

117TH CONGRESS  
1ST SESSION

# H. R. 1251

---

## AN ACT

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,*

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

2 (a) SHORT TITLE.—This Act may be cited as the  
3 “Cyber Diplomacy Act of 2021”.

4 (b) TABLE OF CONTENTS.—The table of contents for  
5 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 diplomacy.
- Sec. 10. Sense of congress on cybersecurity sanctions against north korea and  
cybersecurity legislation in vietnam.

6 **SEC. 2. FINDINGS.**

7 Congress makes the following findings:

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 behav-  
16 ior guide states’ actions, sustain partnerships, and  
17 support the rule of law in cyberspace”.

18 (2) In its June 24, 2013, report, the Group of  
19 Governmental Experts on Developments in the Field  
20 of Information and Telecommunications in the Con-

1 text of International Security (referred to in this  
2 section as “GGE”), established by the United Na-  
3 tions General Assembly, concluded that “State sov-  
4 ereignty and the international norms and principles  
5 that flow from it apply to States’ conduct of [infor-  
6 mation and communications technology] ICT-related  
7 activities and to their jurisdiction over ICT infra-  
8 structure with their territory”.

9 (3) In January 2015, China, Kazakhstan,  
10 Kyrgyzstan, Russia, Tajikistan, and Uzbekistan pro-  
11 posed a troubling international code of conduct for  
12 information security, which could be used as a pre-  
13 text for restricting political dissent, and includes  
14 “curbing the dissemination of information that in-  
15 cites terrorism, separatism or extremism or that in-  
16 flames hatred on ethnic, racial or religious grounds”.

17 (4) In its July 22, 2015, consensus report,  
18 GGE found that “norms of responsible State behav-  
19 ior can reduce risks to international peace, security  
20 and stability”.

21 (5) On September 25, 2015, the United States  
22 and China announced a commitment that neither  
23 country’s government “will conduct or knowingly  
24 support cyber-enabled theft of intellectual property,  
25 including trade secrets or other confidential business

1 information, with the intent of providing competitive  
2 advantages to companies or commercial sectors”.

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

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

8 (B) called on states to refrain from cyber-  
9 enabled theft of intellectual property for com-  
10 mercial gain; and

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

13 (7) The March 2016 Department of State  
14 International Cyberspace Policy Strategy noted that  
15 “the Department of State anticipates a continued in-  
16 crease and expansion of our cyber-focused diplomatic  
17 efforts for the foreseeable future”.

18 (8) On December 1, 2016, the Commission on  
19 Enhancing National Cybersecurity, which was estab-  
20 lished within the Department of Commerce by Exec-  
21 utive Order No. 13718 (81 Fed. Reg. 7441), rec-  
22 ommended that “the President should appoint an  
23 Ambassador for Cybersecurity to lead U.S. engage-  
24 ment with the international community on cyberse-  
25 curity strategies, standards, and practices”.

1           (9) On April 11, 2017, the 2017 Group of 7  
2       Declaration on Responsible States Behavior in  
3       Cyberspace—

4           (A) recognized “the urgent necessity of in-  
5       creased international cooperation to promote se-  
6       curity and stability in cyberspace”;

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

18          (C) reaffirmed that “the same rights that  
19      people have offline must also be protected on-  
20      line”.

21          (10) In testimony before the Select Committee  
22      on Intelligence of the Senate on May 11, 2017, Di-  
23      rector of National Intelligence Daniel R. Coats iden-  
24      tified six cyber threat actors, including—

1 (A) Russia, for “efforts to influence the  
2 2016 U.S. election”;

3 (B) China, for “actively targeting the U.S.  
4 Government, its allies, and U.S. companies for  
5 cyber espionage”;

6 (C) Iran, for “leverag[ing] cyber espionage,  
7 propaganda, and attacks to support its security  
8 priorities, influence events and foreign percep-  
9 tions, and counter threats”;

10 (D) North Korea, for “previously  
11 conduct[ing] cyber-attacks against U.S. com-  
12 mercial entities—specifically, Sony Pictures En-  
13 tertainment in 2014”;

14 (E) terrorists, who “use the Internet to or-  
15 ganize, recruit, spread propaganda, raise funds,  
16 collect intelligence, inspire action by followers,  
17 and coordinate operations”; and

18 (F) criminals, who “are also developing  
19 and using sophisticated cyber tools for a variety  
20 of purposes including theft, extortion, and fa-  
21 cilitation of other criminal activities”.

