

111TH CONGRESS
2D SESSION

S. _____

To establish within the office of the Secretary of State a Coordinator for
Cyberspace and Cybersecurity Issues.

IN THE SENATE OF THE UNITED STATES

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

A BILL

To establish within the office of the Secretary of State a
Coordinator for Cyberspace and Cybersecurity Issues.

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 Cyber-
5 space and Cybersecurity Coordination Act of 2010”.

6 **SEC. 2. FINDINGS.**

7 Congress makes the following findings:

8 (1) On February 2, 2010, Admiral Dennis C.
9 Blair, the Director of National Intelligence, testified
10 before the Select Committee on Intelligence of the

1 Senate regarding the Annual Threat Assessment of
2 the U.S. Intelligence Community, stating “The na-
3 tional security of the United States, our economic
4 prosperity, and the daily functioning of our govern-
5 ment are dependent on a dynamic public and private
6 information infrastructure, which includes tele-
7 communications, computer networks and systems,
8 and the information residing within. This critical in-
9 frastructure is severely threatened. ... We cannot
10 protect cyberspace without a coordinated and col-
11 laborative effort that incorporates both the US pri-
12 vate sector and our international partners.”.

13 (2) In a January 2010 speech on Internet free-
14 dom, Secretary of State Hillary Clinton stated:
15 “Those who disrupt the free flow of information in
16 our society, or any other, pose a threat to our econ-
17 omy, our government, and our civil society. Coun-
18 tries or individuals that engage in cyber attacks
19 should face consequences and international con-
20 demnation. In an Internet-connected world, an at-
21 tack on one nation’s networks can be an attack on
22 all. And by reinforcing that message, we can create
23 norms of behavior among states and encourage re-
24 spect for the global networked commons.”.

1 (3) James Lewis, senior fellow at the Center for
2 Strategic and International Studies asserts, in Se-
3 curing Cyberspace for the 44th Presidency, “The
4 international aspects of cybersecurity have been
5 among the least developed elements of U.S. cyberse-
6 curity policy. Given the multinational and global as-
7 pects of network security, this must be remedied, as
8 energetic engagement could produce real benefits in
9 promoting U.S. objectives and reducing risk.”.

10 (4) The 2010 National Broadband Plan of the
11 Federal Communications Commission recommends
12 that “[t]he Executive Branch should develop a co-
13 ordinated foreign cybersecurity assistance program
14 to assist foreign countries in the development of
15 legal and technical expertise to address cybersecu-
16 rity.”.

17 (5) The May 2009 White House Cyberspace
18 Policy Review asserts “[t]he Nation also needs a
19 strategy for cybersecurity designed to shape the
20 international environment and bring like-minded na-
21 tions together on a host of issues, such as technical
22 standards and acceptable legal norms regarding ter-
23 ritorial jurisdiction, sovereign responsibility, and use
24 of force. International norms are critical to estab-
25 lishing a secure and thriving digital infrastructure.”.

1 **SEC. 3. SENSE OF CONGRESS.**

2 It is the sense of Congress that—

3 (1) even as the United States and the global
4 system have become increasingly more dependent on
5 cyberspace for basic and critical functions and serv-
6 ices, a lack of sufficient norms and principles to gov-
7 ern the international cyberspace environment has re-
8 sulted in significant cyber vulnerabilities and the po-
9 tential for massive state failure in the event of co-
10 ordinated cyber attacks;

11 (2) the multilateral system has not—

12 (A) addressed these vulnerabilities in a
13 consistent or systematic manner; or

14 (B) established a basic framework of best
15 practices and governance to address and re-
16 spond to emerging cyber threats;

17 (3) the international community should strongly
18 consider the utility of negotiating a multilateral
19 framework on cyberwarfare that would create shared
20 norms for cyber conduct and head off the poten-
21 tiality for larger disruptions related to cyberwarfare;

22 (4) United States diplomatic engagement to-
23 wards international cybersecurity issues—

24 (A) has been uncoordinated and frag-
25 mented; and

1 (B) has not taken advantage of securing
2 cyberspace within a multilateral framework;

3 (5) the Secretary of State, in consultation with
4 other relevant Federal agencies, should develop and
5 establish a clear and coordinated strategy for inter-
6 national cyberspace and cybersecurity engagement,
7 which should—

