

111TH CONGRESS
2D SESSION

S. 3155

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

MARCH 23, 2010

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 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.

1 *Be it enacted by the Senate and House of Representa-*
2 *tives of the United States of America in Congress assembled,*

3 **SECTION 1. SHORT TITLE.**

4 This Act may be cited as the “International
5 Cybercrime Reporting and Cooperation Act”.

6 **SEC. 2. DEFINITIONS.**

7 In this Act:

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

5 (2) CONVENTION ON CYBERCRIME.—The term
6 “Convention on Cybercrime” means the Council of
7 Europe Convention on Cybercrime, done at Buda-
8 pest November 23, 2001.

9 (3) CYBERCRIME.—The term “cybercrime” re-
10 fers to criminal offenses relating to computer sys-
11 tems or computer data described in the Convention
12 on Cybercrime.

13 (4) INTERPOL.—The term “INTERPOL”
14 means the International Criminal Police Organiza-
15 tion.

16 (5) RELEVANT FEDERAL AGENCIES.—The term
17 “relevant Federal agencies” means any Federal
18 agency that has responsibility for combating
19 cybercrime globally, including the Department of
20 Justice, the Department of Homeland Security, the
21 Department of the Treasury, and the Department of
22 State.

1 **SEC. 3. ANNUAL REPORT.**

2 (a) IN GENERAL.—Not later than 1 year after the
3 date of the enactment of this Act, and annually thereafter,
4 the President shall submit to Congress a report—

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

7 (A) the extent of the development and uti-
8 lization of information and communications
9 technologies in the critical infrastructure, tele-
10 communications systems, and financial industry
11 of the country;

12 (B) the extent and nature of activities re-
13 lating to cybercrime that are based in the coun-
14 try;

15 (C) the adequacy and effectiveness of the
16 laws, regulations, and judicial and law enforce-
17 ment systems in the country with respect to
18 combating cybercrime; and

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

23 (2) identifying countries that are member states
24 of the United Nations that the President determines
25 have a low level of development or utilization of in-
26 formation and communications technologies in their

1 critical infrastructure, telecommunications systems,
2 and financial industries;

3 (3) assessing any multilateral efforts—

4 (A) to prevent and investigate cybercrime;

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

7 (C) to cooperate and take action with re-
8 spect to the prevention, investigation, and pros-
9 ecution of cybercrime; and

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

13 (b) ADDITIONAL INFORMATION TO BE INCLUDED IN
14 SUBSEQUENT REPORTS.—In each report required to be
15 submitted under subsection (a) after the first report re-
16 quired by that subsection, the President shall include, in
17 addition to the information required by that subsection—

18 (1) an identification of countries for which ac-
19 tion plans have been developed under section 5; and

20 (2) an assessment of the extent of the compli-
21 ance of each such country with the action plan devel-
22 oped for that country.

23 (c) CONSULTATIONS.—It is the sense of Congress
24 that the President should consult with the relevant Fed-
25 eral agencies, industry groups, civil society organizations,

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

4 (d) FORM OF REPORT.—The report required by sub-
5 section (a) shall be submitted in unclassified form, but
6 may contain a classified annex.

7 **SEC. 4. UTILIZATION OF FOREIGN ASSISTANCE PROGRAMS.**

8 (a) PRIORITY WITH RESPECT TO FOREIGN ASSIST-
9 ANCE PROGRAMS TO COMBAT CYBERCRIME.—

10 (1) IN GENERAL.—The President shall give pri-
11 ority to a country described in paragraph (2) with
12 respect to foreign assistance and other programs de-
13 signed to combat cybercrime in the country by im-
14 proving the effectiveness and capacity of the legal
15 and judicial systems and the capabilities of law en-
16 forcement agencies with respect to cybercrime.

17 (2) COUNTRIES DESCRIBED.—A country de-
18 scribed in this paragraph is a country identified
19 under section 3(a)(2) as having a low level of devel-
20 opment or utilization of information and communica-
21 tions technologies in its critical infrastructure, tele-
22 communications systems, and financial industry.

23 (b) SENSE OF CONGRESS WITH RESPECT TO BILAT-
24 ERAL AND MULTILATERAL ASSISTANCE.—It is the sense
25 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-

1 section (b) is a country of cyber concern, an action
2 plan—

3 (A) to assist the government of that coun-
4 try to improve the capacity of the country to
5 combat cybercrime; and

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

8 (2) REASSESSMENT OF COUNTRIES.—Not later
9 than 2 years after the President submits the first re-
10 port required by section 3(a), and annually there-
11 after, the President shall—

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

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

18 (C) determine if additional countries meet
19 the criteria under subsection (b) for being coun-
20 tries of cyber concern and develop action plans
21 for those countries.

22 (3) CONSULTATIONS.—The President, acting
23 through the Secretary of State and, as appropriate,
24 the employees of the Department of State described
25 in section 6, shall consult with the government of

1 each country for which the President develops an ac-
2 tion plan under paragraph (1) or (2) with respect
3 to—

4 (A) the development of the action plan;
5 and

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

9 (b) COUNTRIES OF CYBER CONCERN.—The Presi-
10 dent shall determine that a country is a country of cyber
11 concern if the President finds that—

12 (1) there is significant credible evidence that a
13 pattern of incidents of cybercrime against the
14 United States Government, private entities incor-
15 porated under the laws of the United States, or
16 other United States persons has been carried out by
17 persons within the country during the 2-year period
18 preceding the date of the President's determination;
19 and

20 (2) the government of the country has dem-
21 onstrated a pattern of being uncooperative with ef-
22 forts to combat cybercrime by—

23 (A) failing to conduct its own reasonable
24 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 inves-
tigations, prosecutions, or other proceedings
with respect to such incidents, consistent with
chapter III of the Convention on Cybercrime; or

(C) not adopting or implementing legisla-
tive or other measures consistent with chapter
II of the Convention on Cybercrime with re-
spect to criminal offenses related to computer
systems or computer data.

