MARKUP of H. Res. 75, H.R. 739, H. Res. 156, H.R. 596, and H.R. 295

MARKUP

BEFORE THE

COMMITTEE ON FOREIGN AFFAIRS
HOUSE OF REPRESENTATIVES

ONE HUNDRED SIXTEENTH CONGRESS

FIRST SESSION

MARCH 7, 2019

Serial No. 116–11

Printed for the use of the Committee on Foreign Affairs

Available: http://www.foreignaffairs.house.gov/, http://docs.house.gov, or http://www.govinfo.gov

U.S. GOVERNMENT PUBLISHING OFFICE
35–369PDF WASHINGTON : 2019

COMMITTEE ON FOREIGN AFFAIRS

ELIOT L. ENGEL, New York, *Chairman*

BRAD SHERMAN, California
GREGORY W. MEEKS, New York
ALBIO SIRES, New Jersey
GERALD E. CONNOLLY, Virginia
THEODORE E. DEUTCH, Florida
KAREN BASS, California
WILLIAM KEATING, Massachusetts
DAVID CICILLINE, Rhode Island
AMI BERA, California
JOAQUIN CASTRO, Texas
DINA TITUS, Nevada
ADRIANO ESPAILLAT, New York
TED LIEU, California
SUSAN WILD, Pennsylvania
DEAN PHILLPS, Minnesota
ILHAN OMAR, Minnesota
COLIN ALLRED, Texas
ANDY LEVIN, Michigan
ABIGAIL SPANBERGER, Virginia
CHRISSY HOULAHAN, Pennsylvania
TOM MALINOWSKI, New Jersey
DAVID TRONE, Maryland
JIM COSTA, California
JUAN VARGAS, California
VICENTE GONZALEZ, Texas

MICHAEL T. MCCAUL, Texas, *Ranking Member*

CHRISTOPHER H. SMITH, New Jersey
STEVE CHABOT, Ohio
JOE WILSON, South Carolina
SCOTT PERRY, Pennsylvania
TED S. YOHO, Florida
ADAM KINZINGER, Illinois
LEE ZELDIN, New York
JIM SENSENBRENNER, Wisconsin
ANN WAGNER, Missouri
BRIAN MAST, Florida
FRANCIS ROONEY, Florida
BRIAN FITZPATRICK, Pennsylvania
JOHN CURTIS, Utah
KEN BUCK, Colorado
RON WRIGHT, Texas
GUY RESCHENTHALER, Pennsylvania
TIM BURCHETT, Tennessee
GREG PENCE, Indiana
STEVE WATKINS, Kansas
MIKE GUEST, Mississippi

JASON STEINBAUM, *Staff Director*
BRENDAN SHIELDS, *Republican Staff Director*

CONTENTS

MARKUP OF VARIOUS MEASURES

Thursday, March 7, 2019

HOUSE OF REPRESENTATIVES
COMMITTEE ON FOREIGN AFFAIRS
Washington, DC

The committee met, pursuant to notice, at 10:05 a.m., in Room 2172 Rayburn House Office Building, Hon. Eliot Engel (chairman of the committee) presiding.

Chairman ENGEL. So pursuant to notice, we meet today to mark-up five bipartisan measures. Without objection, all members may have 5 days to submit statements or extraneous materials on today's business.

As members were notified yesterday, we intend to consider today's measures en bloc. The measures are H. Res. 75, strongly condemning the January 2019 terrorist attack on the 14 Riverside Complex in Nairobi, Kenya; H.R. 739, the Cyber Diplomacy Act of 2019 with the McCaul Amendment; H. Res. 156 calling for accountability and justice for the assassination of Boris Nemtsov with the two Malinowski Amendments; H.R. 596, Crimea Annexation Non-recognition Act with the Connolly Amendment in the nature of a substitute; and H.R. 295, End Banking for Human Traffickers Act of 2019 with the Engel Amendment in the nature of a substitute.

[The bills and resolutions offered en bloc follow:]

IV

116TH CONGRESS
1ST SESSION

H. RES. 75

Strongly condemning the January 2019 terrorist attack on the 14 Riverside Complex in Nairobi, Kenya, offering condolences to the family and friends of the victims, and reaffirming solidarity with the people of Kenya.

IN THE HOUSE OF REPRESENTATIVES

JANUARY 24, 2019

Mr. ENGEL (for himself, Mr. MCCAUL, Ms. BASS, and Mr. SMITH of New Jersey) submitted the following resolution; which was referred to the Committee on Foreign Affairs

---

RESOLUTION

Strongly condemning the January 2019 terrorist attack on the 14 Riverside Complex in Nairobi, Kenya, offering condolences to the family and friends of the victims, and reaffirming solidarity with the people of Kenya.

Whereas, on January 15, 2019, armed gunmen attacked the 14 Riverside Complex in Nairobi, Kenya, killing at least 21 people during the 20-hour siege;

Whereas one of the individuals killed in this heinous act of violence was an American citizen named Jason Spindler, a 9/11 survivor and former Peace Corps volunteer who was the CEO and managing director of a strategy and investment firm in Nairobi;

Whereas Kenyan security forces rescued more than 700 civilians from the complex;

Whereas al-Shabaab, an al-Qaeda affiliated terrorist organization based in Somalia designated as a foreign terrorist organization by the Department of State, has claimed responsibility for the attack on the 14 Riverside Complex;

Whereas Kenya has previously been a target for al-Qaeda affiliated terrorist attacks in August 1998, when the United States embassy in Nairobi, Kenya, and the United States embassy in Dar es Salaam, Tanzania, were simultaneously bombed, killing 224 people and injuring over 5,000 people;

Whereas al-Shabaab has previously perpetrated numerous mass-casualty terrorist attacks in Kenya, notably the siege at the Westgate Mall in Nairobi in September 2013, which killed 67 people, and the assault on Garissa University College in April 2015, which killed 148 people;

Whereas the United States and Kenya share a longstanding and mutually beneficial political, economic, and security partnership; and

Whereas security cooperation between the United States and Kenya plays an essential role in combating terrorism and violent extremism in the Horn of Africa, particularly efforts to combat al-Shabaab; Now, therefore, be it

Resolved, That the House of Representatives—

(1) condemns in the strongest terms the recent terrorist attack by al-Shabaab in Nairobi, Kenya, that resulted in the tragic loss of 21 lives;

(2) offers its deepest condolences to the family and friends of the victims and to the Republic of

Kenya, and reaffirms its solidarity with the Kenyan people;

(3) honors the memory of Jason Spindler, who was murdered in this horrific terrorist attack;

(4) recognizes the heroism exhibited by Kenyan citizens, first responders, security forces, and the Kenya Red Cross Society to rescue those held hostage during the siege;

(5) expresses its support for the Government of Kenya's efforts to combat terrorism and violent extremism, including efforts to prevent, detect, and deter future attacks, and encourages all Kenyans to stand together in condemning terrorism and violent extremism;

(6) recognizes Kenya's contributions to countering terrorism and violent extremism in the region, particularly al-Shabaab, including as troop contributors to the African Union Mission in Somalia;

(7) recognizes the important role of United States assistance to combat al-Shabaab and other terrorist activity in the region, including efforts to build Kenya's capacity to respond to and prevent such attacks; and

(8) urges the Government of Kenya to work expeditiously to bring the perpetrators to justice, ad-

hering to the rule of law, respect for human rights, and due process in its efforts to counter terrorism and violent extremism.

○

I

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.

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

SECTION 1. SHORT TITLE; TABLE OF CONTENTS.

(a) SHORT TITLE.—This Act may be cited as the "Cyber Diplomacy Act of 2019".

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

SEC. 2. FINDINGS.

Congress makes the following findings:

(1) The stated goal of the United States International Strategy for Cyberspace, launched on May 16, 2011, is to "work internationally to promote an open, interoperable, secure, and reliable information and communications infrastructure that supports international trade and commerce, strengthens international security, and fosters free expression and innovation . . . in which norms of responsible behavior guide states' actions, sustain partnerships, and support the rule of law in cyberspace".

(2) In its June 24, 2013 report, the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (referred to in this section as "GGE"), established by the United Nations General Assembly, concluded that "State sovereignty and the international norms and principles that flow from it apply to States' conduct of [information and communications technology] ICT-related activities and to their jurisdiction over ICT infrastructure with their territory".

(3) In January 2015, China, Kazakhstan, Kyrgyzstan, Russia, Tajikistan, and Uzbekistan proposed a troubling international code of conduct for information security, which could be used as a pretext for restricting political dissent, and includes "curbing the dissemination of information that incites terrorism, separatism or extremism or that inflames hatred on ethnic, racial or religious grounds".

(4) In its July 22, 2015 consensus report, GGE found that "norms of responsible State behavior can reduce risks to international peace, security and stability".

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

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

(A) affirmed the applicability of international law to state behavior in cyberspace;

(B) called on states to refrain from cyber-enabled theft of intellectual property for commercial gain; and

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

(7) The March 2016 Department of State International Cyberspace Policy Strategy noted that "the Department of State anticipates a continued increase and expansion of our cyber-focused diplomatic efforts for the foreseeable future".

(8) On December 1, 2016, the Commission on Enhancing National Cybersecurity, which was established within the Department of Commerce by Executive Order 13718 (81 Fed. Reg. 7441), recommended that "the President should appoint an Ambassador for Cybersecurity to lead U.S. engagement with the international community on cybersecurity strategies, standards, and practices".

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

(A) recognized "the urgent necessity of increased international cooperation to promote security and stability in cyberspace";

(B) expressed commitment to "promoting a strategic framework for conflict prevention, cooperation and stability in cyberspace, consisting of the recognition of the applicability of existing international law to State behavior in cyberspace, the promotion of voluntary, nonbinding norms of responsible State behavior during peacetime, and the development and the implementation of practical cyber confidence building measures (CBMs) between States"; and

(C) reaffirmed that "the same rights that people have offline must also be protected online".

(10) In testimony before the Select Committee on Intelligence of the Senate on May 11, 2017, Director of National Intelligence Daniel R. Coats identified 6 cyber threat actors, including—

(A) Russia, for "efforts to influence the 2016 US election";

(B) China, for "actively targeting the US Government, its allies, and US companies for cyber espionage";

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

priorities, influence events and foreign perceptions, and counter threats";

(D) North Korea, for "previously conduct[ing] cyber-attacks against US commercial entities—specifically, Sony Pictures Entertainment in 2014";

(E) terrorists, who "use the Internet to organize, recruit, spread propaganda, raise funds, collect intelligence, inspire action by followers, and coordinate operations"; and

(F) criminals, who "are also developing and using sophisticated cyber tools for a variety of purposes including theft, extortion, and facilitation of other criminal activities".

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

(A) designates the Secretary of State to lead an interagency effort to develop an engagement strategy for international cooperation in cybersecurity; and

(B) notes that "the United States is especially dependent on a globally secure and resilient internet and must work with allies and

other partners toward maintaining . . . the policy of the executive branch to promote an open, interoperable, reliable, and secure internet that fosters efficiency, innovation, communication, and economic prosperity, while respecting privacy and guarding against disruption, fraud, and theft".

SEC. 3. DEFINITIONS.

In this Act:

(1) APPROPRIATE CONGRESSIONAL COMMITTEES.—The term "appropriate congressional committees" means the Committee on Foreign Relations of the Senate and the Committee on Foreign Affairs of the House of Representatives.

(2) INFORMATION AND COMMUNICATIONS TECHNOLOGY; ICT.—The terms "information and communications technology" and "ICT" include hardware, software, and other products or services primarily intended to fulfill or enable the function of information processing and communication by electronic means, including transmission and display, including via the Internet.

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

SEC. 4. UNITED STATES INTERNATIONAL CYBERSPACE POLICY.

(a) IN GENERAL.—It is the policy of the United States to work internationally to promote an open, interoperable, reliable, unfettered, and secure Internet governed by the multi-stakeholder model, which—

(1) promotes human rights, democracy, and rule of law, including freedom of expression, innovation, communication, and economic prosperity; and

(2) respects privacy and guards against deception, fraud, and theft.

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

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

(2) Reducing and limiting the risk of escalation and retaliation in cyberspace, damage to critical infrastructure, and other malicious cyber activity that impairs the use and operation of critical infrastructure that provides services to the public.

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

policies with the United States, including respect for human rights, democracy, and the rule of law, to advance such values and policies internationally.

(4) Encouraging the responsible development of new, innovative technologies and ICT products that strengthen a secure Internet architecture that is accessible to all.