22 (11) On May 11, 2017, President Donald J.  
23 Trump issued Executive Order No. 13800 (82 Fed.  
24 Reg. 22391), entitled “Strengthening the Cybersecu-

1 rity of Federal Networks and Infrastructure”,  
2 which—

3 (A) designates the Secretary of State to  
4 lead an interagency effort to develop an engage-  
5 ment strategy for international cooperation in  
6 cybersecurity; and

7 (B) notes that “the United States is espe-  
8 cially dependent on a globally secure and resil-  
9 ient internet and must work with allies and  
10 other partners toward maintaining \* \* \* the  
11 policy of the executive branch to promote an  
12 open, interoperable, reliable, and secure internet  
13 that fosters efficiency, innovation, communica-  
14 tion, and economic prosperity, while respecting  
15 privacy and guarding against disruption, fraud,  
16 and theft”.

17 **SEC. 3. DEFINITIONS.**

18 In this Act:

19 (1) APPROPRIATE CONGRESSIONAL COMMIT-  
20 TEES.—The term “appropriate congressional com-  
21 mittees” means the Committee on Foreign Relations  
22 of the Senate and the Committee on Foreign Affairs  
23 of the House of Representatives.

24 (2) INFORMATION AND COMMUNICATIONS  
25 TECHNOLOGY; ICT.—The terms “information and

1       communications technology” and “ICT” include  
2       hardware, software, and other products or services  
3       primarily intended to fulfill or enable the function of  
4       information processing and communication by elec-  
5       tronic means, including transmission and display, in-  
6       cluding via the Internet.

7               (3) EXECUTIVE AGENCY.—The term “Executive  
8       agency” has the meaning given the term in section  
9       105 of title 5, United States Code.

10 **SEC. 4. UNITED STATES INTERNATIONAL CYBERSPACE**  
11 **POLICY.**

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

16               (1) promotes human rights, democracy, and  
17       rule of law, including freedom of expression, innova-  
18       tion, communication, and economic prosperity; and

19               (2) respects privacy and guards against decep-  
20       tion, fraud, and theft.

21       (b) IMPLEMENTATION.—In implementing the policy  
22 described in subsection (a), the President, in consultation  
23 with outside actors, including private sector companies,  
24 nongovernmental organizations, security researchers, and



1 other relevant stakeholders, in the conduct of bilateral and  
2 multilateral relations, shall pursue the following objectives:

3 (1) Clarifying the applicability of international  
4 laws and norms to the use of ICT.

5 (2) Reducing and limiting the risk of escalation  
6 and retaliation in cyberspace, damage to critical in-  
7 frastructure, and other malicious cyber activity that  
8 impairs the use and operation of critical infrastruc-  
9 ture that provides services to the public.

10 (3) Cooperating with like-minded democratic  
11 countries that share common values and cyberspace  
12 policies with the United States, including respect for  
13 human rights, democracy, and the rule of law, to ad-  
14 vance such values and policies internationally.

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

19 (5) Securing and implementing commitments  
20 on responsible country behavior in cyberspace based  
21 upon accepted norms, including the following:

22 (A) Countries should not conduct, or  
23 knowingly support, cyber-enabled theft of intel-  
24 lectual property, including trade secrets or  
25 other confidential business information, with

1 the intent of providing competitive advantages  
2 to companies or commercial sectors.

3 (B) Countries should take all appropriate  
4 and reasonable efforts to keep their territories  
5 clear of intentionally wrongful acts using ICTs  
6 in violation of international commitments.

