is being achieved, and*
17 *whether such arrangement positively impacts building of*
18 *cyber norms internationally. Each such report shall include*
19 *metrics to support its findings.*

20 (d) *EXISTING EXECUTIVE ARRANGEMENTS.*—*Not later*
21 *than 60 days after the date of the enactment of this Act,*
22 *the President shall satisfy the requirements of subsection (c)*
23 *for the following executive arrangements already in effect:*

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) *Any other similar bilateral or multilateral*
19 *arrangement announced before the date of the enact-*
20 *ment of this Act.*

21 **SEC. 6. INTERNATIONAL STRATEGY FOR CYBERSPACE.**

22 (a) *STRATEGY REQUIRED.*—*Not later than one year*
23 *after the date of the enactment of this Act, the Secretary*
24 *of State, in coordination with the heads of other relevant*
25 *Federal departments and agencies, shall produce a strategy*

1 *relating to United States international policy with regard*
2 *to cyberspace.*

3 (b) *ELEMENTS.*—*The strategy required under sub-*
4 *section (a) shall include the following:*

5 (1) *A review of actions and activities undertaken*
6 *to support the United States international cyberspace*
7 *policy described in section 3.*

8 (2) *A plan of action to guide the diplomacy of*
9 *the Department of State with regard to foreign coun-*
10 *tries, including conducting bilateral and multilateral*
11 *activities to develop the norms of responsible inter-*
12 *national behavior in cyberspace, and status review of*
13 *existing efforts in multilateral fora to obtain agree-*
14 *ments on international norms in cyberspace.*

15 (3) *A review of alternative concepts with regard*
16 *to international norms in cyberspace offered by for-*
17 *foreign countries.*

18 (4) *A detailed description of new and evolving*
19 *threats to United States national security in cyber-*
20 *space from foreign countries, State-sponsored actors,*
21 *and private actors to Federal and private sector in-*
22 *frastructure of the United States, intellectual property*
23 *in the United States, and the privacy of citizens of*
24 *the United States.*

1 (5) *A review of policy tools available to the*
2 *President to deter and de-escalate tensions with for-*
3 *foreign countries, State-sponsored actors, and private ac-*
4 *tors regarding threats in cyberspace, and to what de-*
5 *gree such tools have been used and whether or not*
6 *such tools have been effective.*

7 (6) *A review of resources required to conduct ac-*
8 *tivities to build responsible norms of international*
9 *cyber behavior.*

10 (7) *A clarification of the applicability of inter-*
11 *national laws and norms, including the law of armed*
12 *conflict, to the use of ICT.*

13 (8) *A clarification that countries that fall victim*
14 *to malicious cyber activities have the right to take*
15 *proportionate countermeasures under international*
16 *law, including exercising the right to collective and*
17 *individual self-defense.*

18 (9) *A plan of action to guide the diplomacy of*
19 *the Department of State with regard to existing mu-*
20 *tual defense agreements, including the inclusion in*
21 *such agreements of information relating to the appli-*
22 *cability of malicious cyber activities in triggering*
23 *mutual defense obligations.*

24 (c) *FORM OF STRATEGY.—*

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

5 (2) *CLASSIFIED ANNEX.*—

6 (A) *IN GENERAL.*—*If the Secretary of State*
 7 *determines that such is appropriate, the strategy*
 8 *required under subsection (a) may include a*
 9 *classified annex consistent with United States*
 10 *national security interests.*

11 (B) *RULE OF CONSTRUCTION.*—*Nothing in*
 12 *this subsection may be construed as authorizing*
 13 *the public disclosure of an unclassified annex*
 14 *under subparagraph (A).*

15 (d) *BRIEFING.*—*Not later than 30 days after the pro-*
 16 *duction of the strategy required under subsection (a), the*
 17 *Secretary of State shall brief the Committee on Foreign Af-*
 18 *airs of the House of Representatives and the Committee on*
 19 *Foreign Relations of the Senate on such strategy, including*
 20 *any material contained in a classified annex.*

21 (e) *UPDATES.*—*The strategy required under subsection*
 22 *(a) shall be updated—*

23 (1) *not later than 90 days after there has been*
 24 *any material change to United States policy as de-*
 25 *scribed in such strategy; and*

1 (2) *not later than one year after each inaugura-*
 2 *tion of a new President.*

3 (f) *PREEXISTING REQUIREMENT.*—*Upon the produc-*
 4 *tion and publication of the report required under section*
 5 *3(c) of the Presidential Executive Order 13800 on Strength-*
 6 *ening the Cybersecurity of Federal Networks and Critical*
 7 *Infrastructure on May 11, 2017, such report shall be consid-*
 8 *ered as satisfying the requirement under subsection (a) of*
 9 *this section.*

10 **SEC. 7. ANNUAL COUNTRY REPORTS ON HUMAN RIGHTS**
 11 **PRACTICES.**

12 (a) *REPORT RELATING TO ECONOMIC ASSISTANCE.*—
 13 *Section 116 of the Foreign Assistance Act of 1961 (22*
 14 *U.S.C. 2151n) is amended by adding at the end the fol-*
 15 *lowing new subsection:*

