

111TH CONGRESS
1ST SESSION

S. 773

To ensure the continued free flow of commerce within the United States and with its global trading partners through secure cyber communications, to provide for the continued development and exploitation of the Internet and intranet communications for such purposes, to provide for the development of a cadre of information technology specialists to improve and maintain effective cyber security defenses against disruption, and for other purposes.

IN THE SENATE OF THE UNITED STATES

APRIL 1, 2009

Mr. ROCKEFELLER (for himself, Ms. SNOWE, and Mr. NELSON of Florida) introduced the following bill; which was read twice and referred to the Committee on Commerce, Science, and Transportation

A BILL

To ensure the continued free flow of commerce within the United States and with its global trading partners through secure cyber communications, to provide for the continued development and exploitation of the Internet and intranet communications for such purposes, to provide for the development of a cadre of information technology specialists to improve and maintain effective cybersecurity defenses against disruption, 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,*

1 **SECTION 1. SHORT TITLE; TABLE OF CONTENTS.**

2 (a) SHORT TITLE.—This Act may be cited as the
3 “Cybersecurity Act of 2009”.

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

- Sec. 1. Short title; table of contents.
- Sec. 2. Findings.
- Sec. 3. Cybersecurity Advisory Panel.
- Sec. 4. Real-time cybersecurity dashboard.
- Sec. 5. State and regional cybersecurity enhancement program.
- Sec. 6. NIST standards development and compliance.
- Sec. 7. Licensing and certification of cybersecurity professionals.
- Sec. 8. Review of NTIA domain name contracts.
- Sec. 9. Secure domain name addressing system.
- Sec. 10. Promoting cybersecurity awareness.
- Sec. 11. Federal cybersecurity research and development.
- Sec. 12. Federal Cyber Scholarship-for-Service program.
- Sec. 13. Cybersecurity competition and challenge.
- Sec. 14. Public–private clearinghouse.
- Sec. 15. Cybersecurity risk management report.
- Sec. 16. Legal framework review and report.
- Sec. 17. Authentication and civil liberties report.
- Sec. 18. Cybersecurity responsibilities and authorities.
- Sec. 19. Quadrennial cyber review.
- Sec. 20. Joint intelligence threat assessment.
- Sec. 21. International norms and cybersecurity deterrence measures.
- Sec. 22. Federal Secure Products and Services Acquisitions Board.
- Sec. 23. Definitions.

6 **SEC. 2. FINDINGS.**

7 The Congress finds the following:

8 (1) America’s failure to protect cyberspace is
9 one of the most urgent national security problems
10 facing the country.

11 (2) Since intellectual property is now often
12 stored in digital form, industrial espionage that ex-
13 ploits weak cybersecurity dilutes our investment in
14 innovation while subsidizing the research and devel-
15 opment efforts of foreign competitors. In the new

1 global competition, where economic strength and
2 technological leadership are vital components of na-
3 tional power, failing to secure cyberspace puts us at
4 a disadvantage.

5 (3) According to the 2009 Annual Threat As-
6 sessment, “a successful cyber attack against a major
7 financial service provider could severely impact the
8 national economy, while cyber attacks against phys-
9 ical infrastructure computer systems such as those
10 that control power grids or oil refineries have the po-
11 tential to disrupt services for hours or weeks” and
12 that “Nation states and criminals target our govern-
13 ment and private sector information networks to
14 gain competitive advantage in the commercial sec-
15 tor.”.

16 (4) The Director of National Intelligence testi-
17 fied before the Congress on February 19, 2009, that
18 “a growing array of state and non-state adversaries
19 are increasingly targeting-for exploitation and poten-
20 tially disruption or destruction-our information in-
21 frastructure, including the Internet, telecommuni-
22 cations networks, computer systems, and embedded
23 processors and controllers in critical industries” and
24 these trends are likely to continue.

1 (5) John Brennan, the Assistant to the Presi-
2 dent for Homeland Security and Counterterrorism
3 wrote on March 2, 2009, that “our nation’s security
4 and economic prosperity depend on the security, sta-
5 bility, and integrity of communications and informa-
6 tion infrastructure that are largely privately-owned
7 and globally-operated.”.

