112TH CONGRESS
1ST SESSION

S. 1469

To require reporting on the capacity of foreign countries to combat cybercrime, to develop action plans to improve the capacity of certain countries to combat cybercrime, and for other purposes.

IN THE SENATE OF THE UNITED STATES

AUGUST 2, 2011

Mrs. GILLIBRAND (for herself and Mr. HATCH) introduced the following bill; which was read twice and referred to the Committee on Foreign Relations

---

A BILL

To require reporting on the capacity of foreign countries to combat cybercrime, to develop action plans to improve the capacity of certain countries to combat cybercrime, 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.

This Act may be cited as the ''International Cybercrime Reporting and Cooperation Act''.

SEC. 2. DEFINITIONS.

In this Act:

(1) COMPUTER SYSTEMS; COMPUTER DATA.—The terms ''computer system'' and ''computer data'' have the meanings given those terms in chapter I of the Convention on Cybercrime.

(2) CONVENTION ON CYBERCRIME.—The term ''Convention on Cybercrime'' means the Council of Europe Convention on Cybercrime, done at Budapest November 23, 2001, as ratified by the United States Senate with any relevant reservations or declarations.

(3) CYBERCRIME.—The term ''cybercrime'' refers to criminal offenses relating to computer systems or computer data described in the Convention on Cybercrime.

(4) ELECTRONIC COMMERCE.—The term ''electronic commerce'' has the meaning given that term in section 1105(3) of the Internet Tax Freedom Act (47 U.S.C. 151 note).

(5) INTERPOL.—The term ''INTERPOL'' means the International Criminal Police Organization.

(6) LEAD FEDERAL AGENCY.—The term ''lead Federal agency'' means one of the relevant Federal agencies designated by the President to have pri-

mary responsibility for producing the annual reports required by section 3.

(7) RELEVANT FEDERAL AGENCIES.—The term ''relevant Federal agencies'' means any Federal agency that has responsibility for combating cybercrime globally, including the Department of Commerce, the Department of Homeland Security, the Department of Justice, the Department of State, the Department of the Treasury, and the Office of the United States Trade Representative.

(8) UNITED STATES PERSON.—The term ''United States person'' means—

(A) a United States citizen or an alien lawfully admitted for permanent residence to the United States; or

(B) an entity organized under the laws of the United States or of any jurisdiction within the United States.

SEC. 3. ANNUAL REPORT.

(a) IN GENERAL.—Not later than 1 year after the date of the enactment of this Act, and annually thereafter, the head of the lead Federal agency shall submit to Congress a report—

(1) assessing, after consultation with the entities specified in subsection (c) and with respect to each country described in subsection (b)—

(A) the extent and nature of activities relating to cybercrime that are attributable to persons or property based in the country and impact the United States Government, United States persons, or United States electronic commerce;

(B) the adequacy and effectiveness of the laws, regulations, and judicial and law enforcement systems in the country with respect to combating cybercrime; and

(C) measures taken by the government of the country to protect consumers from cybercrime, including measures described in the Convention on Cybercrime;

(2) assessing, after consultation with the entities specified in subsection (c), any multilateral efforts—

(A) to prevent and investigate cybercrime;

(B) to develop and share best practices with respect to directly or indirectly combating cybercrime; and

(C) to cooperate and take action with respect to the prevention, investigation, and prosecution of cybercrime; and

(3) describing the steps taken by the United States to promote the multilateral efforts described in paragraph (2).

(b) COUNTRIES DESCRIBED.—A country described in this subsection is a country that the head of the lead Federal agency determines, in consultation with the entities specified in subsection (c), is significant with respect to efforts to combat cybercrime—

(1) against the United States Government or United States persons; or

(2) that disrupts United States electronic commerce or otherwise negatively impacts the trade or intellectual property interests of the United States.

(c) ENTITIES SPECIFIED.—The entities specified in this subsection are the relevant Federal agencies, industry groups, civil society organizations, and other organizations selected by the President for consultations under this section based on their interest in combating cybercrime.

(d) CONTRIBUTIONS FROM RELEVANT FEDERAL AGENCIES.—Not later than 30 days before the date on which the report is required to be submitted under subsection (a), the head of each of the relevant Federal agen-

cies shall submit to the head of the lead Federal agency a report containing—

(1) any information obtained by the relevant Federal agency with respect to incidents of cybercrime, impediments to electronic commerce, or efforts of the United States to cooperate with other countries with respect to combating cybercrime; and

(2) any other information obtained by the agency that is relevant to the report required by subsection (a).

