111TH CONGRESS
2D SESSION

S. _____

To require reporting on certain information and communications technologies of foreign countries, 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

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

A BILL

To require reporting on certain information and communications technologies of foreign countries, 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.

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

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

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

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 President shall submit to Congress a report—

(1) assessing, with respect to each country that is a member state of the United Nations—

(A) the extent of the development and utilization of information and communications technologies in the critical infrastructure, telecommunications systems, and financial industry of the country;

(B) the extent and nature of activities relating to cybercrime that are based in the country;

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

(D) measures taken by the government of the country to ensure the free flow of electronic commerce and to protect consumers from cybercrime;

(2) identifying countries that are member states of the United Nations that the President determines have a low level of development or utilization of information and communications technologies in their

critical infrastructure, telecommunications systems, and financial industries;

(3) assessing any multilateral efforts—

(A) to prevent and investigate cybercrime;

(B) to develop and share best practices to directly or indirectly combat cybercrime; and

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

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

(b) 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 President 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 of the extent of the compliance of each such country with the action plan developed for that country.

(c) CONSULTATIONS.—It is the sense of Congress that the President should consult with the relevant Federal agencies, industry groups, civil society organizations,

and other interested parties in making the assessments required by paragraphs (1) through (3) of subsection (a) and subsection (b).

(d) 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 identified under section 3(a)(2) as having a low level of development or utilization of information and communications technologies in its critical infrastructure, telecommunications systems, and financial industry.

(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 extended to a country identified under section 3(a)(2) as having a low level of development or utilization of information and communications technologies in its critical infrastructure, telecommunications systems, and financial industry; 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 President submits the first report required by section 3(a), the President shall develop, for each country that the President determines under sub-

section (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 President 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 Secretary of State and, as appropriate, the employees of the Department of State described in section 6, 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 a pattern of incidents of cybercrime against the United States Government, private entities incorporated under the laws of the United States, or other United States persons has been carried out by persons within the country during the 2-year period preceding the date of the President's determination; 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) 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 relevant Federal agencies, 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 paragraph with respect to a country are the following:

(i) OVERSEAS PRIVATE INVESTMENT CORPORATION FINANCING.—Suspend, restrict, or prohibit the approval of new financing (including loans, guarantees, other credits, insurance, and reinsurance) by the Overseas Private Investment Corporation 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) EXPORT-IMPORT BANK FINANCING.—Suspend, restrict, or prohibit the approval of new financing (including loans, guarantees, other credits, insurance, and reinsurance) by the Export-Import Bank of the United States in connection with the export of any good or service to the country or to an entity owned or controlled by the government of the country.

(iii) MULTILATERAL DEVELOPMENT BANK FINANCING.—Instruct the United States Executive Director of each multilateral development bank (as defined in section 1307(g) of the International Financial Institutions Act (22 U.S.C. 262m–7(g))) to 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.

(iv) TRADE AND DEVELOPMENT AGENCY.—Suspend, restrict, or prohibit the provision of assistance by the Trade and Development Agency in connection with a project located in the country or in which an entity owned or controlled by the government of the country participates.

(v) PREFERENTIAL TRADE PROGRAMS.—Suspend, limit, or withdraw any preferential treatment for which the country qualifies under the Generalized System

of Preferences under title V of the Trade Act of 1974 (19 U.S.C. 2461 et seq.), the Caribbean Basin Economic Recovery Act (19 U.S.C. 2701 et seq.), the Andean Trade Preference Act (19 U.S.C. 3201 et seq.), or the African Growth and Opportunity Act (19 U.S.C. 3701 et seq.).

(vi) 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 clause (iv) or (vi) of subparagraph (A) that is provided for projects related to building capacity or taking 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 relevant Federal agencies, determines and certifies to Congress

that the government of the country has complied with the benchmarks described in subsection (c).

(e) 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 OFFICIALS IN THE DEPARTMENT OF STATE TO BE RESPONSIBLE FOR COMBATING CYBERCRIME.

The Secretary of State shall—

(1) designate a high-level employee of the Department of State—

(A) to coordinate the full range of activities, policies, and opportunities associated with combating cybercrime and foreign policy; and

(B) whose primary responsibility will be to further those activities, policies, and opportunities at an international level; and

(2) in consultation with the heads of other relevant Federal agencies and in coordination with the relevant chief of mission, assign an employee to have primary responsibility with respect to matters relating to cybercrime policy in each country or region that the Secretary considers significant with respect to efforts of the United States Government to combat cybercrime globally.

SEC. 7. AUTHORIZATION OF APPROPRIATIONS.

There are authorized to be appropriated such sums as may be necessary to carry out the provisions of this Act.