7 (C) Countries should not conduct or know-  
8 ingly support ICT activity that, contrary to  
9 international law, intentionally damages or oth-  
10 erwise impairs the use and operation of critical  
11 infrastructure providing services to the public,  
12 and should take appropriate measures to pro-  
13 tect their critical infrastructure from ICT  
14 threats.

15 (D) Countries should not conduct or know-  
16 ingly support malicious international activity  
17 that, contrary to international law, harms the  
18 information systems of authorized emergency  
19 response teams (also known as “computer  
20 emergency response teams” or “cybersecurity  
21 incident response teams”) of another country or  
22 authorize emergency response teams to engage  
23 in malicious international activity.

24 (E) Countries should respond to appro-  
25 priate requests for assistance to mitigate mali-

1           cious ICT activity emanating from their terri-  
2           tory and aimed at the critical infrastructure of  
3           another country.

4           (F) Countries should not restrict cross-bor-  
5           der data flows or require local storage or proc-  
6           essing of data.

7           (G) Countries should protect the exercise  
8           of human rights and fundamental freedoms on  
9           the Internet and commit to the principle that  
10          the human rights that people have offline  
11          should also be protected online.

12          (6) Advancing, encouraging, and supporting the  
13          development and adoption of internationally recog-  
14          nized technical standards and best practices.

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

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

19               (1) by redesignating subsection (g) as sub-  
20               section (h); and

21               (2) by inserting after subsection (f) the fol-  
22               lowing new subsection:

23          “(g) BUREAU OF INTERNATIONAL CYBERSPACE POL-  
24          ICY.—

1           “(1) IN GENERAL.—There is established, within  
2           the Department of State, a Bureau of International  
3           Cyberspace Policy (referred to in this subsection as  
4           the ‘Bureau’). The head of the Bureau shall have  
5           the rank and status of ambassador and shall be ap-  
6           pointed by the President, by and with the advice and  
7           consent of the Senate.

8           “(2) DUTIES.—

9                   “(A) IN GENERAL.—The head of the Bu-  
10           reau shall perform such duties and exercise  
11           such powers as the Secretary of State shall pre-  
12           scribe, including implementing the policy of the  
13           United States described in section 4 of the  
14           Cyber Diplomacy Act of 2021.

15                   “(B) DUTIES DESCRIBED.—The principal  
16           duties and responsibilities of the head of the  
17           Bureau shall be—

18                           “(i) to serve as the principal cyber-  
19           space policy official within the senior man-  
20           agement of the Department of State and  
21           as the advisor to the Secretary of State for  
22           cyberspace issues;

23                           “(ii) to lead the Department of  
24           State’s diplomatic cyberspace efforts, in-  
25           cluding efforts relating to international cy-

1           bersecurity, Internet access, Internet free-  
2           dom, digital economy, cybercrime, deter-  
3           rence and international responses to cyber  
4           threats, and other issues that the Sec-  
5           retary assigns to the Bureau;

6           “(iii) to coordinate cyberspace policy  
7           and other relevant functions within the De-  
8           partment of State and with other compo-  
9           nents of the United States Government, in-  
10          cluding through the Cyberspace Policy Co-  
11          ordinating Committee described in para-  
12          graph (6), and by convening other coordi-  
13          nating meetings with appropriate officials  
14          from the Department and other compo-  
15          nents of the United States Government on  
16          a regular basis;

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

21          “(v) to represent the Secretary of  
22          State in interagency efforts to develop and  
23          advance the policy described in section 4 of  
24          the Cyber Diplomacy Act of 2021;

1 “(vi) to act as a liaison to civil soci-  
2 ety, the private sector, academia, and other  
3 public and private entities on relevant  
4 international cyberspace issues;

5 “(vii) to lead United States Govern-  
6 ment efforts to establish a global deter-  
7 rence framework for malicious cyber activ-  
8 ity;