(e) ADDITIONAL INFORMATION TO BE INCLUDED IN SUBSEQUENT REPORTS.—In each report required to be submitted under subsection (a) after the first report required by that subsection, the head of the lead Federal agency shall include, in addition to the information required by that subsection—

(1) an identification of countries for which action plans have been developed under section 5; and

(2) an assessment, after consultation with the entities specified in subsection (c), of the extent of the compliance of each such country with the action plan developed for that country.

(f) FORM OF REPORT.—The report required by subsection (a) shall be submitted in unclassified form, but may contain a classified annex.

SEC. 4. UTILIZATION OF FOREIGN ASSISTANCE PROGRAMS.

(a) PRIORITY WITH RESPECT TO FOREIGN ASSISTANCE PROGRAMS TO COMBAT CYBERCRIME.—

(1) IN GENERAL.—The President shall give priority to a country described in paragraph (2) with respect to foreign assistance and other programs designed to combat cybercrime in the country by improving the effectiveness and capacity of the legal and judicial systems and the capabilities of law enforcement agencies with respect to cybercrime.

(2) COUNTRIES DESCRIBED.—A country described in this paragraph is a country described in section 3(b) that the President, in consultation with the entities described in section 3(c), determines has a low capacity to combat cybercrime.

(b) SENSE OF CONGRESS WITH RESPECT TO BILATERAL AND MULTILATERAL ASSISTANCE.—It is the sense of Congress that—

(1) the President should include programs designed to combat cybercrime in any bilateral or multilateral assistance that—

(A) is provided to a country described in subsection (a)(2); and

(B) addresses the critical infrastructure, telecommunications systems, financial industry,

legal or judicial systems, or law enforcement capabilities of that country; and

(2) such assistance should be provided in a manner that allows the country to sustain the advancements in combating cybercrime resulting from the assistance after the termination of the assistance.

SEC. 5. ACTION PLANS FOR COMBATING CYBERCRIME FOR COUNTRIES OF CYBER CONCERN.

(a) DEVELOPMENT OF ACTION PLANS.—

(1) IN GENERAL.—Not later than 1 year after the head of the lead Federal agency submits the first report required by section 3(a), the President shall develop, for each country that the President determines under subsection (b) is a country of cyber concern, an action plan—

(A) to assist the government of that country to improve the capacity of the country to combat cybercrime; and

(B) that contains benchmarks described in subsection (c).

(2) REASSESSMENT OF COUNTRIES.—Not later than 2 years after the head of the lead Federal agency submits the first report required by section 3(a), and annually thereafter, the President shall—

(A) reassess the countries for which the President has developed action plans under paragraph (1);

(B) determine if any of those countries no longer meet the criteria under subsection (b) for being countries of cyber concern; and

(C) determine if additional countries meet the criteria under subsection (b) for being countries of cyber concern and develop action plans for those countries.

(3) CONSULTATIONS.—The President, acting through the head of the lead Federal agency and, as appropriate, an employee designated to have responsibility for cybercrime under section 6 or 7, shall consult with the government of each country for which the President develops an action plan under paragraph (1) or (2) with respect to—

(A) the development of the action plan; and

(B) the efforts of the government of that country to comply with the benchmarks set forth in the action plan.

(b) COUNTRIES OF CYBER CONCERN.—The President shall determine that a country is a country of cyber concern if the President finds that—

(1) there is significant credible evidence that there has been a pattern of incidents of cybercrime, during the 2-year period preceding the date of the President's determination—

(A) against the United States Government or United States persons or that disrupt United States electronic commerce or otherwise negatively impact the trade or intellectual property interests of the United States; and

(B) that are attributable to persons or property based in the country; and

(2) the government of the country has demonstrated a pattern of being uncooperative with efforts to combat cybercrime by—

(A) failing to conduct its own reasonable criminal investigations, prosecutions, or other proceedings with respect to the incidents of cybercrime described in paragraph (1);

(B) failing to cooperate with the United States, any other party to the Convention on Cybercrime, or INTERPOL, in criminal investigations, prosecutions, or other proceedings with respect to such incidents, consistent with chapter III of the Convention on Cybercrime; or

(C) not adopting or implementing legislative or other measures consistent with chapter II of the Convention on Cybercrime with respect to criminal offenses related to computer systems or computer data.