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

(A) Countries should not conduct, or knowingly support, cyber-enabled theft of intellectual property, including trade secrets or other confidential business information, with the intent of providing competitive advantages to companies or commercial sectors.

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

(C) Countries should not conduct or knowingly support ICT activity that, contrary to international law, intentionally damages or otherwise impairs the use and operation of critical infrastructure providing services to the public,

and should take appropriate measures to protect their critical infrastructure from ICT threats.

(D) Countries should not conduct or knowingly support malicious international activity that, contrary to international law, harms the information systems of authorized emergency response teams (also known as "computer emergency response teams" or "cybersecurity incident response teams") of another country or authorize emergency response teams to engage in malicious international activity.

(E) Countries should respond to appropriate requests for assistance to mitigate malicious ICT activity emanating from their territory and aimed at the critical infrastructure of another country.

(F) Countries should not restrict cross-border data flows or require local storage or processing of data.

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

(6) Advancing, encouraging, and supporting the development and adoption of internationally recognized technical standards and best practices.

SEC. 5. DEPARTMENT OF STATE RESPONSIBILITIES.

(a) IN GENERAL.—Section 1 of the State Department Basic Authorities Act of 1956 (22 U.S.C. 2651a) is amended—

(1) by redesignating subsection (g) as subsection (h); and

(2) by inserting after subsection (f) the following:

"(g) OFFICE OF INTERNATIONAL CYBERSPACE POLICY.—

"(1) IN GENERAL.—There is established, within the Department of State, an Office of International Cyberspace Policy (referred to in this subsection as the 'Office'). The head of the Office shall have the rank and status of ambassador and shall be appointed by the President, by and with the advice and consent of the Senate.

"(2) DUTIES.—

"(A) IN GENERAL.—The head of the Office shall perform such duties and exercise such powers as the Secretary of State shall prescribe, including implementing the policy of the United

States described in section 4 of the Cyber Diplomacy Act of 2019.

"(B) DUTIES DESCRIBED.—The principal duties and responsibilities of the head of the Office shall be—

"(i) to serve as the principal cyberspace policy official within the senior management of the Department of State and as the advisor to the Secretary of State for cyberspace issues;

"(ii) to lead the Department of State's diplomatic cyberspace efforts, including efforts relating to international cybersecurity, Internet access, Internet freedom, digital economy, cybercrime, deterrence and international responses to cyber threats, and other issues that the Secretary assigns to the Office;

"(iii) to promote an open, interoperable, reliable, unfettered, and secure information and communications technology infrastructure globally;

"(iv) to represent the Secretary of State in interagency efforts to develop and

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

"(v) to coordinate cyberspace efforts and other relevant functions, including countering terrorists' use of cyberspace, within the Department of State and with other components of the United States Government;

"(vi) to act as a liaison to public and private sector entities on relevant international cyberspace issues;

"(vii) to lead United States Government efforts to establish a global deterrence framework for malicious cyber activity;

"(viii) to develop and execute adversary-specific strategies to influence adversary decisionmaking through the imposition of costs and deterrence strategies, in coordination with other relevant Executive agencies;

"(ix) to advise the Secretary and coordinate with foreign governments on external responses to national-security-level cyber incidents, including coordination on

diplomatic response efforts to support allies threatened by malicious cyber activity, in conjunction with members of the North Atlantic Treaty Organization and other like-minded countries;

"(x) to promote the adoption of national processes and programs that enable threat detection, prevention, and response to malicious cyber activity emanating from the territory of a foreign country, including as such activity relates to the United States' European allies, as appropriate;

"(xi) to promote the building of foreign capacity to protect the global network with the goal of enabling like-minded participation in deterrence frameworks;

"(xii) to promote the maintenance of an open and interoperable Internet governed by the multi-stakeholder model, instead of by centralized government control;

"(xiii) to promote an international regulatory environment for technology investments and the Internet that benefits United States economic and national security interests;

"(xiv) to promote cross-border flow of data and combat international initiatives seeking to impose unreasonable requirements on United States businesses;

"(xv) to promote international policies to protect the integrity of United States and international telecommunications infrastructure from foreign-based, cyber-enabled threats;

"(xvi) to lead engagement, in coordination with Executive agencies, with foreign governments on cyberspace and digital economy issues as described in the Cyber Diplomacy Act of 2019;

"(xvii) to promote international policies to secure radio frequency spectrum for United States businesses and national security needs;

"(xviii) to promote and protect the exercise of human rights, including freedom of speech and religion, through the Internet;

"(xix) to build capacity of United States diplomatic officials to engage on cyber issues;

"(xx) to encourage the development and adoption by foreign countries of internationally recognized standards, policies, and best practices; and

"(xxi) to consult, as appropriate, with other Executive agencies with related functions vested in such Executive agencies by law.

"(3) QUALIFICATIONS.—The head of the Office should be an individual of demonstrated competency in the fields of—

"(A) cybersecurity and other relevant cyber issues; and

"(B) international diplomacy.

"(4) ORGANIZATIONAL PLACEMENT.—During the 4-year period beginning on the date of the enactment of the Cyber Diplomacy Act of 2019, the head of the Office shall report to the Under Secretary for Political Affairs or to an official holding a higher position than the Under Secretary for Political Affairs in the Department of State. After the conclusion of such period, the head of the Office shall report to an appropriate Under Secretary or to an official holding a higher position than Under Secretary.

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

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

"(B) the head of the Office from being elevated to an Assistant Secretary, if such an Assistant Secretary position does not increase the number of Assistant Secretary positions at the Department above the number authorized under subsection (c)(1).".

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

(c) UNITED NATIONS.—The Permanent Representative of the United States to the United Nations should use the voice, vote, and influence of the United States to oppose any measure that is inconsistent with the policy described in section 4.

SEC. 6. INTERNATIONAL CYBERSPACE EXECUTIVE ARRANGEMENTS.

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

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

(1) in subsection (a) by striking "International Relations" and inserting "Foreign Affairs";

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

"(iii) A bilateral or multilateral cyberspace agreement.";

(3) by redesignating subsection (f) as subsection (g); and

(4) by inserting after subsection (e) the following:

"(f) With respect to any bilateral or multilateral cyberspace agreement under subsection (e)(2)(B)(iii) and the information required to be transmitted to Congress under subsection (a), or with respect to any arrangement that seeks to secure commitments on responsible country behavior in cyberspace consistent with section 4(b)(5) of the Cyber Diplomacy Act of 2019, the Secretary of State shall provide an explanation of such arrangement, including—

"(1) the purpose of such arrangement;

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

"(3) how such arrangement will be implemented.".

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

(1) notify the appropriate congressional committees if another country fails to adhere to significant commitments contained in such agreement; and

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

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

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

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

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

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

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

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

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

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

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

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

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

(12) any other similar bilateral or multilateral arrangement announced before such date of enactment.

SEC. 7. INTERNATIONAL STRATEGY FOR CYBERSPACE.

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

(b) ELEMENTS.—The strategy required under subsection (a) shall include the following:

(1) A review of actions and activities undertaken to support the policy described in section 4.

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

(A) conducting bilateral and multilateral activities to develop norms of responsible country behavior in cyberspace consistent with the objectives under section 4(b)(5); and

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

(3) A review of alternative concepts with regard to international norms in cyberspace offered by foreign countries.

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

(A) United States national security;

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

(C) intellectual property in the United States; and

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

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

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

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

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

(c) FORM OF STRATEGY.—

(1) PUBLIC AVAILABILITY.—The strategy required under subsection (a) shall be available to the public in unclassified form, including through publication in the Federal Register.

(2) CLASSIFIED ANNEX.—The strategy required under subsection (a) may include a classified annex, consistent with United States national security interests, if the Secretary of State determines that such annex is appropriate.

(d) BRIEFING.—Not later than 30 days after the completion of the strategy required under subsection (a), the Secretary of State shall brief the appropriate congressional committees on the strategy, including any material contained in a classified annex.

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

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

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

(f) PREEXISTING REQUIREMENT.—The Recommendations to the President on Protecting American Cyber Interests through International Engagement, prepared by the Office of the Coordinator for Cyber Issues on May 31, 2018, pursuant to section 3(c) of Executive Order 13800 (82 Fed. Reg. 22391), shall be deemed to satisfy the requirement under subsection (a).

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

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

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

"(A) An assessment of the extent to which government authorities in the country inappropriately attempt to filter, censor, or otherwise block or remove nonviolent expression of political or religious opinion or belief through the Internet, including electronic mail, and a description of the means by which such authorities attempt to inappropriately block or remove such expression.

"(B) An assessment of the extent to which government authorities in the country have persecuted or otherwise punished, arbitrarily and without due process, an individual or group for the nonviolent expression of political, religious, or ideological opinion or belief through the Internet, including electronic mail.

"(C) An assessment of the extent to which government authorities in the country have sought, inappropriately and with malicious intent, to collect, request, obtain, or disclose without due process personally identifiable information of a person in connection with that person's nonviolent expression of political, religious, or ideological opinion or belief, including expression that would be protected by the International Covenant on Civil and Political Rights, adopted at New York December 16, 1966, and entered into force March 23, 1976, as interpreted by the United States.

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

"(2) In compiling data and making assessments under paragraph (1), United States diplomatic personnel should consult with relevant entities, including human rights organizations, the private sector, the governments of like-minded countries, technology and Internet companies, and other appropriate nongovernmental organizations or entities.

"(3) In this subsection—

"(A) the term 'electronic communication' has the meaning given the term in section 2510 of title 18, United States Code;

"(B) the term 'Internet' has the meaning given the term in section 231(e)(3) of the Communications Act of 1934 (47 U.S.C. 231(e)(3));

"(C) the term 'personally identifiable information' means data in a form that identifies a particular person; and

"(D) the term 'wire communication' has the meaning given the term in section 2510 of title 18, United States Code.".

SEC. 9. GAO REPORT ON CYBER THREATS AND DATA MISUSE.

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

shall submit a report and provide a briefing to the appropriate congressional committees that includes—

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

(2) an assessment of the extent to which United States diplomatic processes and other efforts with foreign countries, including through multilateral fora, bilateral engagements, and negotiated cyberspace agreements, strengthen the protections of United States citizens' personal information;

(3) an assessment of the Department of State's report in response to Executive Order 13800 (82 Fed. Reg. 22391), which documents an engagement strategy for international cooperation in cybersecurity and the extent to which this strategy addresses protections of United States citizens' personal information;

(4) recommendations for United States policymakers on methods to properly address and strengthen the protections of United States citizens' personal information from misuse by international actors; and

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

SEC. 10. SENSE OF CONGRESS ON CYBERSECURITY SANCTIONS AGAINST NORTH KOREA AND CYBERSECURITY LEGISLATION IN VIETNAM.

It is the sense of Congress that—

(1) the President should designate all entities that knowingly engage in significant activities undermining cybersecurity through the use of computer networks or systems against foreign persons, governments, or other entities on behalf of the Government of North Korea, consistent with section 209(b) of the North Korea Sanctions and Policy Enhancement Act of 2016 (22 U.S.C. 9229(b));

(2) the cybersecurity law approved by the National Assembly of Vietnam on June 12, 2018—

(A) may not be consistent with international trade standards; and

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

(3) the Government of Vietnam should work with the United States and other countries to ensure that such law meets all relevant international standards.

SEC. 11. RULE OF CONSTRUCTION.

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

of any Executive agency vested in such agency under any provision of law.

○

AMENDMENT IN THE NATURE OF A SUBSTITUTE

TO H.R. 739

OFFERED BY MR. MCCAUL OF TEXAS

Strike all after the enacting clause and insert the following:

SECTION 1. SHORT TITLE; TABLE OF CONTENTS.

(a) SHORT TITLE.—This Act may be cited as the "Cyber Diplomacy Act of 2019".

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

SEC. 2. FINDINGS.

Congress makes the following findings:

(1) The stated goal of the United States International Strategy for Cyberspace, launched on May 16, 2011, is to "work internationally to promote an open, interoperable, secure, and reliable information and communications infrastructure that supports

international trade and commerce, strengthens international security, and fosters free expression and innovation . . . in which norms of responsible behavior guide states' actions, sustain partnerships, and support the rule of law in cyberspace".

(2) In its June 24, 2013 report, the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (referred to in this section as "GGE"), established by the United Nations General Assembly, concluded that "State sovereignty and the international norms and principles that flow from it apply to States' conduct of [information and communications technology] ICT-related activities and to their jurisdiction over ICT infrastructure with their territory".