8 (6) Paul Kurtz, a Partner and chief operating
9 officer of Good Harbor Consulting as well as a sen-
10 ior advisor to the Obama Transition Team for cyber-
11 security, recently stated that the United States is
12 unprepared to respond to a “cyber-Katrina” and
13 that “a massive cyber disruption could have a cas-
14 cading, long-term impact without adequate co-ordi-
15 nation between government and the private sector.”.

16 (7) The Cyber Strategic Inquiry 2008, spon-
17 sored by Business Executives for National Security
18 and executed by Booz Allen Hamilton, recommended
19 to “establish a single voice for cybersecurity within
20 government” concluding that the “unique nature of
21 cybersecurity requires a new leadership paradigm.”.

22 (8) Alan Paller, the Director of Research at the
23 SANS Institute, testified before the Congress that
24 “the fight against cybercrime resembles an arms
25 race where each time the defenders build a new wall,

1 the attackers create new tools to scale the wall.
2 What is particularly important in this analogy is
3 that, unlike conventional warfare where deployment
4 takes time and money and is quite visible, in the
5 cyber world, when the attackers find a new weapon,
6 they can attack millions of computers, and success-
7 fully infect hundreds of thousands, in a few hours or
8 days, and remain completely hidden.”.

9 (9) According to the February 2003 National
10 Strategy to Secure Cyberspace, “our nation’s critical
11 infrastructures are composed of public and private
12 institutions in the sectors of agriculture, food, water,
13 public health, emergency services, government, de-
14 fense industrial base, information and telecommuni-
15 cations, energy, transportation, banking finance,
16 chemicals and hazardous materials, and postal and
17 shipping. Cyberspace is their nervous system—the
18 control system of our country” and that “the corner-
19 stone of America’s cyberspace security strategy is
20 and will remain a public-private partnership.”.

21 (10) According to the National Journal, Mike
22 McConnell, the former Director of National Intel-
23 ligence, told President Bush in May 2007 that if the
24 9/11 attackers had chosen computers instead of air-
25 planes as their weapons and had waged a massive

1 assault on a U.S. bank, the economic consequences
2 would have been “an order of magnitude greater”
3 than those caused by the physical attack on the
4 World Trade Center. Mike McConnell has subse-
5 quently referred to cybersecurity as the “soft under-
6 belly of this country.”.

7 (11) The Center for Strategic and International
8 Studies report on Cybersecurity for the 44th Presi-
9 dency concluded that (A) cybersecurity is now a
10 major national security problem for the United
11 States, (B) decisions and actions must respect pri-
12 vacy and civil liberties, and (C) only a comprehen-
13 sive national security strategy that embraces both
14 the domestic and international aspects of cybersecu-
15 rity will make us more secure. The report continued
16 stating that the United States faces “a long-term
17 challenge in cyberspace from foreign intelligence
18 agencies and militaries, criminals, and others, and
19 that losing this struggle will wreak serious damage
20 on the economic health and national security of the
21 United States.”.

22 (12) James Lewis, Director and Senior Fellow,
23 Technology and Public Policy Program, Center for
24 Strategic and International Studies, testified on be-
25 half of the Center for Strategic and International

1 Studies that “the United States is not organized and
2 lacks a coherent national strategy for addressing”
3 cybersecurity.

4 (13) President Obama said in a speech at Pur-
5 due University on July 16, 2008, that “every Amer-
6 ican depends—directly or indirectly—on our system
7 of information networks. They are increasingly the
8 backbone of our economy and our infrastructure; our
9 national security and our personal well-being. But
10 it’s no secret that terrorists could use our computer
11 networks to deal us a crippling blow. We know that
12 cyber-espionage and common crime is already on the
13 rise. And yet while countries like China have been
14 quick to recognize this change, for the last eight
15 years we have been dragging our feet.” Moreover,
16 President Obama stated that “we need to build the
17 capacity to identify, isolate, and respond to any
18 cyber-attack.”.

19 (14) The President’s Information Technology
20 Advisory Committee reported in 2005 that software
21 is a major vulnerability and that “software develop-
22 ment methods that have been the norm fail to pro-
23 vide the high-quality, reliable, and secure software
24 that the IT infrastructure requires. . . . Today, as
25 with cancer, vulnerable software can be invaded and

1 modified to cause damage to previously healthy soft-
2 ware, and infected software can replicate itself and
3 be carried across networks to cause damage in other
4 systems.”.