9 “(viii) to develop and execute adver-  
10 sary-specific strategies to influence adver-  
11 sary decisionmaking through the imposi-  
12 tion of costs and deterrence strategies, in  
13 coordination with other relevant Executive  
14 agencies;

15 “(ix) to advise the Secretary and co-  
16 ordinate with foreign governments on ex-  
17 ternal responses to national security-level  
18 cyber incidents, including coordination on  
19 diplomatic response efforts to support al-  
20 lies threatened by malicious cyber activity,  
21 in conjunction with members of the North  
22 Atlantic Treaty Organization and other  
23 like-minded countries;

24 “(x) to promote the adoption of na-  
25 tional processes and programs that enable

1 threat detection, prevention, and response  
2 to malicious cyber activity emanating from  
3 the territory of a foreign country, including  
4 as such activity relates to the United  
5 States' European allies, as appropriate;

6 “(xi) to promote the building of for-  
7 eign capacity relating to cyberspace policy  
8 priorities;

9 “(xii) to promote the maintenance of  
10 an open and interoperable Internet gov-  
11 erned by the multistakeholder model, in-  
12 stead of by centralized government control;

13 “(xiii) to promote an international  
14 regulatory environment for technology in-  
15 vestments and the Internet that benefits  
16 United States economic and national secu-  
17 rity interests;

18 “(xiv) to promote cross-border flow of  
19 data and combat international initiatives  
20 seeking to impose unreasonable require-  
21 ments on United States businesses;

22 “(xv) to promote international policies  
23 to protect the integrity of United States  
24 and international telecommunications in-

1 frastructure from foreign-based, cyber-en-  
2 abled threats;

3 “(xvi) to lead engagement, in coordi-  
4 nation with Executive agencies, with for-  
5 eign governments on relevant international  
6 cyberspace and digital economy issues as  
7 described in the Cyber Diplomacy Act of  
8 2021;

9 “(xvii) to promote international poli-  
10 cies to secure radio frequency spectrum for  
11 United States businesses and national se-  
12 curity needs;

13 “(xviii) to promote and protect the ex-  
14 ercise of human rights, including freedom  
15 of speech and religion, through the Inter-  
16 net;

17 “(xix) to promote international initia-  
18 tives to strengthen civilian and private sec-  
19 tor resiliency to threats in cyberspace;

20 “(xx) to build capacity of United  
21 States diplomatic officials to engage on  
22 cyberspace issues;

23 “(xxi) to encourage the development  
24 and adoption by foreign countries of inter-



1 nationally recognized standards, policies,  
2 and best practices;

3 “(xxii) to consult, as appropriate, with  
4 other Executive agencies with related func-  
5 tions vested in such Executive agencies by  
6 law; and

7 “(xxiii) to conduct such other matters  
8 as the Secretary of State may assign.

9 “(3) QUALIFICATIONS.—The head of the Bu-  
10 reau should be an individual of demonstrated com-  
11 petency in the fields of—

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

14 “(B) international diplomacy.

15 “(4) ORGANIZATIONAL PLACEMENT.—During  
16 the 1-year period beginning on the date of the enact-  
17 ment of the Cyber Diplomacy Act of 2021, the head  
18 of the Bureau shall report to the Under Secretary  
19 for Political Affairs or to an official holding a higher  
20 position in the Department of State than the Under  
21 Secretary for Political Affairs. After the conclusion  
22 of such period, the head of the Bureau may report  
23 to a different Under Secretary or to an official hold-  
24 ing a higher position than Under Secretary if, not  
25 less than 15 days prior to any change in such re-

1        reporting structure, the Secretary of State consults  
2        with and provides to the Committee on Foreign Re-  
3        lations of the Senate and the Committee on Foreign  
4        Affairs of the House of Representatives the fol-  
5        lowing:

6                “(A) A notification that the Secretary has,  
7                with respect to the reporting structure of the  
8                Bureau, consulted with and solicited feedback  
9                from—