16 “(h)(1) *The report required by subsection (d) shall in-*
 17 *clude an assessment of freedom of expression with respect*
 18 *to electronic information in each foreign country. Such as-*
 19 *essment shall consist of the following:*

20 “(A) *An assessment of the extent to which gov-*
 21 *ernment authorities in each country inappropriately*
 22 *attempt to filter, censor, or otherwise block or remove*
 23 *nonviolent expression of political or religious opinion*
 24 *or belief via the internet, including electronic mail, as*

1 *well as a description of the means by which such au-*
2 *thorities attempt to block or remove such expression.*

3 *“(B) An assessment of the extent to which gov-*
4 *ernment authorities in each country have persecuted*
5 *or otherwise punished an individual or group for the*
6 *nonviolent expression of political, religious, or ideo-*
7 *logical opinion or belief via the internet, including*
8 *electronic mail.*

9 *“(C) An assessment of the extent to which gov-*
10 *ernment authorities in each country have sought to*
11 *inappropriately collect, request, obtain, or disclose*
12 *personally identifiable information of a person in*
13 *connection with such 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 *“(D) An assessment of the extent to which wire*
18 *communications and electronic communications are*
19 *monitored without regard to the principles of privacy,*
20 *human rights, democracy, and rule of law.*

21 *“(2) In compiling data and making assessments for*
22 *the purposes of paragraph (1), United States diplomatic*
23 *personnel shall consult with human rights organizations,*
24 *technology and internet companies, and other appropriate*
25 *nongovernmental organizations.*

1 “(3) *In this subsection—*

2 “(A) *the term ‘electronic communication’ has the*
3 *meaning given such term in section 2510 of title 18,*
4 *United States Code;*

5 “(B) *the term ‘internet’ has the meaning given*
6 *such term in section 231(e)(3) of the Communications*
7 *Act of 1934 (47 U.S.C. 231(e)(3));*

8 “(C) *the term ‘personally identifiable informa-*
9 *tion’ means data in a form that identifies a par-*
10 *ticular person; and*

11 “(D) *the term ‘wire communication’ has the*
12 *meaning given such term in section 2510 of title 18,*
13 *United States Code.”.*

14 (b) *REPORT RELATING TO SECURITY ASSISTANCE.—*
15 *Section 502B of the Foreign Assistance Act of 1961 (22*
16 *U.S.C. 2304) is amended—*

17 (1) *by redesignating the second subsection (i) (re-*
18 *lating to child marriage status) as subsection (j); and*

19 (2) *by adding at the end the following new sub-*
20 *section:*

21 “(k)(1) *The report required by subsection (b) shall in-*
22 *clude an assessment of freedom of expression with respect*
23 *to electronic information in each foreign country. Such as-*
24 *essment shall consist of the following:*

1 “(A) *An assessment of the extent to which gov-*
2 *ernment authorities in each country inappropriately*
3 *attempt to filter, censor, or otherwise block or remove*
4 *nonviolent expression of political or religious opinion*
5 *or belief via the internet, including electronic mail, as*
6 *well as a description of the means by which such au-*
7 *thorities attempt to block or remove such expression.*

8 “(B) *An assessment of the extent to which gov-*
9 *ernment authorities in each country have persecuted*
10 *or otherwise punished an individual or group for the*
11 *nonviolent expression of political, religious, or ideo-*
12 *logical opinion or belief via the internet, including*
13 *electronic mail.*

14 “(C) *An assessment of the extent to which gov-*
15 *ernment authorities in each country have sought to*
16 *inappropriately collect, request, obtain, or disclose*
17 *personally identifiable information of a person in*
18 *connection with such person’s nonviolent expression of*
19 *political, religious, or ideological opinion or belief, in-*
20 *cluding expression that would be protected by the*
21 *International Covenant on Civil and Political Rights.*

22 “(D) *An assessment of the extent to which wire*
23 *communications and electronic communications are*
24 *monitored without regard to the principles of privacy,*
25 *human rights, democracy, and rule of law.*

1 “(2) *In compiling data and making assessments for*
2 *the purposes of paragraph (1), United States diplomatic*
3 *personnel shall consult with human rights organizations,*
4 *technology and internet companies, and other appropriate*
5 *nongovernmental organizations.*

6 “(3) *In this subsection—*

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

10 “(B) *the term ‘internet’ has the meaning given*
11 *such term in section 231(e)(3) of the Communications*
12 *Act of 1934 (47 U.S.C. 231(e)(3));*

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

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

Union Calendar No. 357

115TH CONGRESS
2D Session

H. R. 3776

[Report No. 115-483]

A BILL

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

JANUARY 3, 2018

Reported with an amendment, committed to the Committee of the Whole House on the State of the Union, and ordered to be printed