5 **SEC. 3. CYBERSECURITY ADVISORY PANEL.**

6 (a) IN GENERAL.—The President shall establish or
7 designate a Cybersecurity Advisory Panel.

8 (b) QUALIFICATIONS.—The President—

9 (1) shall appoint as members of the panel rep-
10 resentatives of industry, academic, non-profit organi-
11 zations, interest groups and advocacy organizations,
12 and State and local governments who are qualified
13 to provide advice and information on cybersecurity
14 research, development, demonstrations, education,
15 technology transfer, commercial application, or soci-
16 etal and civil liberty concerns; and

17 (2) may seek and give consideration to rec-
18 ommendations from the Congress, industry, the cy-
19 bersecurity community, the defense community,
20 State and local governments, and other appropriate
21 organizations.

22 (c) DUTIES.—The panel shall advise the President on
23 matters relating to the national cybersecurity program
24 and strategy and shall assess—

1 (1) trends and developments in cybersecurity
2 science research and development;

3 (2) progress made in implementing the strat-
4 egy;

5 (3) the need to revise the strategy;

6 (4) the balance among the components of the
7 national strategy, including funding for program
8 components;

9 (5) whether the strategy, priorities, and goals
10 are helping to maintain United States leadership
11 and defense in cybersecurity;

12 (6) the management, coordination, implementa-
13 tion, and activities of the strategy; and

14 (7) whether societal and civil liberty concerns
15 are adequately addressed.

16 (d) REPORTS.—The panel shall report, not less fre-
17 quently than once every 2 years, to the President on its
18 assessments under subsection (c) and its recommendations
19 for ways to improve the strategy.

20 (e) TRAVEL EXPENSES OF NON-FEDERAL MEM-
21 BERS.—Non-Federal members of the panel, while attend-
22 ing meetings of the panel or while otherwise serving at
23 the request of the head of the panel while away from their
24 homes or regular places of business, may be allowed travel
25 expenses, including per diem in lieu of subsistence, as au-

1 thorized by section 5703 of title 5, United States Code,
2 for individuals in the government serving without pay.
3 Nothing in this subsection shall be construed to prohibit
4 members of the panel who are officers or employees of the
5 United States from being allowed travel expenses, includ-
6 ing per diem in lieu of subsistence, in accordance with law.

7 (f) EXEMPTION FROM FACA SUNSET.—Section 14
8 of the Federal Advisory Committee Act (5 U.S.C. App.)
9 shall not apply to the Advisory Panel.

10 **SEC. 4. REAL-TIME CYBERSECURITY DASHBOARD.**

11 The Secretary of Commerce shall—

12 (1) in consultation with the Office of Manage-
13 ment and Budget, develop a plan within 90 days
14 after the date of enactment of this Act to implement
15 a system to provide dynamic, comprehensive, real-
16 time cybersecurity status and vulnerability informa-
17 tion of all Federal Government information systems
18 and networks managed by the Department of Com-
19 merce; and

20 (2) implement the plan within 1 year after the
21 date of enactment of this Act.

22 **SEC. 5. STATE AND REGIONAL CYBERSECURITY ENHANCE-**
23 **MENT PROGRAM.**

24 (a) CREATION AND SUPPORT OF CYBERSECURITY
25 CENTERS.—The Secretary of Commerce shall provide as-

1 sistance for the creation and support of Regional Cyberse-
2 curity Centers for the promotion and implementation of
3 cybersecurity standards. Each Center shall be affiliated
4 with a United States-based nonprofit institution or organi-
5 zation, or consortium thereof, that applies for and is
6 awarded financial assistance under this section.

7 (b) PURPOSE.—The purpose of the Centers is to en-
8 hance the cybersecurity of small and medium sized busi-
9 nesses in United States through—

10 (1) the transfer of cybersecurity standards,
11 processes, technology, and techniques developed at
12 the National Institute of Standards and Technology
13 to Centers and, through them, to small- and me-
14 dium-sized companies throughout the United States;

15 (2) the participation of individuals from indus-
16 try, universities, State governments, other Federal
17 agencies, and, when appropriate, the Institute in co-
18 operative technology transfer activities;

19 (3) efforts to make new cybersecurity tech-
20 nology, standards, and processes usable by United
21 States-based small- and medium-sized companies;

22 (4) the active dissemination of scientific, engi-
23 neering, technical, and management information
24 about cybersecurity to industrial firms, including
25 small- and medium-sized companies; and

1 (5) the utilization, when appropriate, of the ex-
2 pertise and capability that exists in Federal labora-
3 tories other than the Institute.