(3) In January 2015, China, Kazakhstan, Kyrgyzstan, Russia, Tajikistan, and Uzbekistan proposed a troubling international code of conduct for information security, which could be used as a pretext for restricting political dissent, and includes "curbing the dissemination of information that incites terrorism, separatism or extremism or that inflames hatred on ethnic, racial or religious grounds".

(4) In its July 22, 2015 consensus report, GGE found that "norms of responsible State behavior can reduce risks to international peace, security and stability".

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

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

(A) affirmed the applicability of international law to state behavior in cyberspace;

(B) called on states to refrain from cyber-enabled theft of intellectual property for commercial gain; and

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

(7) The March 2016 Department of State International Cyberspace Policy Strategy noted that "the Department of State anticipates a continued in-

crease and expansion of our cyber-focused diplomatic efforts for the foreseeable future".

(8) On December 1, 2016, the Commission on Enhancing National Cybersecurity, which was established within the Department of Commerce by Executive Order 13718 (81 Fed. Reg. 7441), recommended that "the President should appoint an Ambassador for Cybersecurity to lead U.S. engagement with the international community on cybersecurity strategies, standards, and practices".

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

(A) recognized "the urgent necessity of increased international cooperation to promote security and stability in cyberspace";

(B) expressed commitment to "promoting a strategic framework for conflict prevention, cooperation and stability in cyberspace, consisting of the recognition of the applicability of existing international law to State behavior in cyberspace, the promotion of voluntary, non-binding norms of responsible State behavior during peacetime, and the development and the implementation of practical cyber confidence

building measures (CBMs) between States"; and

(C) reaffirmed that "the same rights that people have offline must also be protected online".

(10) In testimony before the Select Committee on Intelligence of the Senate on May 11, 2017, Director of National Intelligence Daniel R. Coats identified 6 cyber threat actors, including—

(A) Russia, for "efforts to influence the 2016 US election";

(B) China, for "actively targeting the US Government, its allies, and US companies for cyber espionage";

(C) Iran, for "leverag[ing] cyber espionage, propaganda, and attacks to support its security priorities, influence events and foreign perceptions, and counter threats";

(D) North Korea, for "previously conduct[ing] cyber-attacks against US commercial entities—specifically, Sony Pictures Entertainment in 2014";

(E) terrorists, who "use the Internet to organize, recruit, spread propaganda, raise funds,

collect intelligence, inspire action by followers, and coordinate operations"; and

(F) criminals, who "are also developing and using sophisticated cyber tools for a variety of purposes including theft, extortion, and facilitation of other criminal activities".

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

(A) designates the Secretary of State to lead an interagency effort to develop an engagement strategy for international cooperation in cybersecurity; and

(B) notes that "the United States is especially dependent on a globally secure and resilient internet and must work with allies and other partners toward maintaining . . . the policy of the executive branch to promote an open, interoperable, reliable, and secure internet that fosters efficiency, innovation, communication, and economic prosperity, while respecting privacy and guarding against disruption, fraud, and theft".

SEC. 3. DEFINITIONS.

In this Act:

(1) APPROPRIATE CONGRESSIONAL COMMITTEES.—The term "appropriate congressional committees" means the Committee on Foreign Relations of the Senate and the Committee on Foreign Affairs of the House of Representatives.

(2) INFORMATION AND COMMUNICATIONS TECHNOLOGY; ICT.—The terms "information and communications technology" and "ICT" include hardware, software, and other products or services primarily intended to fulfill or enable the function of information processing and communication by electronic means, including transmission and display, including via the Internet.

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

SEC. 4. UNITED STATES INTERNATIONAL CYBERSPACE POLICY.

(a) IN GENERAL.—It is the policy of the United States to work internationally to promote an open, interoperable, reliable, unfettered, and secure Internet governed by the multi-stakeholder model, which—

(1) promotes human rights, democracy, and rule of law, including freedom of expression, innovation, communication, and economic prosperity; and

(2) respects privacy and guards against deception, fraud, and theft.

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

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

(2) Reducing and limiting the risk of escalation and retaliation in cyberspace, damage to critical infrastructure, and other malicious cyber activity that impairs the use and operation of critical infrastructure that provides services to the public.

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

(4) Encouraging the responsible development of new, innovative technologies and ICT products that

strengthen a secure Internet architecture that is accessible to all.

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

(A) Countries should not conduct, or knowingly support, cyber-enabled theft of intellectual property, including trade secrets or other confidential business information, with the intent of providing competitive advantages to companies or commercial sectors.

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

(C) Countries should not conduct or knowingly support ICT activity that, contrary to international law, intentionally damages or otherwise impairs the use and operation of critical infrastructure providing services to the public, and should take appropriate measures to protect their critical infrastructure from ICT threats.

(D) Countries should not conduct or knowingly support malicious international activity

that, contrary to international law, harms the information systems of authorized emergency response teams (also known as "computer emergency response teams" or "cybersecurity incident response teams") of another country or authorize emergency response teams to engage in malicious international activity.

(E) Countries should respond to appropriate requests for assistance to mitigate malicious ICT activity emanating from their territory and aimed at the critical infrastructure of another country.

(F) Countries should not restrict cross-border data flows or require local storage or processing of data.

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

(6) Advancing, encouraging, and supporting the development and adoption of internationally recognized technical standards and best practices.

SEC. 5. DEPARTMENT OF STATE RESPONSIBILITIES.

(a) IN GENERAL.—Section 1 of the State Department Basic Authorities Act of 1956 (22 U.S.C. 2651a) is amended—

(1) by redesignating subsection (g) as subsection (h); and

(2) by inserting after subsection (f) the following:

"(g) OFFICE OF INTERNATIONAL CYBERSPACE POLICY.—

"(1) IN GENERAL.—There is established, within the Department of State, an Office of International Cyberspace Policy (referred to in this subsection as the 'Office'). The head of the Office shall have the rank and status of ambassador and shall be appointed by the President, by and with the advice and consent of the Senate.

"(2) DUTIES.—

"(A) IN GENERAL.—The head of the Office shall perform such duties and exercise such powers as the Secretary of State shall prescribe, including implementing the policy of the United States described in section 4 of the Cyber Diplomacy Act of 2019.

"(B) DUTIES DESCRIBED.—The principal duties and responsibilities of the head of the Office shall be—

"(i) to serve as the principal cyberspace policy official within the senior management of the Department of State and as the advisor to the Secretary of State for cyberspace issues;

"(ii) to lead the Department of State's diplomatic cyberspace efforts, including efforts relating to international cybersecurity, Internet access, Internet freedom, digital economy, cybercrime, deterrence and international responses to cyber threats, and other issues that the Secretary assigns to the Office;

"(iii) to promote an open, interoperable, reliable, unfettered, and secure information and communications technology infrastructure globally;

"(iv) to represent the Secretary of State in interagency efforts to develop and advance the policy described in section 4 of the Cyber Diplomacy Act of 2019;

"(v) to coordinate cyberspace efforts and other relevant functions, including countering terrorists' use of cyberspace, within the Department of State and with other components of the United States Government;

"(vi) to act as a liaison to public and private sector entities on relevant international cyberspace issues;

"(vii) to lead United States Government efforts to establish a global deterrence framework for malicious cyber activity;

"(viii) to develop and execute adversary-specific strategies to influence adversary decisionmaking through the imposition of costs and deterrence strategies, in coordination with other relevant Executive agencies;

"(ix) to advise the Secretary and coordinate with foreign governments on external responses to national-security-level cyber incidents, including coordination on diplomatic response efforts to support allies threatened by malicious cyber activity,

in conjunction with members of the North Atlantic Treaty Organization and other like-minded countries;

"(x) to promote the adoption of national processes and programs that enable threat detection, prevention, and response to malicious cyber activity emanating from the territory of a foreign country, including as such activity relates to the United States' European allies, as appropriate;

"(xi) to promote the building of foreign capacity to protect the global network with the goal of enabling like-minded participation in deterrence frameworks;

"(xii) to promote the maintenance of an open and interoperable Internet governed by the multi-stakeholder model, instead of by centralized government control;

"(xiii) to promote an international regulatory environment for technology investments and the Internet that benefits United States economic and national security interests;

"(xiv) to promote cross-border flow of data and combat international initiatives

seeking to impose unreasonable requirements on United States businesses;

"(xv) to promote international policies to protect the integrity of United States and international telecommunications infrastructure from foreign-based, cyber-enabled threats;

"(xvi) to lead engagement, in coordination with Executive agencies, with foreign governments on relevant international cyberspace and digital economy issues as described in the Cyber Diplomacy Act of 2019;

"(xvii) to promote international policies to secure radio frequency spectrum for United States businesses and national security needs;

"(xviii) to promote and protect the exercise of human rights, including freedom of speech and religion, through the Internet;

"(xix) to build capacity of United States diplomatic officials to engage on cyberspace issues;

"(xx) to encourage the development and adoption by foreign countries of internationally recognized standards, policies, and best practices; and

"(xxi) to consult, as appropriate, with other Executive agencies with related functions vested in such Executive agencies by law.

"(3) QUALIFICATIONS.—The head of the Office should be an individual of demonstrated competency in the fields of—

"(A) cybersecurity and other relevant cyberspace issues; and

"(B) international diplomacy.

"(4) ORGANIZATIONAL PLACEMENT.—During the 4-year period beginning on the date of the enactment of the Cyber Diplomacy Act of 2019, the head of the Office shall report to the Under Secretary for Political Affairs or to an official holding a higher position than the Under Secretary for Political Affairs in the Department of State. After the conclusion of such period, the head of the Office shall report to an appropriate Under Secretary or to an official holding a higher position than Under Secretary.

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

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

"(B) the head of the Office from being elevated to an Assistant Secretary, if such an Assistant Secretary position does not increase the number of Assistant Secretary positions at the Department above the number authorized under subsection (c)(1).".

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

(c) UNITED NATIONS.—The Permanent Representative of the United States to the United Nations should use the voice, vote, and influence of the United States to oppose any measure that is inconsistent with the policy described in section 4.

SEC. 6. INTERNATIONAL CYBERSPACE EXECUTIVE ARRANGEMENTS.

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

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

(1) in subsection (a) by striking "International Relations" and inserting "Foreign Affairs";

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

"(iii) A bilateral or multilateral cyberspace agreement.";

(3) by redesignating subsection (f) as subsection (g); and

(4) by inserting after subsection (e) the following:

"(f) With respect to any bilateral or multilateral cyberspace agreement under subsection (e)(2)(B)(iii) and the information required to be transmitted to Congress under subsection (a), or with respect to any arrangement that seeks to secure commitments on responsible country behavior in cyberspace consistent with section 4(b)(5) of the Cyber Diplomacy Act of 2019, the Secretary of State shall provide an explanation of such arrangement, including—

"(1) the purpose of such arrangement;

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

"(3) how such arrangement will be implemented.".

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

(1) notify the appropriate congressional committees if another country fails to adhere to significant commitments contained in such agreement; and

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

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

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

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

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

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

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

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

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

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

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

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

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

(12) any other similar bilateral or multilateral arrangement announced before such date of enactment.

SEC. 7. INTERNATIONAL STRATEGY FOR CYBERSPACE.

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

(b) ELEMENTS.—The strategy required under subsection (a) shall include the following:

(1) A review of actions and activities undertaken to support the policy described in section 4.

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

(A) conducting bilateral and multilateral activities to develop norms of responsible country behavior in cyberspace consistent with the objectives under section 4(b)(5); and

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

(3) A review of alternative concepts with regard to international norms in cyberspace offered by foreign countries.

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

(A) United States national security;

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

(C) intellectual property in the United States; and

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

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

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

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

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

(c) FORM OF STRATEGY.—

(1) PUBLIC AVAILABILITY.—The strategy required under subsection (a) shall be available to the public in unclassified form, including through publication in the Federal Register.

(2) CLASSIFIED ANNEX.—The strategy required under subsection (a) may include a classified annex, consistent with United States national security interests, if the Secretary of State determines that such annex is appropriate.

(d) BRIEFING.—Not later than 30 days after the completion of the strategy required under subsection (a), the Secretary of State shall brief the appropriate congressional committees on the strategy, including any material contained in a classified annex.

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

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

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

(f) PREEXISTING REQUIREMENT.—The Recommendations to the President on Protecting American Cyber Interests through International Engagement, prepared by the Office of the Coordinator for Cyber Issues on May 31, 2018, pursuant to section 3(c) of Executive Order 13800 (82 Fed. Reg. 22391), shall be deemed to satisfy the requirement under subsection (a).