(c) BENCHMARKS DESCRIBED.—The benchmarks described in this subsection—

(1) are such legislative, institutional, enforcement, or other actions as the President determines necessary to improve the capacity of the country to combat cybercrime; and

(2) may include—

(A) the initiation of credible criminal investigations, prosecutions, or other proceedings with respect to the incidents of cybercrime that resulted in the determination of the President under subsection (b) that the country is a country of cyber concern;

(B) cooperation with, or support for the efforts of, the United States, other parties to the Convention on Cybercrime, or INTERPOL in criminal investigations, prosecutions, or other proceedings with respect to such persons, consistent with chapter III of the Convention on Cybercrime; or

(C) the implementation of legislative or other measures consistent with chapter II of the Convention on Cybercrime with respect to criminal offenses related to computer systems or computer data.

(d) DETERMINATION OF CONSISTENCY WITH CONVENTION ON CYBERCRIME.—For purposes of subsections (b) and (c), a measure is not consistent with the Convention on Cybercrime if the measure imposes a criminal penalty for an activity that is not a criminal offense under the Convention.

(e) FAILURE TO MEET ACTION PLAN BENCHMARKS.—

(1) IN GENERAL.—If, 1 year after the date on which an action plan is developed under subsection (a), the President, in consultation with the entities described in section 3(c), determines that the government of the country for which the action plan was developed has not complied with the benchmarks in the action plan, the President is urged to take one or more of the actions described in paragraph (2) with respect to the country.

(2) PRESIDENTIAL ACTION DESCRIBED.—

(A) IN GENERAL.—Subject to subparagraph (B), the actions described in this para-

graph with respect to a country are the following:

(i) MULTILATERAL DEVELOPMENT BANK FINANCING.—Instruct the United States Executive Director of each multilateral development bank (as defined in section 1701(c)(4) of the International Financial Institutions Act (22 U.S.C. 262r(c)(4))) to restrict or oppose the approval of any new financing (including loans, guarantees, other credits, insurance, and reinsurance) by the multilateral development bank to the government of the country or with respect to a project located in the country or in which an entity owned or controlled by the government of the country participates.

(ii) PREFERENTIAL TRADE PROGRAMS.—Suspend, limit, or withdraw any preferential treatment for which the country qualifies under the Caribbean Basin Economic Recovery Act (19 U.S.C. 2701 et seq.), the African Growth and Opportunity Act (19 U.S.C. 3701 et seq.), or any other trade preference program in effect.

(iii) FOREIGN ASSISTANCE.—Suspend, restrict, or withdraw the provision of foreign assistance to the country or with respect to projects carried out in the country, including assistance provided under the Foreign Assistance Act of 1961 (22 U.S.C. 2151 et seq.).

(B) EXCEPTION.—The President may not suspend, restrict, prohibit, or withdraw assistance described in subparagraph (A)(iii) that is provided for humanitarian or disaster relief or for projects related to building capacity or actions to combat cybercrime.

(3) RESTORATION OF BENEFITS.—The President shall revoke any actions taken with respect to a country under paragraph (2) on the date on which the President, in consultation with the entities described in section 3(c), determines and certifies to Congress that the government of the country has complied with the benchmarks described in subsection (c).

(f) WAIVER.—

(1) IN GENERAL.—The President may waive the requirement under subsection (a) to develop an action plan for a country or the requirement under

subsection (b) to make a determination with respect to a country if the President—

(A) determines that such a waiver is in the national interest of the United States; and

(B) submits to Congress a report describing the reasons for the determination.

(2) FORM OF REPORT.—A report submitted under paragraph (1)(B) shall be submitted in unclassified form, but may contain a classified annex.

SEC. 6. DESIGNATION OF COORDINATOR FOR CYBERSECURITY ISSUES IN THE DEPARTMENT OF STATE.

The Secretary of State shall designate a high-level employee of the Department of State—

(1) to coordinate a full range of cybersecurity issues, including activities, policies, and opportunities of the Department of State associated with foreign policy and combating cybercrime; and

(2) whose primary responsibilities shall include increasing opportunities with respect to combating cybercrime at an international level.

SEC. 7. DESIGNATION OF OFFICIALS TO BE RESPONSIBLE FOR COMBATING CYBERCRIME.

The President shall ensure that—

(1) there is an employee of the United States Government with primary responsibility with respect

to matters relating to cybercrime policy in each country or region that the President considers significant with respect to the efforts of the United States Government to combat cybercrime globally; and

(2) each such employee consults with industry groups in the United States, civil society organizations, and other organizations with an interest in combating cybercrime in carrying out the employee's duties with respect to matters relating to cybercrime.

SEC. 8. CONSIDERATION OF CYBERCRIME IN TRADE AGREEMENT NEGOTIATIONS.

Before finalizing or modifying any trade agreement with another country, the President shall take into consideration the efforts of the government of that country to combat cybercrime.

○