10               “(i) other relevant Federal entities  
11               with a role in international aspects of  
12               cyber policy; and

13               “(ii) the elements of the Department  
14               of State with responsibility over aspects of  
15               cyber policy, including the elements report-  
16               ing to—

17               “(I) the Under Secretary for Po-  
18               litical Affairs;

19               “(II) the Under Secretary for Ci-  
20               vilian Security, Democracy, and  
21               Human Rights;

22               “(III) the Under Secretary for  
23               Economic Growth, Energy, and the  
24               Environment;

1 “(IV) the Under Secretary for  
2 Arms Control and International Secu-  
3 rity Affairs; and

4 “(V) the Under Secretary for  
5 Management.

6 “(B) A description of the new reporting  
7 structure for the head of the Bureau, as well as  
8 a description of the data and evidence used to  
9 justify such new structure.

10 “(C) A plan describing how the new re-  
11 porting structure will better enable the head of  
12 the Bureau to carry out the responsibilities  
13 specified in paragraph (2), including the secu-  
14 rity, economic, and human rights aspects of  
15 cyber diplomacy.

16 “(5) RULE OF CONSTRUCTION.—Nothing in  
17 this subsection may be construed to preclude the  
18 head of the Bureau from being designated as an As-  
19 sistant Secretary, if such an Assistant Secretary po-  
20 sition does not increase the number of Assistant  
21 Secretary positions at the Department above the  
22 number authorized under subsection (c)(1).

23 “(6) COORDINATION.—

24 “(A) CYBERSPACE POLICY COORDINATING  
25 COMMITTEE.—In conjunction with establishing

1 the Bureau pursuant to this subsection, there is  
2 established a senior-level Cyberspace Policy Co-  
3 ordinating Committee to ensure that cyberspace  
4 issues receive broad senior level-attention and  
5 coordination across the Department of State  
6 and provide ongoing oversight of such issues.  
7 The Cyberspace Policy Coordinating Committee  
8 shall be chaired by the head of the Bureau or  
9 an official of the Department of State holding  
10 a higher position, and operate on an ongoing  
11 basis, meeting not less frequently than quar-  
12 terly. Committee members shall include appro-  
13 priate officials at the Assistant Secretary level  
14 or higher from—

15 “(i) the Under Secretariat for Polit-  
16 ical Affairs;

17 “(ii) the Under Secretariat for Civil-  
18 ian Security, Democracy, and Human  
19 Rights;

20 “(iii) the Under Secretariat for Eco-  
21 nomic Growth, Energy and the Environ-  
22 ment;

23 “(iv) the Under Secretariat for Arms  
24 Control and International Security;

1                   “(v) the Under Secretariat for Man-  
2                   agement; and

3                   “(vi) other senior level Department  
4                   participants, as appropriate.

5                   “(B) OTHER MEETINGS.—The head of the  
6                   Bureau shall convene other coordinating meet-  
7                   ings with appropriate officials from the Depart-  
8                   ment of State and other components of the  
9                   United States Government to ensure regular co-  
10                  ordination and collaboration on crosscutting  
11                  cyber policy issues.

12               “(b) SENSE OF CONGRESS.—It is the sense of Con-  
13               gress that the Bureau of International Cyberspace Policy  
14               established under section 1(g) of the State Department  
15               Basic Authorities Act of 1956, as added by subsection (a),  
16               should have a diverse workforce composed of qualified in-  
17               dividuals, including such individuals from traditionally  
18               under-represented groups.

19               “(c) UNITED NATIONS.—The Permanent Represent-  
20               ative of the United States to the United Nations should  
21               use the voice, vote, and influence of the United States to  
22               oppose any measure that is inconsistent with the policy  
23               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 new clause:

12 “(iii) A bilateral or multilateral cyber-  
13 space agreement.”;

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

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

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 2021, 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 clause (iii) of section  
9 112b(e)(2)(B) of title 1, United States Code, as added by  
10 subsection (b)(2), or until such agreement has been dis-  
11 continued, if discontinued within 5 years, the President  
12 shall—

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

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

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

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

3           (2) the arrangement announced between the  
4       United States and the United Kingdom on January  
5       16, 2015;

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

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

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

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

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

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

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

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

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



1           (12) any other similar bilateral or multilateral  
2           arrangement announced before such date of enact-  
3           ment.