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

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

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

"(A) An assessment of the extent to which government authorities in the country inappropriately attempt to filter, censor, or otherwise block or remove nonviolent expression of political or religious opinion or belief through the Internet, including electronic mail, and a description of the means by which such authorities attempt to inappropriately block or remove such expression.

"(B) An assessment of the extent to which government authorities in the country have persecuted or otherwise punished, arbitrarily and without due process, an individual or group for the nonviolent expression of political, religious, or ideological opinion or belief through the Internet, including electronic mail.

"(C) An assessment of the extent to which government authorities in the country have sought, inappropriately and with malicious intent, to collect, request, obtain, or disclose without due process personally identifiable information of a person in connection with that person's nonviolent expression of political, religious, or ideological opinion or belief, including expression that would be protected by the International Covenant on Civil and Political Rights, adopted at New York December 16, 1966, and entered into force March 23, 1976, as interpreted by the United States.

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

"(2) In compiling data and making assessments under paragraph (1), United States diplomatic personnel should consult with relevant entities, including human rights organizations, the private sector, the governments of like-minded countries, technology and Internet companies, and other appropriate nongovernmental organizations or entities.

"(3) In this subsection—

"(A) the term 'electronic communication' has the meaning given the term in section 2510 of title 18, United States Code;

"(B) the term 'Internet' has the meaning given the term in section 231(e)(3) of the Communications Act of 1934 (47 U.S.C. 231(e)(3));

"(C) the term 'personally identifiable information' means data in a form that identifies a particular person; and

"(D) the term 'wire communication' has the meaning given the term in section 2510 of title 18, United States Code.".

SEC. 9. GAO REPORT ON CYBER DIPLOMACY.

Not later than 1 year after the date of the enactment of this Act, the Comptroller General of the United States shall submit a report and provide a briefing to the appropriate congressional committees that includes—

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

(2) an assessment of the Department of State's organizational structure and approach to managing its diplomatic efforts to advance the full range of United States interests in cyberspace, including a review of—

(A) the establishment of a bureau in the Department of State to lead the Department's international cyber mission;

(B) the current or proposed diplomatic mission, structure, staffing, funding, and activities of the bureau;

(C) how the establishment of the bureau has impacted or is likely to impact the structure and organization of the Department; and

(D) what challenges, if any, the Department has faced or will face in establishing such bureau; and

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

SEC. 10. SENSE OF CONGRESS ON CYBERSECURITY SANCTIONS AGAINST NORTH KOREA AND CYBERSECURITY LEGISLATION IN VIETNAM.

It is the sense of Congress that—

(1) the President should designate all entities that knowingly engage in significant activities undermining cybersecurity through the use of computer networks or systems against foreign persons, governments, or other entities on behalf of the Government of North Korea, consistent with section 209(b) of the North Korea Sanctions and Policy Enhancement Act of 2016 (22 U.S.C. 9229(b));

(2) the cybersecurity law approved by the National Assembly of Vietnam on June 12, 2018—

(A) may not be consistent with international trade standards; and

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

(3) the Government of Vietnam should work with the United States and other countries to ensure that such law meets all relevant international standards.

SEC. 11. RULE OF CONSTRUCTION.

(a) RULE OF CONSTRUCTION.—Nothing in this Act may be construed to infringe upon the related functions of any Executive agency vested in such agency under any provision of law.

IV

116TH CONGRESS
1ST SESSION

H. RES. 156

Calling for accountability and justice for the assassination of Boris Nemtsov.

IN THE HOUSE OF REPRESENTATIVES

FEBRUARY 27, 2019

Mr. ENGEL (for himself, Mr. MCCAUL, Mr. MALINOWSKI, and Ms. CHENEY) submitted the following resolution; which was referred to the Committee on Foreign Affairs

---

RESOLUTION

Calling for accountability and justice for the assassination of Boris Nemtsov.

Whereas Boris Nemtsov was a Russian statesman who, over 25 years of public service, served as a Member of Parliament, Governor of the Nizhny Novgorod Region, and First Deputy Prime Minister of Russia;

Whereas throughout his life, Boris Nemtsov showed an unwavering commitment to the ideals of democracy, freedom, and the rule of law, and to upholding the rights and dignity of Russian citizens;

Whereas Boris Nemtsov was a powerful voice in opposition to the authoritarianism and corruption of Vladimir Putin's government, publicizing its abuses, leading street protests against election fraud and the war on Ukraine, and suc-

cessfully advocating for international sanctions on human rights violators;

Whereas Boris Nemtsov was co-chairman of a leading opposition party, won election to the Yaroslavl Regional Duma in 2013, and was planning to run for the Russian Parliament in 2016 and challenge Vladimir Putin for the Presidency in 2018;

Whereas, on the evening of February 27, 2015, Boris Nemtsov was shot in the back and killed as he walked across Bolshoi Moskvoretsky Bridge near the Kremlin in Moscow;

Whereas, on March 7 and 8, 2015, Russian authorities arrested five individuals, all of them natives of the Chechen Republic, on suspicion of carrying out the assassination, while a sixth suspect allegedly blew himself up during the attempted arrest;

Whereas the defendants were tried at the Moscow District Military Court, which on June 29, 2017, found them guilty of carrying out the assassination of Boris Nemtsov, and on July 13, 2017, sentenced them to different prison terms;

Whereas at the time of the assassination, the now-convicted gunman, Zaur Dadayev, was serving as a Lieutenant in the Internal Troops of the Interior Ministry of the Russian Federation and as Deputy Battalion Commander in the "Sever" ("North") Regiment stationed in the Chechen Republic, under the command of the Internal Troops Commander, General Viktor Zolotov, and the Kremlin-backed head of the Chechen Republic, Ramzan Kadyrov;

Whereas Ramzan Kadyrov has called Lieutenant Zaur Dadayev a "true patriot" and has publicly referred to Boris Nemtsov as an "enemy of Russia";

Whereas by Decree No. 115 issued on March 8, 2015, President Vladimir Putin awarded Ramzan Kadyrov the Order of Honor;

Whereas according to reports published in the RosBusinessConsulting (RBC) newspaper on January 20, 2016, General Alexander Bastrykin, chairman of the Investigative Committee of the Russian Federation, has on two occasions prevented investigators from indicting Major Ruslan Geremeyev, Battalion Commander in the "Sever" ("North") Regiment of the Internal Troops of the Ministry of Internal Affairs of the Russian Federation stationed in the Chechen Republic and a close associate of Ramzan Kadyrov, as an organizer in the assassination;

Whereas according to reports published in Novaya Gazeta newspaper on December 9, 2016, operatives of the Federal Security Service of the Russian Federation in the Chechen Republic have failed to serve Major Ruslan Geremeyev with a summons for questioning as a witness, reporting to their superiors that on the sole occasion they attempted to do so, "nobody opened the door";

Whereas despite requests from the legal team representing Boris Nemtsov's family, the Investigative Committee of the Russian Federation and the Moscow District Military Court have refused to question high-ranking persons of interest, including Ramzan Kadyrov and General Viktor Zolotov;

Whereas the Investigative Committee of the Russian Federation has, to this day, not issued any indictments against

the organizers or masterminds of the assassination of Boris Nemtsov, with the exception of Major Ruslan Geremeyev's driver, Ruslan Mukhudinov, who is named alongside "other unidentified persons";

Whereas the Investigative Committee of the Russian Federation and the Moscow District Military Court have refused to classify the assassination of Boris Nemtsov under Article 277 of the Criminal Code as "encroachment on the life of a statesman or a public figure," choosing instead Article 105 that deals with common domestic murders;

Whereas throughout the proceedings at the Moscow District Military Court, the judge repeatedly disallowed questions relating to political motives behind the assassination;

Whereas the Federal Protective Service of the Russian Federation has refused to release video footage from the security cameras on Bolshoi Moskvoretsky Bridge from the night of the assassination, claiming in a letter to State Duma Member Dmitry Gudkov on November 6, 2015, that the bridge next to the Kremlin is "not a protected object";

Whereas, on May 18, 2017, the Parliamentary Assembly of the Council of Europe appointed Lithuanian Member of Parliament Emanuelis Zingeris as its special rapporteur on the need to shed light on the background of the murder of Boris Nemtsov, with a mandate to review and report on the case and on the progress of the official Russian investigation;

Whereas, on May 24, 2018, the Russian Foreign Ministry informed Emanuelis Zingeris that he is forbidden from entering the Russian Federation;

Whereas, at its 27th annual session held on July 7 through 11, 2018, the Parliamentary Assembly of the Organization for Security and Cooperation in Europe (OSCE) adopted a resolution urging Russian authorities to "undertake a new, full and thorough investigation into the February 2015 assassination of Boris Nemtsov";

Whereas, on July 8, 2018, the Parliamentary Assembly of the Organization for Security and Cooperation in Europe held a public event to discuss the need for OSCE oversight of the official Russian investigation into the assassination of Boris Nemtsov;

Whereas the United States and the Russian Federation are full members of the Organization for Security and Cooperation in Europe;

Whereas the OSCE Moscow Document has established that "issues relating to human rights, fundamental freedoms, democracy and the rule of law . . . are matters of direct and legitimate concern to all participating States and do not belong exclusively to the internal affairs of the State concerned";

Whereas, on February 27, 2018, Washington, DC, designated the street in front of the Embassy of the Russian Federation as "Boris Nemtsov Plaza" to honor Mr. Nemtsov; and

Whereas, on February 22, 2019, the President of the Parliamentary Assembly of the OSCE, George Tsereteli, appointed Swedish Member of Parliament and Vice President of the Assembly Margareta Cederfelt as the rapporteur on the investigation of the assassination of Boris Nemtsov, with a mandate to review and report on

the case and on the progress of the official Russian investigation: Now, therefore, be it

Resolved, That the House of Representatives—

(1) condemns Vladimir Putin and his regime for targeting political opponents and covering up the assassination of Boris Nemtsov, a Russian opposition leader who worked to advance democracy and human rights in Russia;

(2) urges the United States Government, in all its interactions with the Government of the Russian Federation, to raise the case of the assassination of Boris Nemtsov and underscore the necessity of bringing the organizers and masterminds to justice;

(3) supports the efforts by the Organization for Security and Cooperation in Europe (OSCE) and its Parliamentary Assembly to initiate oversight of the official Russian investigation into the assassination of Boris Nemtsov;

(4) calls on the Government of the Russian Federation to allow an impartial international investigation of the assassination of Boris Nemtsov and to cooperate with the Parliamentary Assembly of the OSCE and the Parliamentary Assembly of the Council of Europe in their ongoing inquiries over this case;

(5) calls on the Secretary of State and the Secretary of the Treasury to use their authority under the Sergei Magnitsky Rule of Law Accountability Act of 2012 (title IV of Public Law 112–208) and the Global Magnitsky Human Rights Accountability Act (subtitle F of title XII of Public Law 114–328) to designate individuals whom they determine to have been involved in the assassination of Boris Nemtsov as perpetrators, organizers, or masterminds, on the list of specially designated nationals and blocked persons maintained by the Office of Foreign Assets Control of the Department of the Treasury, freezing their assets and making them ineligible to receive United States visas; and

(6) calls on the Secretary of State, in consultation with the Director of National Intelligence, to prepare and submit to Congress a report detailing the circumstances of the February 27, 2015, assassination of Boris Nemtsov, including the list of individuals whom they determine to have been involved in the assassination as perpetrators, organizers, or masterminds, and identifying what measures, if any, have been taken by the Government of the Russian Federation to investigate this crime and bring its

perpetrators, organizers, and masterminds to justice, and evaluating the effectiveness of such measures.

○

AMENDMENT TO H. RES. 156

OFFERED BY MR. MALINOWSKI OF NEW JERSEY

In the 11th clause of the preamble, insert "and Russian State Duma Member Adam Delimkhanov" after "Ramzan Kadyrov".

In the 13th clause of the preamble, strike "and General Victor Zolotov" and insert ", General Victor Zolotov, and Adam Delimkhanov".

☒

AMENDMENT TO H. RES. 156

OFFERED BY MR. MALINOWSKI OF NEW JERSEY

Page 7, line 14, strike "; and" and insert ";".

Page 8, line 2, strike the period at the end and insert "; and".

Page 8, after line 2, insert the following:

(7) urges the Secretary of State to take all possible steps to—

(A) investigate the business activities of Ramzan Kadyrov and any entities controlled by Ramzan Kadyrov outside the Russian Federation; and

(B) determine whether any such activities, or any entities facilitating such activities, are in violation of the sanctions imposed on Ramzan Kadyrov pursuant to the authorities provided by the Global Magnitsky Human Rights Accountability Act (22 U.S.C. 2656 note).