(c) BENCHMARKS DESCRIBED.—The benchmarks de-
scribed in this subsection—

(1) are such legislative, institutional, enforce-
ment, 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 inves-
tigations, prosecutions, or other proceedings
with respect to the incidents of cybercrime that
resulted in the determination of the President

1 under subsection (b) that the country is a coun-
2 try of cyber concern;

3 (B) cooperation with, or support for the ef-
4 forts of, the United States, other parties to the
5 Convention on Cybercrime, or INTERPOL in
6 criminal investigations, prosecutions, or other
7 proceedings with respect to such persons, con-
8 sistent with chapter III of the Convention on
9 Cybercrime; or

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

15 (d) FAILURE TO MEET ACTION PLAN BENCH-
16 MARKS.—

17 (1) IN GENERAL.—If, 1 year after the date on
18 which an action plan is developed under subsection
19 (a), the President, in consultation with the relevant
20 Federal agencies, determines that the government of
21 the country for which the action plan was developed
22 has not complied with the benchmarks in the action
23 plan, the President is urged to take one or more of
24 the actions described in paragraph (2) with respect
25 to the country.

1 (2) PRESIDENTIAL ACTION DESCRIBED.—

2 (A) IN GENERAL.—Subject to subpara-
3 graph (B), the actions described in this para-
4 graph with respect to a country are the fol-
5 lowing:

6 (i) OVERSEAS PRIVATE INVESTMENT
7 CORPORATION FINANCING.—Suspend, re-
8 strict, or prohibit the approval of new fi-
9 nancing (including loans, guarantees, other
10 credits, insurance, and reinsurance) by the
11 Overseas Private Investment Corporation
12 with respect to a project located in the
13 country or in which an entity owned or
14 controlled by the government of the coun-
15 try participates.

16 (ii) EXPORT-IMPORT BANK FINANC-
17 ING.—Suspend, restrict, or prohibit the ap-
18 proval of new financing (including loans,
19 guarantees, other credits, insurance, and
20 reinsurance) by the Export-Import Bank of
21 the United States in connection with the
22 export of any good or service to the coun-
23 try or to an entity owned or controlled by
24 the government of the country.

1 (iii) MULTILATERAL DEVELOPMENT
2 BANK FINANCING.—Instruct the United
3 States Executive Director of each multilat-
4 eral development bank (as defined in sec-
5 tion 1307(g) of the International Financial
6 Institutions Act (22 U.S.C. 262m–7(g)))
7 to oppose the approval of any new financ-
8 ing (including loans, guarantees, other
9 credits, insurance, and reinsurance) by the
10 multilateral development bank to the gov-
11 ernment of the country or with respect to
12 a project located in the country or in which
13 an entity owned or controlled by the gov-
14 ernment of the country participates.

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

22 (v) PREFERENTIAL TRADE PRO-
23 GRAMS.—Suspend, limit, or withdraw any
24 preferential treatment for which the coun-
25 try qualifies under the Generalized System

1 of Preferences under title V of the Trade
2 Act of 1974 (19 U.S.C. 2461 et seq.), the
3 Caribbean Basin Economic Recovery Act
4 (19 U.S.C. 2701 et seq.), the Andean
5 Trade Preference Act (19 U.S.C. 3201 et
6 seq.), or the African Growth and Oppor-
7 tunity Act (19 U.S.C. 3701 et seq.).

8 (vi) FOREIGN ASSISTANCE.—Suspend,
9 restrict, or withdraw the provision of for-
10 eign assistance to the country or with re-
11 spect to projects carried out in the coun-
12 try, including assistance provided under
13 the Foreign Assistance Act of 1961 (22
14 U.S.C. 2151 et seq.).

15 (B) EXCEPTION.—The President may not
16 suspend, restrict, prohibit, or withdraw assist-
17 ance described in clause (iv) or (vi) of subpara-
18 graph (A) that is provided for projects related
19 to building capacity or taking actions to combat
20 cybercrime.

21 (3) RESTORATION OF BENEFITS.—The Presi-
22 dent shall revoke any actions taken with respect to
23 a country under paragraph (2) on the date on which
24 the President, in consultation with the relevant Fed-
25 eral agencies, determines and certifies to Congress

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

3 (e) WAIVER.—

4 (1) IN GENERAL.—The President may waive
 5 the requirement under subsection (a) to develop an
 6 action plan for a country or the requirement under
 7 subsection (b) to make a determination with respect
 8 to a country if the President—

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

11 (B) submits to Congress a report describ-
 12 ing the reasons for the determination.

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

16 **SEC. 6. DESIGNATION OF OFFICIALS IN THE DEPARTMENT**
 17 **OF STATE TO BE RESPONSIBLE FOR COM-**
 18 **BATING CYBERCRIME.**

19 The Secretary of State shall—

20 (1) designate a high-level employee of the De-
 21 partment of State—

22 (A) to coordinate the full range of activi-
 23 ties, policies, and opportunities associated with
 24 combating cybercrime and foreign policy; and

1 (B) whose primary responsibility will be to
2 further those activities, policies, and opportuni-
3 ties at an international level; and

4 (2) in consultation with the heads of other rel-
5 evant Federal agencies and in coordination with the
6 relevant chief of mission, assign an employee to have
7 primary responsibility with respect to matters relat-
8 ing to cybercrime policy in each country or region
9 that the Secretary considers significant with respect
10 to efforts of the United States Government to com-
11 bat cybercrime globally.

12 **SEC. 7. AUTHORIZATION OF APPROPRIATIONS.**

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

○