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

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

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

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

17                (2) A plan of action to guide the diplomacy of  
18                the Department of State with regard to foreign  
19                countries, including—

20                        (A) conducting bilateral and multilateral  
21                        activities to—

22                               (i) develop norms of responsible coun-  
23                               try behavior in cyberspace consistent with  
24                               the objectives specified in section 4(b)(5);  
25                               and

1 (ii) share best practices and advance  
2 proposals to strengthen civilian and private  
3 sector resiliency to threats and access to  
4 opportunities in cyberspace; and

5 (B) reviewing the status of existing efforts  
6 in relevant multilateral fora, as appropriate, to  
7 obtain commitments on international norms in  
8 cyberspace.

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

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

15 (A) United States national security;

16 (B) Federal and private sector cyberspace  
17 infrastructure of the United States;

18 (C) intellectual property in the United  
19 States; and

20 (D) the privacy and security of citizens of  
21 the United States.

22 (5) A review of policy tools available to the  
23 President to deter and de-escalate tensions with for-  
24 eign countries, state-sponsored actors, and private  
25 actors regarding threats in cyberspace, the degree to

1       which such tools have been used, and whether such  
2       tools have been effective deterrents.

3           (6) A review of resources required to conduct  
4       activities to build responsible norms of international  
5       cyber behavior.

6           (7) A plan of action, developed in consultation  
7       with relevant Federal departments and agencies as  
8       the President may direct, to guide the diplomacy of  
9       the Department of State with regard to inclusion of  
10      cyber issues in mutual defense agreements.

11      (c) FORM OF STRATEGY.—

12           (1) PUBLIC AVAILABILITY.—The strategy re-  
13      quired under subsection (a) shall be available to the  
14      public in unclassified form, including through publi-  
15      cation in the Federal Register.

16           (2) CLASSIFIED ANNEX.—The strategy required  
17      under subsection (a) may include a classified annex,  
18      consistent with United States national security inter-  
19      ests, if the Secretary of State determines that such  
20      annex is appropriate.

21      (d) BRIEFING.—Not later than 30 days after the  
22      completion of the strategy required under subsection (a),  
23      the Secretary of State shall brief the appropriate congres-  
24      sional committees on the strategy, including any material  
25      contained in a classified annex.

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

3 (1) not later than 90 days after any material  
 4 change to United States policy described in such  
 5 strategy; and

6 (2) not later than one year after the inaugura-  
 7 tion of each new President.

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

10 The Foreign Assistance Act of 1961 is amended—

11 (1) in section 116 (22 U.S.C. 2151n), by add-  
 12 ing at the end the following new subsection:

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 which information shall include 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.”; and

21              (2) in section 502B (22 U.S.C. 2304)—

22                      (A) by redesignating the second subsection

23                      (i) (relating to child marriage) as subsection (j);

24                      and

1 (B) by adding at the end the following new  
2 subsection:

3 “(k)(1) The report required under subsection (b)  
4 shall include an assessment of freedom of expression with  
5 respect to electronic information in each foreign country,  
6 which information shall include the following:

7 “(A) An assessment of the extent to which gov-  
8 ernment authorities in the country inappropriately  
9 attempt to filter, censor, or otherwise block or re-  
10 move nonviolent expression of political or religious  
11 opinion or belief through the Internet, including  
12 electronic mail, and a description of the means by  
13 which such authorities attempt to inappropriately  
14 block or remove such expression.

15 “(B) An assessment of the extent to which gov-  
16 ernment authorities in the country have persecuted  
17 or otherwise punished, arbitrarily and without due  
18 process, an individual or group for the nonviolent ex-  
19 pression of political, religious, or ideological opinion  
20 or belief through the Internet, including electronic  
21 mail.