☒

I

116TH CONGRESS
1ST SESSION

H. R. 596

To prohibit United States Government recognition of Russia's annexation of Crimea.

IN THE HOUSE OF REPRESENTATIVES

JANUARY 16, 2019

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

---

A BILL

To prohibit United States Government recognition of Russia's annexation of Crimea.

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

SECTION 1. SHORT TITLE.

This Act may be cited as the "Crimea Annexation Non-recognition Act".

SEC. 2. PROHIBITION AGAINST UNITED STATES RECOGNITION OF RUSSIA'S ANNEXATION OF CRIMEA.

(a) STATEMENT OF POLICY.—It is the policy of the United States not to recognize the de jure or de facto sov-

ereignty of the Russian Federation over Crimea, its airspace, or its territorial waters.

(b) PROHIBITION.—In accordance with subsection (a), no Federal department or agency may take any action or extend any assistance that recognizes or implies recognition of the de jure or de facto sovereignty of the Russian Federation over Crimea, its airspace, or its territorial waters.

(c) WAIVER.—The President may waive subsection (a) or (b) if the President determines that it is vital to the national security interests of the United States to do so.

○

AMENDMENT IN THE NATURE OF A SUBSTITUTE

TO H.R. 596

OFFERED BY MR. CONNOLLY OF VIRGINIA

Strike all after the enacting clause and insert the following:

SECTION 1. SHORT TITLE.

This Act may be cited as the "Crimea Annexation Non-recognition Act".

SEC. 2. PROHIBITION AGAINST UNITED STATES RECOGNITION OF THE RUSSIAN FEDERATION'S CLAIM OF SOVEREIGNTY OVER CRIMEA.

(a) STATEMENT OF POLICY.—It is the policy of the United States not to recognize the Russian Federation's claim of sovereignty over Crimea, its airspace, or its territorial waters.

(b) PROHIBITION.—In accordance with subsection (a), no Federal department or agency may take any action or extend any assistance that implies recognition of the Russian Federation's claim of sovereignty over Crimea, its airspace, or its territorial waters.

(c) WAIVER.—The President may waive the prohibition in subsection (b) on a case-by-case basis if the Presi-

dent determines that it is vital to the national security interests of the United States to do so.

Amend the title so as to read: "A bill to prohibit United States Government recognition of the Russian Federation's claim of sovereignty over Crimea, and for other purposes.".

I

116TH CONGRESS
1ST SESSION

H. R. 295

To increase the role of the financial industry in combating human trafficking.

IN THE HOUSE OF REPRESENTATIVES

JANUARY 8, 2019

Mr. FITZPATRICK (for himself, Mr. KEATING, Mr. MCCAUL, and Mrs. CAROLYN B. MALONEY of New York) introduced the following bill; which was referred to the Committee on Foreign Affairs, and in addition to the Committee on Financial Services, for a period to be subsequently determined by the Speaker, in each case for consideration of such provisions as fall within the jurisdiction of the committee concerned

---

A BILL

To increase the role of the financial industry in combating human trafficking.

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

SECTION 1. SHORT TITLE.

This Act may be cited as the "End Banking for Human Traffickers Act of 2019".

SEC. 2. INCREASING THE ROLE OF THE FINANCIAL INDUSTRY IN COMBATING HUMAN TRAFFICKING.

(a) TREASURY AS A MEMBER OF THE PRESIDENT'S INTERAGENCY TASK FORCE TO MONITOR AND COMBAT

TRAFFICKING.—Section 105(b) of the Victims of Trafficking and Violence Protection Act of 2000 (22 U.S.C. 7103(b)) is amended by inserting "the Secretary of the Treasury," after "the Secretary of Education,".

(b) REQUIRED REVIEW OF PROCEDURES.—Not later than 180 days after the date of the enactment of this Act, the Financial Institutions Examination Council, in consultation with the Secretary of the Treasury, the private sector, victims of severe forms of trafficking in persons, advocates of persons at risk of becoming victims of severe forms of trafficking in persons, and appropriate law enforcement agencies, shall—

(1) review and enhance training and examinations procedures to improve the capabilities of anti-money laundering and countering the financing of terrorism programs to detect financial transactions relating to severe forms of trafficking in persons;

(2) review and enhance procedures for referring potential cases relating to severe forms of trafficking in persons to the appropriate law enforcement agency; and

(3) determine, as appropriate, whether requirements for financial institutions are sufficient to detect and deter money laundering relating to severe forms of trafficking in persons.

(c) INTERAGENCY TASK FORCE RECOMMENDATIONS TARGETING MONEY LAUNDERING RELATED TO HUMAN TRAFFICKING.—

(1) IN GENERAL.—Not later than 270 days after the date of the enactment of this Act, the Interagency Task Force To Monitor and Combat Trafficking shall submit to the Committee on Financial Services and the Committee on the Judiciary of the House of Representatives, the Committee on Banking, Housing, and Urban Affairs and the Committee on the Judiciary of the Senate, and the head of each appropriate Federal banking agency—

(A) an analysis of anti-money laundering efforts of the United States Government and United States financial institutions relating to severe forms of trafficking in persons; and

(B) appropriate legislative, administrative, and other recommendations to strengthen efforts against money laundering relating to severe forms of trafficking in persons.

(2) REQUIRED RECOMMENDATIONS.—The recommendations under paragraph (1) shall include—

(A) feedback from financial institutions on best practices of successful programs to combat severe forms of trafficking in persons currently

in place that may be suitable for broader adoption by similarly situated financial institutions;

(B) feedback from stakeholders, including victims of severe forms of trafficking in persons, advocates of persons at risk of becoming victims of severe forms of trafficking in persons, and financial institutions, on policy proposals derived from the analysis conducted by the task force referred to in paragraph (1) that would enhance the efforts and programs of financial institutions to detect and deter money laundering relating to severe forms of trafficking in persons, including any recommended changes to internal policies, procedures, and controls relating to severe forms of trafficking in persons;

(C) any recommended changes to training programs at financial institutions to better equip employees to deter and detect money laundering relating to severe forms of trafficking in persons;

(D) any recommended changes to expand information sharing relating to severe forms of trafficking in persons among financial institutions and between such financial institutions,

appropriate law enforcement agencies, and appropriate Federal agencies; and

(E) recommended changes, if necessary, to existing statutory law to more effectively detect and deter money laundering relating to severe forms of trafficking in persons, where such money laundering involves the use of emerging technologies and virtual currencies.

(d) LIMITATION.—Nothing in this Act shall be construed to—

(1) grant rulemaking authority to the Interagency Task Force To Monitor and Combat Trafficking; or

(2) encourage financial institutions to deny services to victims of trafficking, victims of severe forms of trafficking in persons, or individuals not responsible for promoting severe forms of trafficking in persons.

(e) DEFINITIONS.—As used in this section—

(1) the term "appropriate Federal banking agency" has the meaning given the term in section 3(q) of the Federal Deposit Insurance Act (12 U.S.C. 1813(q));

(2) the term "severe forms of trafficking in persons" has the meaning given such term in section

103 of the Trafficking Victims Protection Act of 2000 (22 U.S.C. 7102);

(3) the term "Interagency Task Force To Monitor and Combat Trafficking" means the Interagency Task Force To Monitor and Combat Trafficking established by the President pursuant to section 105 of the Victims of Trafficking and Violence Protection Act of 2000 (22 U.S.C. 7103); and

(4) the term "law enforcement agency" means an agency of the United States, a State, or a political subdivision of a State, authorized by law or by a government agency to engage in or supervise the prevention, detection, investigation, or prosecution of any violation of criminal or civil law.

SEC. 3. COORDINATION OF HUMAN TRAFFICKING ISSUES BY THE OFFICE OF TERRORISM AND FINANCIAL INTELLIGENCE.

(a) FUNCTIONS.—Section 312(a)(4) of title 31, United States Code, is amended—

(1) by redesignating subparagraphs (E), (F), and (G) as subparagraphs (F), (G), and (H), respectively; and

(2) by inserting after subparagraph (D) the following:

"(E) combating illicit financing relating to severe forms of trafficking in persons;".

(b) INTERAGENCY COORDINATION.—Section 312(a) of title 31, United States Code, is amended by adding at the end the following:

"(8) INTERAGENCY COORDINATION.—The Secretary of the Treasury, after consultation with the Undersecretary for Terrorism and Financial Crimes, shall designate an office within the OTFI that shall coordinate efforts to combat the illicit financing of severe forms of trafficking in persons with—

"(A) other offices of the Department of the Treasury;

"(B) other Federal agencies, including—

"(i) the Office To Monitor and Combat Trafficking in Persons of the Department of State; and

"(ii) the Interagency Task Force To Monitor and Combat Trafficking;

"(C) State and local law enforcement agencies; and

"(D) foreign governments.".

(c) DEFINITION.—Section 312(a) of title 31, United States Code, as amended by this section, is further amended by adding at the end the following:

"(9) DEFINITION.—In this subsection, the term 'severe forms of trafficking in persons' has the meaning given such term in section 103 of the Trafficking Victims Protection Act of 2000 (22 U.S.C. 7102).".

SEC. 4. ADDITIONAL REPORTING REQUIREMENT UNDER THE TRAFFICKING VICTIMS PROTECTION ACT OF 2000.

Section 105(d)(7) of the Trafficking Victims Protection Act of 2000 (22 U.S.C. 7103(d)(7)) is amended—

(1) in the matter preceding subparagraph (A)—

(A) by inserting "the Committee on Financial Services," after "the Committee on Foreign Affairs,"; and

(B) by inserting "the Committee on Banking, Housing, and Urban Affairs," after "the Committee on Foreign Relations,";

(2) in subparagraph (Q)(vii), by striking "; and" and inserting a semicolon;

(3) in subparagraph (R), by striking the period at the end and inserting "; and"; and

(4) by adding at the end the following:

"(S) the efforts of the United States to eliminate money laundering relating to severe forms of trafficking in persons and the number

of investigations, arrests, indictments, and convictions in money laundering cases with a nexus to severe forms of trafficking in persons.''.

SEC. 5. MINIMUM STANDARDS FOR THE ELIMINATION OF TRAFFICKING.

Section 108(b) of the Trafficking Victims Protection Act of 2000 (22 U.S.C. 7106(b)) is amended by adding at the end the following new paragraph:

''(13) Whether the government of the country, consistent with the capacity of the country, has in effect a framework to prevent financial transactions involving the proceeds of severe forms of trafficking in persons, and is taking steps to implement such a framework, including by investigating, prosecuting, convicting, and sentencing individuals who attempt or conduct such transactions.''.

○

AMENDMENT IN THE NATURE OF A SUBSTITUTE

TO H.R. 295

OFFERED BY MR. ENGEL OF NEW YORK

Strike all after the enacting clause and insert the following:

SECTION 1. SHORT TITLE.

This Act may be cited as the "End Banking for Human Traffickers Act of 2019".

SEC. 2. INCREASING THE ROLE OF THE FINANCIAL INDUSTRY IN COMBATING HUMAN TRAFFICKING.

(a) REQUIRED REVIEW OF PROCEDURES.—Not later than 180 days after the date of the enactment of this Act, the Financial Institutions Examination Council, in consultation with the Secretary of the Treasury, the private sector, victims of severe forms of trafficking in persons, advocates of persons at risk of becoming victims of severe forms of trafficking in persons, and appropriate law enforcement agencies, shall—

(1) review and enhance training and examinations procedures to improve the capabilities of anti-money laundering and countering the financing of terrorism programs to detect financial transactions relating to severe forms of trafficking in persons;

(2) review and enhance procedures for referring potential cases relating to severe forms of trafficking in persons to the appropriate law enforcement agency; and

(3) determine, as appropriate, whether requirements for financial institutions are sufficient to detect and deter money laundering relating to severe forms of trafficking in persons.

(b) INTERAGENCY TASK FORCE RECOMMENDATIONS TARGETING MONEY LAUNDERING RELATED TO HUMAN TRAFFICKING.—

(1) IN GENERAL.—Not later than 270 days after the date of the enactment of this Act, the Interagency Task Force To Monitor and Combat Trafficking shall submit to the Committee on Financial Services and the Committee on the Judiciary of the House of Representatives, the Committee on Banking, Housing, and Urban Affairs and the Committee on the Judiciary of the Senate, and the head of each appropriate Federal banking agency—

(A) an analysis of anti-money laundering efforts of the United States Government and United States financial institutions relating to severe forms of trafficking in persons; and

(B) appropriate legislative, administrative, and other recommendations to strengthen efforts against money laundering relating to severe forms of trafficking in persons.