8 (A) review and assess existing strategies
9 for international cyberspace and cybersecurity
10 policy and engagement;

11 (B) define short- and long-term objectives
12 for United States cyberspace and cybersecurity
13 policy;

14 (C) consider how to support a policy of
15 United States Government collaboration and co-
16 ordination with other countries and organiza-
17 tions in order to bolster an international frame-
18 work of cyber norms, governance, and deter-
19 rence;

20 (D) consider the utility of negotiating a
21 multilateral framework that would provide
22 internationally acceptable principles to better
23 mitigate cyberwarfare, including noncombat-
24 ants;

1 (E) share and disseminate relevant threat
2 information with key stakeholders;

3 (F) be developed in consultation with other
4 United States Government agencies with rel-
5 evant technical expertise or policy mandates
6 pertaining to cyberspace and cybersecurity
7 issues; and

8 (G) draw upon the expertise of technology,
9 security, and policy experts, private sector ac-
10 tors, international organizations, and other ap-
11 propriate entities.

12 **SEC. 4. COORDINATOR FOR CYBERSPACE AND CYBERSECU-**
13 **RITY ISSUES.**

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

16 (1) in subsection (e), by striking “in this para-
17 graph referred to” and inserting “referred to in this
18 subsection”

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

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

23 “(g) CYBERSPACE AND CYBERSECURITY ISSUES.—

24 “(1) IN GENERAL.—There is established within
25 the office of the Secretary of State a Coordinator for

1 Cyberspace and Cybersecurity Issues (referred to in
2 this subsection as the ‘Coordinator’), who shall be
3 appointed by the President, by and with the advice
4 and consent of the Senate.

5 “(2) DUTIES.—

6 “(A) PRINCIPAL DUTIES.—The Coordi-
7 nator shall—

8 “(i) be the principal official within the
9 senior management of the Department of
10 State responsible for cyberspace and cyber-
11 security issues;

12 “(ii) be the principal advisor to the
13 Secretary of State on international cyber-
14 space and cybersecurity issues;

15 “(iii) report directly to the Secretary
16 of State; and

17 “(iv) perform such duties and exercise
18 such powers as the Secretary of State shall
19 prescribe.

20 “(B) ADDITIONAL DUTIES.—In addition to
21 the duties described in subparagraph (A), the
22 Coordinator shall—

23 “(i) provide strategic direction and co-
24 ordination for United States Government
25 policy and programs aimed at addressing

1 and responding to cyberspace and cyberse-
2 curity issues overseas, especially in relation
3 to issues that affect United States foreign
4 policy and related national security con-
5 cerns;

6 “(ii) coordinate with relevant Federal
7 departments and agencies, including the
8 Department of Homeland Security, the De-
9 partment of Defense, the Department of
10 the Treasury, the Department of Justice,
11 the Department of Commerce, and the in-
12 telligence community to develop inter-
13 agency plans regarding international cyber-
14 space and cybersecurity issues;

15 “(iii) provide a focal point for the pri-
16 vate sector to coordinate on international
17 cyberspace and cybersecurity issues; and

18 “(iv) build multilateral cooperation to
19 develop international norms, common poli-
20 cies, and responses to secure the integrity
21 of cyberspace.

22 “(3) RANK AND STATUS OF AMBASSADOR.—

23 The Coordinator shall have the rank and status of
24 Ambassador at Large.

1 “(4) COUNTRY AND REGIONAL CYBERSPACE
2 AND CYBERSECURITY POLICY COORDINATORS.—The
3 Secretary of State, in consultation with the heads of
4 other relevant Federal agencies and in coordination
5 with the relevant Chief of Mission, should designate
6 an employee to have primary responsibility for mat-
7 ters relating to cyberspace and cybersecurity policy
8 in each country or region that the Secretary con-
9 siders significant with respect to efforts of the
10 United States Government to combat cybersecurity
11 globally.”.

12 **SEC. 5. AUTHORIZATION OF APPROPRIATIONS.**

13 There are authorized to be appropriated such sums
14 as may be necessary to carry out this Act and the amend-
15 ments made by this Act.