22 “(C) An assessment of the extent to which gov-  
23 ernment authorities in the country have sought, in-  
24 appropriately and with malicious intent, to collect,  
25 request, obtain, or disclose without due process per-

1       sonally identifiable information of a person in con-  
2       nection with that person’s nonviolent expression of  
3       political, religious, or ideological opinion or belief, in-  
4       cluding expression that would be protected by the  
5       International Covenant on Civil and Political Rights,  
6       adopted at New York December 16, 1966, and en-  
7       tered into force March 23, 1976, as interpreted by  
8       the United States.

9               “(D) An assessment of the extent to which wire  
10       communications and electronic communications are  
11       monitored without due process and in contravention  
12       to United States policy with respect to the principles  
13       of privacy, human rights, democracy, and rule of  
14       law.

15       “(2) In compiling data and making assessments  
16       under paragraph (1), United States diplomatic personnel  
17       should consult with relevant entities, including human  
18       rights organizations, the private sector, the governments  
19       of like-minded countries, technology and Internet compa-  
20       nies, and other appropriate nongovernmental organiza-  
21       tions or entities.

22       “(3) In this subsection—

23               “(A) the term ‘electronic communication’ has  
24       the meaning given the term in section 2510 of title  
25       18, United States Code;



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

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

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

10 **SEC. 9. GAO REPORT ON CYBER DIPLOMACY.**

11 Not later than one year after the date of the enact-  
12 ment of this Act, the Comptroller General of the United  
13 States shall submit a report and provide a briefing to the  
14 appropriate congressional committees that includes—

15 (1) an assessment of the extent to which United  
16 States diplomatic processes and other efforts with  
17 foreign countries, including through multilateral  
18 fora, bilateral engagements, and negotiated cyber-  
19 space agreements, advance the full range of United  
20 States interests in cyberspace, including the policy  
21 described in section 4;

22 (2) an assessment of the Department of State’s  
23 organizational structure and approach to managing  
24 its diplomatic efforts to advance the full range of

1 United States interests in cyberspace, including a re-  
 2 view of—

3 (A) the establishment of a Bureau in the  
 4 Department of State to lead the Department's  
 5 international cyber mission;

6 (B) the current or proposed diplomatic  
 7 mission, structure, staffing, funding, and activi-  
 8 ties of the Bureau;

9 (C) how the establishment of the Bureau  
 10 has impacted or is likely to impact the structure  
 11 and organization of the Department; and

12 (D) what challenges, if any, the Depart-  
 13 ment has faced or will face in establishing such  
 14 Bureau; and

15 (3) any other matters determined relevant by  
 16 the Comptroller General.

17 **SEC. 10. SENSE OF CONGRESS ON CYBERSECURITY SANC-**  
 18 **TIONS AGAINST NORTH KOREA AND CYBER-**  
 19 **SECURITY LEGISLATION IN VIETNAM.**

20 It is the sense of Congress that—

21 (1) the President should designate all entities  
 22 that knowingly engage in significant activities under-  
 23 mining cybersecurity through the use of computer  
 24 networks or systems against foreign persons, govern-  
 25 ments, or other entities on behalf of the Government

1 of North Korea, consistent with section 209(b) of  
2 the North Korea Sanctions and Policy Enhancement  
3 Act of 2016 (22 U.S.C. 9229(b));

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

6 (A) may not be consistent with inter-  
7 national trade standards; and

8 (B) may endanger the privacy of citizens  
9 of Vietnam; and

10 (3) the Government of Vietnam should work  
11 with the United States and other countries to ensure  
12 that such law meets all relevant international stand-  
13 ards.

Passed the House of Representatives April 20, 2021.

Attest:

*Clerk.*

117<sup>TH</sup> CONGRESS  
1<sup>ST</sup> SESSION

**H. R. 1251**

---

**AN ACT**

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