(2) REQUIRED RECOMMENDATIONS.—The recommendations under paragraph (1) shall include—

(A) feedback from financial institutions on best practices of successful programs to combat severe forms of trafficking in persons currently in place that may be suitable for broader adoption by similarly situated financial institutions;

(B) feedback from stakeholders, including victims of severe forms of trafficking in persons, advocates of persons at risk of becoming victims of severe forms of trafficking in persons, and financial institutions, on policy proposals derived from the analysis conducted by the task force referred to in paragraph (1) that would enhance the efforts and programs of financial institutions to detect and deter money laundering relating to severe forms of trafficking in persons, including any recommended changes to internal policies, procedures, and controls relating to severe forms of trafficking in persons;

(C) any recommended changes to training programs at financial institutions to better equip employees to deter and detect money laundering relating to severe forms of trafficking in persons;

(D) any recommended changes to expand information sharing relating to severe forms of trafficking in persons among financial institutions and between such financial institutions, appropriate law enforcement agencies, and appropriate Federal agencies; and

(E) recommended changes, if necessary, to existing statutory law to more effectively detect and deter money laundering relating to severe forms of trafficking in persons, where such money laundering involves the use of emerging technologies and virtual currencies.

(c) LIMITATION.—Nothing in this Act shall be construed to—

(1) grant rulemaking authority to the Interagency Task Force To Monitor and Combat Trafficking; or

(2) encourage financial institutions to deny services to victims of trafficking, victims of severe forms of trafficking in persons, or individuals not re-

sponsible for promoting severe forms of trafficking in persons.

(d) DEFINITIONS.—As used in this section—

(1) the term "appropriate Federal banking agency" has the meaning given the term in section 3(q) of the Federal Deposit Insurance Act (12 U.S.C. 1813(q));

(2) the term "severe forms of trafficking in persons" has the meaning given such term in section 103 of the Trafficking Victims Protection Act of 2000 (22 U.S.C. 7102);

(3) the term "Interagency Task Force To Monitor and Combat Trafficking" means the Interagency Task Force To Monitor and Combat Trafficking established by the President pursuant to section 105 of the Victims of Trafficking and Violence Protection Act of 2000 (22 U.S.C. 7103); and

(4) the term "law enforcement agency" means an agency of the United States, a State, or a political subdivision of a State, authorized by law or by a government agency to engage in or supervise the prevention, detection, investigation, or prosecution of any violation of criminal or civil law.

SEC. 3. COORDINATION OF HUMAN TRAFFICKING ISSUES BY THE OFFICE OF TERRORISM AND FINANCIAL INTELLIGENCE.

(a) FUNCTIONS.—Section 312(a)(4) of title 31, United States Code, is amended—

(1) by redesignating subparagraphs (E), (F), and (G) as subparagraphs (F), (G), and (H), respectively; and

(2) by inserting after subparagraph (D) the following:

"(E) combating illicit financing relating to severe forms of trafficking in persons;".

(b) INTERAGENCY COORDINATION.—Section 312(a) of title 31, United States Code, is amended by adding at the end the following:

"(8) INTERAGENCY COORDINATION.—The Secretary of the Treasury, after consultation with the Undersecretary for Terrorism and Financial Crimes, shall designate an office within the OTFI that shall coordinate efforts to combat the illicit financing of severe forms of trafficking in persons with—

"(A) other offices of the Department of the Treasury;

"(B) other Federal agencies, including—

"(i) the Office To Monitor and Combat Trafficking in Persons of the Department of State; and

"(ii) the Interagency Task Force To Monitor and Combat Trafficking;

"(C) State and local law enforcement agencies; and

"(D) foreign governments.".

(c) DEFINITION.—Section 312(a) of title 31, United States Code, as amended by this section, is further amended by adding at the end the following:

"(9) DEFINITION.—In this subsection, the term 'severe forms of trafficking in persons' has the meaning given such term in section 103 of the Trafficking Victims Protection Act of 2000 (22 U.S.C. 7102).".

SEC. 4. ADDITIONAL REPORTING REQUIREMENT UNDER THE TRAFFICKING VICTIMS PROTECTION ACT OF 2000.

Section 105(d)(7) of the Trafficking Victims Protection Act of 2000 (22 U.S.C. 7103(d)(7)) is amended—

(1) in the matter preceding subparagraph (A)—

(A) by inserting "the Committee on Financial Services," after "the Committee on Foreign Affairs,"; and

(B) by inserting "the Committee on Banking, Housing, and Urban Affairs," after "the Committee on Foreign Relations,";

(2) in subparagraph (Q)—

(A) in clause (vii), by inserting "and" after the semicolon; and

(B) in clause (viii), by striking "and" after the semicolon;

(3) in subparagraph (R), by striking "and" after the semicolon;

(4) in subparagraph (S), by striking the period and inserting "; and"; and

(5) by adding at the end the following:

"(T) the efforts of the United States to eliminate money laundering relating to severe forms of trafficking in persons and the number of investigations, arrests, indictments, and convictions in money laundering cases with a nexus to severe forms of trafficking in persons.".

SEC. 5. MINIMUM STANDARDS FOR THE ELIMINATION OF TRAFFICKING.

Section 108(b) of the Trafficking Victims Protection Act of 2000 (22 U.S.C. 7106(b)) is amended by adding at the end the following new paragraph:

"(13) Whether the government of the country, consistent with the capacity of the country, has in effect a framework to prevent financial transactions involving the proceeds of severe forms of trafficking in persons, and is taking steps to implement such a framework, including by investigating, prosecuting, convicting, and sentencing individuals who attempt or conduct such transactions.".

Chairman ENGEL. At this time I recognize myself to speak on today's business.

We have five good measures before us today and I am pleased to support them all. The first measure I want to discuss is H. Res. 156, a resolution I authored with Ranking Member McCaul that calls for justice for the assassination of Boris Nemtsov.

Nemtsov was a brave advocate for democracy and free elections in Russia. Sadly, that put him right in Vladimir Putin's cross hairs.

Now he joins a long list of brave journalists, human rights activists, and political opponents murdered by Putin's henchmen in their quest to silence all criticism of the Kremlin and stamp out any perceived threat to Putin's authoritarian regime.

This resolution condemns the Kremlin's systematic targeting of its political opponents and it calls on the administration to implement Magnitsky Act sanctions on those responsible for Nemtsov's murder and cover up.

It also requires the administration to deliver to Congress a thorough report on Nemtsov's assassination. That is a critical part of this legislation because, sadly, the administration has not done nearly enough to give us much reason to stand up to Russia and call out Putin's thuggery.

So it is up to Congress to assert American leadership on this issue and Putin's strong arm tactics extend beyond the authoritarian rule in his own country. We have seen this all too clearly in Russia's malign actions with its neighbors, which brings me to our next measure.

But before I do that, I want to just personally tell you I have on my desk in my office a picture of me shaking hands with Boris Nemtsov. It is shocking. When we moved offices I saw that picture. I had forgotten about it.

He came and visited me and told me he was the opponent of Putin and that he was for free, independent elections and for a free Russia.

I was very, very impressed with him and thought, wow, this man is really special. Unfortunately, Putin thought so too and had him killed right in Moscow. But I remember him telling me about how he felt how important his work was, and I told him that I thought he was really working, not for just the people in Russia, but for people all over the world.

So I want to just mention that because it was quite an honor for me to meet Boris Nemtsov and, of course, just a few months later he was murdered.

And so it is just startling.

The Crimea Annexation Nonrecognition Act puts that conviction into law by stating that the United States will not recognize Russia's claims of sovereignty in Ukraine.

Putin's disrespect for independent, sovereign democracies is something we in the United States know all too well. By advancing this legislation we send a clear message to our Ukrainian partners and their neighbors. We stand with you. I support this bill and I urge my colleagues to do the same.

And just as an aside, I have been a strong supporter of Ukraine being admitted to NATO and I think we should pursue that down the road.

It is critical that we support our partners and allies whenever they are under threat and that brings me to our next measure, H. Res. 75. I want to thank Mr. McCaul, Ms. Bass, and Mr. Smith for joining me in this resolution that strongly condemns the January 2019 attack by the terrorist group Al-Shabaab in Nairobi, Kenya.

This horrific attack killed dozens of people, including American citizen Jason Spindler. Just last week, we saw another Al-Shabaab attack in Mogadishu, Somalia, claim the lives of nearly 30 people.

So this resolution rightly affirms that the United States supports our regional partners in their ongoing efforts to counter terrorism and violent extremism in the Horn of Africa. I hope all members will join me in supporting this measure.

Next, I would like to discuss the End Banking for Human Traffickers Act introduced by Mr. Fitzpatrick and Mr. Keating. It is horrible that in 2019, we still live in a world where human beings are held in slavery. It is a moral outrage.

So we need to be consistently evaluating our government's efforts on this issue and looking for areas where we can improve. This bill does just that by having the financial industry play a bigger role in tracking down human traffickers.

By connecting the industry with experts on human trafficking, banks and other financial institutions will be better equipped to spot suspect financial transactions that may be related to this heinous criminal enterprise.

This bill continues our fight against the scourge of human trafficking, and I urge my colleagues to join me in supporting it.

And finally, we turn to Ranking Member McCall's bill, the Cyber Diplomacy Act. Last Congress, I worked with Chairman Royce on this bill and we got it through this committee, the House, and the Senate Foreign Relations Committee with broad bipartisan support.

This Congress, Ranking Member McCaul has taken up that mantle and I am pleased to join him as we work to get this bill over the finish line and on the president's desk.

Cyberspace is an increasingly critical part of foreign policy and we desperately need to update our government agencies to reflect that reality.

America has significant interest in cybersecurity, the digital economy, issues of internet freedom, and we need to be engaging with the international community to articulate and protect those interests.

If we do not focus on all of these areas, we run the real risk of seeing authoritarian regimes like Russia and China playing a bigger role in determining the way the international community handles these issues.

So this bill would create a high-level Ambassador position at the State Department dedicated to this endeavor and require a comprehensive cyberspace strategy.

I am frustrated by the lack of progress on this issue at the State Department, and I hope they will work with us to ensure that this bill becomes law.

I hope my colleagues will join me in supporting this measure.

Thank you to all of our members for your hard work on these good bills before us today. As I said before, I am pleased to support them all.

And now, I recognize the ranking member, Mike McCaul of Texas, for his opening remarks.

Mr. MCCAUL. Thank you, Mr. Chairman.

Today, our committee will markup three important bills and two resolutions, the Cyber Diplomacy Act, which I introduced with you, Mr. Chairman. I want to thank you for working with me on that. It takes several steps to support an open and secure cyberspace. As chairman of Homeland Security, I elevated the mission at the Department of Homeland Security and I intend to do the same with you, sir, at the Department of State.

It establishes an ambassador at large to lead the State's cyber diplomacy efforts, outlines an international cyber policy to advance democratic principles and reject Russian and Chinese attempts to control and censor the internet.

It requires the State Department to provide assessments related to internet freedom, freedoms in other countries, and, as you know, Mr. Chairman, malicious cyber activity by State and non-State actors threatens our national security and harms our economic interests.

We understand the State Department has plans for a new cyber bureau, which varies a little bit from what our bill calls for. I pledge to work with the State Department and you, Mr. Chairman, and the Senate to find the best path forward to advance our shared goals of bolstering and elevating State's critical cyber mission.

I also want to thank Mr. Fitzpatrick and Mr. Keating for their bipartisan bill, the End Banking for Human Traffickers Act, which will help address the scourge of human trafficking.

This bill will help choke off traffickers' access to financial systems. It is time we put an end to this modern-day form of slavery once and for all.

We are also marking up the Crimea Annexation Nonrecognition Act. This bill clearly states that America will not recognize Russian sovereignty over Crimea.

Doing so would condone Russia's belligerent behavior toward its neighbors. Vladimir Putin needs to understand that we will not tolerate this kind of aggression in Crimea or anywhere else in the world.

And that is also why today's resolution condemning the assassination of Boris Nemtsov is also important. We cannot be silent when political opponents are targeted for supporting democratic reforms.

I was proud to introduce this resolution with Chairman Engel because Putin needs to know that both Democrats and Republicans will call out and condemn his authoritarian ways.

And finally, we must continue to stand united in our fight against Islamist terrorism. The terror attack in Nairobi, Kenya, on January the 15th that killed 21 people including Jason Spindler, a fellow Texan, was a painful reminder that our fight against terrorism is a global struggle.

Our resolution condemns this attack and reaffirms our commitment to eradicating this evil.

I look forward to passing these bills out of committee with bipartisan support.

And, finally, Mr. Chairman, on the floor and in the halls of Congress there has been much discussion recently about anti-Semitism. I want to thank you for your leadership on this issue and I look forward to continuing to work with you on measures that support our close ally, Israel, and denounce anti-Semitism wherever it may be.

And with that, I yield back the balance of my time.

Chairman ENGEL. Thank you, Mr. McCaul.

Are there any other members seeking recognition?

Mr. CONNOLLY. Mr. Chairman?

Chairman ENGEL. Yes, Mr. Connolly.

Mr. CONNOLLY. I thank the chair and the ranking member. I want to thank them both for putting together this bipartisan package of five bills for our consideration today.

These measures condemn terrorist attacks, strengthen U.S. diplomacy, condemn Russia's violations of human rights and territorial sovereignty, and bolster U.S. efforts to reduce global human trafficking, the scourge of our time.

In particular, Mr. Chairman, I would like to thank you and the ranking member for including in this markup H.R. 596, the Crimea Annexation Nonrecognition Act, which I introduced with my good friend and Republican colleague, Representative Steve Chabot.

This bill states that it is the policy of the United States not to recognize the Russian Federation's claim of sovereignty over Crimea, its airspace, or its territorial waters.

Furthermore, this bill prohibits the U.S. Government from taking any action that implies recognition of Russian sovereignty over Crimea.

It has been the longstanding policy of the United States to not recognize territorial changes effected by force as dictated by the long-ago Stimson Doctrine established in 1932 by then-Secretary of State Henry Stimson.

The matter of rejecting the forcible and illegal attack on sovereign territory is so important we should be satisfied with nothing less than absolute clarity about our position, which is one that supports Ukraine sovereignty over its own territory in Crimea.

Failure to stand up, as Mr. McCaul just said, to Putin's illegal annexation of Crimea sets a dangerous and irrevocable precedent. Crimea was Russia's original violation in Ukraine and we have limited credibility objecting to Russia's subsequent invasion of the Luhansk and Donetsk if we do not take a stand in Crimea.

Russian occupation of Crimea has inflicted great harm within the Ukraine, throughout former Soviet occupied territories, and beyond.

What has happened in Ukraine—Russia's forcible and illegal annexation of Crimea, its invasion of Eastern Ukraine, and continued occupation in Crimea, Luhansk and Donetsk, has precipitated an international crisis and the resulting conflict has claimed more than 10,000 lives.

Russia has subjected Crimeans who refuse Russian citizenship to discrimination in accessing education, health care, and employ-

ment, and Russian authorities have attacked travel rights and the free press.

Acquiesence on the part of the United States threatens the security of all sovereign nations. Russia's forcible and illegal annexation of Crimea has sent shock waves throughout the former Soviet occupied territories, many of whom are now NATO allies, including the Baltic States.

After the Welles Declaration in June 1940, the U.S. refused to recognize the Soviet Union's de facto or de jure sovereignty over the Baltics during the Soviet Union's 50 years of illegal occupation.

The Baltic Republics eventually received their independence and they are now reliable NATO allies, in part because of our steadfastness.

We first introduced this bill in the wake of Russia's forcible and illegal annexation in 2014. This committee previously passed this legislation in the 113th Congress.

I inserted similar language into the Fiscal Year 2016 National Defense Authorization Act in order to prohibit the use of defense funds in a manner that recognizes Russian sovereignty over Crimea. That is to say that we did not.

That language has remained in the NDAA, I am grateful to say, every year since. I have also successfully authored an amendment to Stand For Ukraine Act, which would create only one condition under which the president can relax Crimea-related sanctions—the restoration of Ukraine sovereignty.

The United States must lead the way in refusing to recognize or legitimize Russia's illegal and forcible annexation in Crimea. That is why both Mr. Chabot and I are glad to offer this bill, which expresses the will of Congress as a loud and declarative voice for sovereignty and freedom and I urge my colleagues to support it.

And, again, I thank the chair and ranking member for including it in today's markup. I yield back.

Chairman ENGEL. Thank you very much, Mr. Connolly.

Mr. SMITH.

Mr. SMITH. Thank you very much, Mr. Chairman.

Chairman, I strongly support your resolution, H. Res. 156, calling for accountability and justice for the assassination of Boris Nemtsov, a Russian patriot killed in 2015, a great defender of democracy in his home country of Russia.

Last July, I had the privilege of leading the United States delegation to the OSCE Parliamentary Assembly in Berlin and I actually chaired the public event that you reference in your resolution, the July 8th public event, and we featured Hanna Nemtsova, Boris Nemtsov's daughter, who was absolutely compelling and brave and full of courage.

Boris's friend and colleague, Vladimir Kara-Murza, who serves as chairman of the board of trustees for the Boris Nemtsov Foundation for Freedom, and Vadim Prokhorov, who is a lawyer for the Nemtsov family.

I believe that this resolution is a timely followup to that OSCE effort because we have been calling on the administration to do more and I think the fact that you articulate the concern and the need, frankly, to do some better reporting and to hold those respon-

sible besides the five low-level individuals who have been tried—who ordered the hit.

It was an assassination, and it seems to me that it is time, frankly, to really impose Magnitsky sanctions on those who are directly responsible for this. But we need that information. We need our government to redouble down. So thank you for that resolution.

Second, I do want to thank you for marking up H.R. 295, the End Banking for Human Traffickers Act of 2019. This is authored, of course, by my good friend and colleague, Mr. Fitzpatrick.

This bill will help ensure that human traffickers find trafficking even more unprofitable because they will be curbed in their financial work that they do. They often use banks. This helps to increase that net to catch these people.

We have been making strides, Mr. Chairman, in this direction. For example, last Congress the Frederick Douglass Trafficking Victims Prevention and Protection Reauthorization Act, which I authored along with my friend and colleague, Karen Bass, the prime Democratic co-sponsor, was signed into law on January 8th, and among its many provisions, it added the secretary of the Treasury to the President's Inter-Agency Task Force to monitor and combat trafficking in persons.

H.R. 295 calls on the task force to evaluate the anti-money laundering efforts of the U.S. Government and U.S. financial institutions to see if we are doing enough, and I do not think we are, to recognize and act against financial movements to signal red flags that human trafficking is occurring.

The task force will consult with trafficking survivors and the financial industry representatives who have been pioneering anti-trafficking efforts in their best practices.

So, again, I want to thank you for all of these bills. I think they are all excellent pieces of legislation and I especially want to thank Mr. Fitzpatrick for his leadership on combatting the scourge of human trafficking.

Chairman ENGEL. Thank you, Mr. Smith.

Is there anyone else who seeks recognition?

Mr. CHABOT. Mr. Chairman? Mr. Chairman?

Chairman ENGEL. Mr. Chabot.

Mr. CHABOT. Thank you, Mr. Chairman. Move to strike the last word.

Mr. Chairman, I want to thank you for holding this markup today, and I want to thank you for this slate of five excellent bipartisan bills.

First, Ukraine—I am honored to be the lead Republican co-sponsor of H.R. 596, Mr. Connolly's Crimean Annexation Nonrecognition Act, and I want to thank him for his hard work on this important legislation.

We have been working together on this since the bully Putin first acted on Crimea. I know a number of members of this committee have done so and I think it is critical that we continue to do so. So I want to thank Mr. Connolly for his hard work on this.

Passage of this bill would cement firmly in place the policy that the United States will not recognize Putin's bogus claims over Crimea and will prohibit any part of our government from taking any

action that would imply our recognition of Russian sovereignty over the peninsula.

It is vitally important that we support a democratic and unified Ukraine by not giving in to Putin's thuggish behavior and that behavior continues.

For example, in November, Russian vessels blockaded the Kerch Strait, the entrance to the Sea of Azov, and illegally seized Ukrainian naval vessels.

By these and other actions, Putin is seeking to strangle Ukraine's trade and in all likelihood annex more of it. We cannot let that happen. The world cannot stand by as it did previously when Putin annexed Crimea.

Unfortunately, Putin's gangster ways are not confined to his foreign policy. That is why we are considering H. Res. 156, which I am also a co-sponsor of. This resolution calls for justice for Boris Nemtsov, who, as was mentioned, was murdered in cold blood near the Kremlin on February 25th of 2015.

For those who do not know, Mr. Nemtsov was a leading opposition figure, outspoken Putin critic, and the former first deputy prime minister of Russia and was in all likelihood—we do not know for absolutely sure—but in all likelihood was executed at the direction of Putin.

The Russian government must do a thorough investigation to uncover the truth behind Mr. Nemtsov—that we should not let this rest.

I also want to turn briefly to a couple of other bills we have. The terrorist attack on Kenya earlier this year is yet another example of the scourge of radical terrorism and we must continue to fight against that every time it rears its ugly head.

That is why I am a co-sponsor of H. Res. 75. And finally, I want to thank Ranking Member McCaul for his leadership on the critical issue of Cybersecurity.

As a co-sponsor of the Cyber Diplomacy Act, I think it is necessary that we work with our like-minded allies to ensure that the internet remains a place of robust debate and access to uncensored information.

This legislation provides the State Department tools and direction to help accomplish this important priority, and I want to echo the words that our ranking member mentioned before—Mr. McCaul.

I completely agree with him that there is absolutely no place for anti-Semitism in this country, on this globe, or in this committee. I have been on this committee for a long time—23 years—and we have always been bipartisan on that issue. I would hope that would continue.

Israel is a strong ally of the United States. The Jewish people have been for a long time and will continue to be, whether it is as a nation or whether as a people, and there is absolutely no room for anti-Semitism.

And I think that we should work on that in a bipartisan manner, and it always has been that way. I hope it will be in the future. There is absolutely no place for anti-Semitism.

Thank you, Mr. Chairman.

Chairman ENGEL. Thank you very much, Mr. Chabot.

Mr. MALINOWSKI.

Mr. MALINOWSKI. Thank you. Thank you so much, Chairman Engel, Ranking Member McCaul.

I wanted to say a few words in particular about the resolution regarding Boris Nemtsov and to explain the two small amendments that I will be offering today.

First of all, thank you for introducing this resolution to help us remember this very good man and to put the Putin regime on notice that we are not going to forget what happened and who is responsible.

If you read the resolution, you will see that one of the central villains in this terrible story is Ramzan Kadyrov, the strong man who rules and has ruled Chechnya with an iron hand for many, many years.

Even the flawed Russian investigation of the murder of Mr. Nemtsov determined that the murder was carried out by members of an elite battalion loyal to Kadyrov.

Kadyrov publicly praised the gunmen. Previously, he had publicly called for the death of Nemtsov. One of the chief suspects is still living at large in Chechnya under Kadyrov's protection.

Kadyrov has also, over the years, been credibly accused of murdering human rights activists, journalists. He has ordered his police forces to round up and torture gay men and women in Chechnya. He has ordered the assassination of his critics living in other countries, in Europe, and in the Middle East.

In 2017, the U.S. Government put Mr. Kadyrov on the Global Magnitsky sanctions list, which means that his business activities overseas involving any sort of transactions through international banks should be blocked.

In reality, though, Mr. Kadyrov has repeatedly shown himself outside of Russia, particularly in Persian Gulf countries such as the UAE and Saudi Arabia.

His hobby is horse racing. He spends millions of dollars purchasing race horses, winning races around the world, again, particularly in the Middle East.

He is blocked in Europe. What my first amendment does is simply to urge the administration to prioritize sanctions-enforcement with respect to Ramzan Kadyrov, to investigate his business activities and that of entities he may control outside of the Russian federation and to determine whether any of them might implicate the sanctions that we have imposed.

The second amendment ensures that the resolution includes an additional key suspect in Mr. Nemtsov's murder, Adam Delimkhanov, who is a notorious associate and relative of Ramzan Kadyrov.

Delimkhanov is a member of the Russian State Duma where he has abused his immunity to shield himself from accountability for a range of human rights abuses.

He has been identified by multiple independent sources as one of the organizers of Mr. Nemtsov's murder. So this amendment would add his name to the list of suspects in two clauses of the resolution's preamble.

I ask my colleagues to support both of these amendments. Thank you very much.

Chairman ENGEL. Thank you, Mr. Malinowski.

Mr. FITZPATRICK.

Mr. FITZPATRICK. Thank you, Mr. Chairman.

Chairman, Ranking Member, I really do appreciate your considering of H.R. 295. As an FBI agent, one of the most horrific crimes that we were called upon to investigate was human trafficking, and human trafficking continues to devastate millions of lives around the world.

And this criminal conduct may seem a distant problem but it is far from it. It exists right in all of our back yards, in every single congressional district in this country, in all of our communities, and at times it is right in front of us and we do not even know it exists.

My legislation, H.R. 295, the End Banking of Human Traffickers Act, is one step we can take to end the suffering caused by human trafficking.

Traffickers are not hiding their illegal profits under a mattress or burying them in their back yard. They use our very sophisticated global financial system to launder their illicit funds through banks, credit card companies, and money transfer companies, which are all used by traffickers to facilitate their business and to perpetuate their exploitation of victims.

The scale of profits from this illicit trade is really staggering. The International Labor Organization estimates that over $150 billion in illegal profits are made from forced labor each year, and $99 billion are earned through the exploitation of victims of sexual exploitation, making human trafficking the third most lucrative criminal enterprise on this planet.

The perpetrators of this exploitation play on the defenseless in our society, including young children. Cutting off their access to the banking system is a critical aspect both from the investigative standpoint, and the legislative standpoint and I am proud to push this bipartisan bill with my friend and colleague, Congressman Keating, to continue working to end this horror once and for all.

And I thank my colleagues both on and off this committee for their support, many of whom have joined this effort. I also want to thank Congressman Chris Smith from New Jersey, who has made it one of his top priorities to advance this mission.

This legislation directs Federal banking regulators to work with law enforcement and financial institutions to combat the use of the financial system for human trafficking.

The bill further increases collaboration between law enforcement and experts in financial crimes by adding financial intelligence and regulatory officers to the President's Inter-Agency Task Force to monitor and combat trafficking in persons and requires the task force to develop recommendations for Congress and regulators that would strengthen anti-money laundering programs to better target human trafficking.

Moreover, this bill allows advocates of human trafficking victims to serve as stakeholders and to provide feedback to the U.S. Treasury and, additionally, clarifies that banks not restrict trafficker victims' access to bank accounts.

I urge ever Member of Congress, especially those on this committee, to support this legislation, which passed both the committee and the House last Congress with broad bipartisan support.

We must do everything possible to put an end to human trafficking and this legislation is a very important step along that path.

Mr. Chairman, I yield back.

Chairman ENGEL. Thank you, Mr. Fitzpatrick.

Is there anyone else who seeks recognition?

OK. Hearing no further requests for recognition, then without objection the committee will proceed to consider the noticed items en bloc. A reporting quorum is present.

Without objection, the question occurs on the measures en bloc as amended.

All those in favor, say aye.

All those opposed, no.

In the opinion of the chair, the ayes have it.

The measures considered en bloc are agreed to and without objection each measure in the en bloc is ordered favorably reported as amended and each amendment to each bill shall be reported as a single amendment in the nature of a substitute.

Without objection, staff is authorized to make any technical and conforming changes and the chair is authorized to seek House consideration under suspension of the rules.

This concludes——

Mr. MCCAUL. Mr. Chairman?

Chairman ENGEL. Yes, Mr. McCaul.

Mr. MCCAUL. Pursuant to House rules, I request that members have the opportunity to submit views for any committee report that may be produced on any of today's measures.

Chairman ENGEL. Obviously, there is no objection to that and I thank Ranking Member McCaul and all of the committee members for their contribution and assistance with today's markup.

The committee stands adjourned.

[Whereupon, at 10:37 a.m., the committee was adjourned.]

FULL COMMITTEE MARKUP NOTICE
COMMITTEE ON FOREIGN AFFAIRS
U.S. HOUSE OF REPRESENTATIVES
WASHINGTON, DC 20515-6128

Eliot L. Engel (D-NY), Chairman

March 7, 2019

TO: MEMBERS OF THE COMMITTEE ON FOREIGN AFFAIRS

You are respectfully requested to attend an OPEN markup of the Committee on Foreign Affairs to be held in Room 2172 of the Rayburn House Office Building (and available live on the Committee website at https://foreignaffairs.house.gov/):

DATE: Thursday, March 7, 2019

TIME: 10:00 a.m.

MARKUP OF: H.Res. 75, Strongly condemning the January 2019 terrorist attack on the 14 Riverside Complex in Nairobi, Kenya

H.R. 739, Cyber Diplomacy Act of 2019

H.Res. 156, Calling for accountability and justice for the assassination of Boris Nemtsov

H.R. 596, Crimea Annexation Non-recognition Act

H.R. 295, End Banking for Human Traffickers Act of 2019

By Direction of the Chairman

The Committee on Foreign Affairs seeks to make its facilities accessible to persons with disabilities. If you are in need of special accommodations, please call 202/225-5021 at least four business days in advance of the event, whenever practicable. Questions with regard to special accommodations in general (including availability of Committee materials in alternative formats and assistive listening devices) may be directed to the Committee.

COMMITTEE ON FOREIGN AFFAIRS

MINUTES OF FULL COMMITTEE MARKUP

Day *Thursday* **Date** *03/07/19* **Room** *2172 RHOB*

Starting Time *10:05 a.m.* **Ending Time** *10:37 a.m.*

Recesses *0* (____to____) (____to____) (____to____) (____to____) (____to____) (____to____)

Presiding Member(s)
Chairman Eliot Engel

Check all of the following that apply:

Open Session ☑
Executive (closed) Session ☐
Televised ☑

Electronically Recorded (taped) ☑
Stenographic Record ☑

BILLS FOR MARKUP: *(Include bill number(s) and title(s) of legislation.)*
H.Res. 75, Strongly condemning the January 2019 terrorist attack on the 14 Riverside Complex in Nairobi, Kenya
H.R. 739, Cyber Diplomacy Act of 2019
H.Res. 156, Calling for accountability and justice for the assassination of Boris Nemtsov
H.R. 596, Crimea Annexation Non-recognition Act
H.R. 395, End Banking for Human Traffickers Act of 2019

COMMITTEE MEMBERS PRESENT:
See attached.

NON-COMMITTEE MEMBERS PRESENT:
N/A

STATEMENTS FOR THE RECORD: *(List any statements submitted for the record.)*
SFR_Castro

ACTIONS TAKEN DURING THE MARKUP: *(Attach copies of legislation and amendments.)*

The measures considered en bloc were agreed to by voice vote.

RECORDED VOTES TAKEN (FOR MARKUP): *(Attach final vote tally sheet listing each member.)*

Subject	Yeas	Nays	Present	Not Voting
N/A	*N/A*	*N/A*	*N/A*	*N/A*

TIME SCHEDULED TO RECONVENE _____
or
TIME ADJOURNED *10:37 a.m.*

Evan Burberry

Full Committee Hearing Coordinator

HOUSE COMMITTEE ON FOREIGN AFFAIRS

FULL COMMITTEE MARKUP

PRESENT	*MEMBER*
X	Eliot L. Engel, NY
X	Brad Sherman, CA
	Gregory W. Meeks, NY
X	Albio Sires, NJ
X	Gerald E. Connolly, VA
	Theodore E. Deutch, FL
	Karen Bass, CA
	William Keating, MA
	David Cicilline, RI
	Ami Bera, CA
X	Joaquin Castro, TX
X	Dina Titus, NV
	Adriano Espaillat, NY
X	Ted Lieu, CA
X	Susan Wild, PA
X	Dean Phillips, MN
X	Ilhan Omar, MN
X	Colin Allred, TX
X	Andy Levin, MI
X	Abigail Spanberger, VA
X	Chrissy Houlahan, PA
X	Tom Malinowski, NJ
	David Trone, MD
X	Jim Costa, CA
X	Juan Vargas, CA
X	Vicente Gonzalez, TX

PRESENT	*MEMBER*
X	Michael T. McCaul, TX
X	Christopher H. Smith, NJ
X	Steve Chabot, OH
	Joe Wilson, SC
X	Scott Perry, PA
X	Ted Yoho, FL
X	Adam Kinzinger, IL
X	Lee Zeldin, NY
	James Sensenbrenner, Jr., WI
X	Ann Wagner, MO
X	Brian J. Mast, FL
X	Francis Rooney, FL
X	Brian K. Fitzpatrick, PA
X	John Curtis, UT
X	Ken Buck, CO
X	Ron Wright, TX
X	Guy Reschenthaler, PA
X	Tim Burchett, TN
X	Greg Pence, IN
X	Steve Watkins, KS
X	Michael Guest, MS

Statement for the Record from Representative Joaquin Castro
Markup of Various Measures
March 7, 2019

Thank you, Chairman Engel and Ranking Member McCaul, for your leadership on this committee.

I want to congratulate all the members whose bills are being considered here today.

These measures cover a wide range of challenges we face around the world.

These challenges include terrorism, assassination, cyber diplomacy, human trafficking, international aggression—all of which fall within this Committee's jurisdiction.

I am happy to support each of the measures brought today that will address these important issues.

I'd like to speak about just a few.

Firstly, we are acutely aware of the many challenges that cyber space presents to our national security.

Our adversaries have actively used the domain to meddle in our democracy, steal data, and much more.

But there are also opportunities to strengthen diplomacy to address these challenges and in turn strengthen our alliances abroad.

It is only natural that we should complement our cyber defenses with cyber diplomacy.

This bipartisan bill sets forth a U.S. international cyberspace policy that promotes an open, interoperable, reliable, unfettered, and secure Internet.

It also lays out a model that promotes human rights, democracy, and the rule of law, while respecting privacy and guarding against deception, fraud, and theft.

The State Department will have the lead in setting cyber diplomacy policy with the establishment of an Office of Cyber Issues.

This legislation will improve our nation's ability to conduct cyber diplomacy within a policy framework.

I'm happy to support this important measure that will strengthen U.S. national security and diplomacy abroad.

We've seen Putin's growing aggression and disregard for international law with his annexation of Crimea in 2014, hacking of our democracy in 2016, 2018 and now likely 2020, and repeated murders of opposition figures within Russia's society.

I'd like to thank Mr. Chabot for sending Congress' disapproval message of the annexation of Crimea, and introducing a resolution that will prohibit any federal department from recognizing Russia as exercising sovereignty over Crimea.

It only makes logical sense that the U.S. government should not be in the business of rewarding such aggression.

This resolution makes the correct statement of policy that the U.S. government will not recognize Russia's annexation of Crimea and I'm proud to support it.

I would also like to voice my support for this resolution that demands justice for Boris Nemtsov, a Russian statesman who was assassinated in February of 2015.

Mr. Nemtsov had an unwavering commitment to the ideals of democracy, freedom, and the rule of law, vocally opposing the authoritarianism espoused by Vladimir Putin.

Ultimately becoming victim to state-sponsored murder, this is not an isolated event.

From Saudi Arabia, to North Korea, and other places in between, we continue to see authoritarians target people who dare to critique their policies and regimes.

We have a President who would rather nurture relationships with authoritarian thugs than repudiate their strong man tactics.

This resolution allows Congress to send a message loud and clear.

Brutal authoritarian regimes that target their political critics are a threat to democracy and rule of law globally.

Lastly, human traffickers are preying on vulnerable populations throughout the world.

We must do everything in our power to combat an issue that in many cases amounts to modern day slavery.

One facet of that is clamping down on financial streams that breathe life into these networks.

This legislation does just that, and I'm proud to support it.

I'm glad to support all the measures before us today.

Thank you again Mr. Chairman for your leadership, and to my colleagues for introducing these important measures.

03/07/2019 House Foreign Affairs Committee Markup Summary

By unanimous consent, the Chair called up the following measures and amendments, previously provided to Members, to be considered *en bloc:*

(1). H.Res. 75, Strongly condemning the January 2019 terrorist attack on the 14 Riverside Complex in Nairobi Kenya, (Engel)

(2) H.R. 739, Cyber Diplomacy Act of 2019, (McCaul)

- McCaul Amendment #14

(3) H.Res. 156, Calling for accountability and justice for the assassination of Boris Nemtsov (Engel)

- Malinowski Amendment #11
- Malinowski Amendment #A1

(4) H.R. 596, Crimea Annexation Non-recognition Act (Connolly)

- Connolly, an amendment in the nature of a substitute to H.R. 596

(5) H.R. 295, End Banking for Human Traffickers Act of 2019 (Fitzpatrick)

- Engel, an amendment in the nature of a substitute to H.R. 295

The measures considered *en bloc* were agreed to by voice vote.

By unanimous consent, the measures were ordered favorably reported, as amended, to the House, and the Chairman was authorized to seek House consideration under suspension of the rules.

The Committee adjourned.

○