4 (c) ACTIVITIES.—The Centers shall—

5 (1) disseminate cybersecurity technologies,
6 standard, and processes based on research by the In-
7 stitute for the purpose of demonstrations and tech-
8 nology transfer;

9 (2) actively transfer and disseminate cybersecu-
10 rity strategies, best practices, standards, and tech-
11 nologies to protect against and mitigate the risk of
12 cyber attacks to a wide range of companies and en-
13 terprises, particularly small- and medium-sized busi-
14 nesses; and

15 (3) make loans, on a selective, short-term basis,
16 of items of advanced cybersecurity countermeasures
17 to small businesses with less than 100 employees.

18 (c) DURATION AND AMOUNT OF SUPPORT; PROGRAM
19 DESCRIPTIONS; APPLICATIONS; MERIT REVIEW; EVALUA-
20 TIONS OF ASSISTANCE.—

21 (1) FINANCIAL SUPPORT.—The Secretary may
22 provide financial support, not to exceed 50 percent
23 of its annual operating and maintenance costs, to
24 any Center for a period not to exceed 6 years (ex-
25 cept as provided in paragraph (5)(D)).

1 (2) PROGRAM DESCRIPTION.—Within 90 days
2 after the date of enactment of this Act, the Sec-
3 retary shall publish in the Federal Register a draft
4 description of a program for establishing Centers
5 and, after a 30-day comment period, shall publish a
6 final description of the program. The description
7 shall include—

8 (A) a description of the program;

9 (B) procedures to be followed by appli-
10 cants;

11 (C) criteria for determining qualified appli-
12 cants;

13 (D) criteria, including those described in
14 paragraph (4), for choosing recipients of finan-
15 cial assistance under this section from among
16 the qualified applicants; and

17 (E) maximum support levels expected to be
18 available to Centers under the program in the
19 fourth through sixth years of assistance under
20 this section.

21 (3) APPLICATIONS; SUPPORT COMMITMENT.—

22 Any nonprofit institution, or consortia of nonprofit
23 institutions, may submit to the Secretary an applica-
24 tion for financial support under this section, in ac-
25 cordance with the procedures established by the Sec-

1 retary. In order to receive assistance under this sec-
2 tion, an applicant shall provide adequate assurances
3 that it will contribute 50 percent or more of the pro-
4 posed Center's annual operating and maintenance
5 costs for the first 3 years and an increasing share
6 for each of the next 3 years.

7 (4) AWARD CRITERIA.—Awards shall be made
8 on a competitive, merit-based review. In making a
9 decision whether to approve an application and pro-
10 vide financial support under this section, the Sec-
11 retary shall consider, at a minimum—

12 (A) the merits of the application, particu-
13 larly those portions of the application regarding
14 technology transfer, training and education, and
15 adaptation of cybersecurity technologies to the
16 needs of particular industrial sectors;

17 (B) the quality of service to be provided;

18 (C) geographical diversity and extent of
19 service area; and

20 (D) the percentage of funding and amount
21 of in-kind commitment from other sources.

22 (5) THIRD YEAR EVALUATION.—

23 (A) IN GENERAL.—Each Center which re-
24 ceives financial assistance under this section
25 shall be evaluated during its third year of oper-

1 ation by an evaluation panel appointed by the
2 Secretary.

3 (B) EVALUATION PANEL.—Each evalua-
4 tion panel shall be composed of private experts,
5 none of whom shall be connected with the in-
6 volved Center, and Federal officials. An official
7 of the Institute shall chair the panel. Each eval-
8 uation panel shall measure the Center’s per-
9 formance against the objectives specified in this
10 section.

11 (C) POSITIVE EVALUATION REQUIRED FOR
12 CONTINUED FUNDING.—The Secretary may not
13 provide funding for the fourth through the sixth
14 years of a Center’s operation unless the evalua-
15 tion by the evaluation panel is positive. If the
16 evaluation is positive, the Secretary may pro-
17 vide continued funding through the sixth year
18 at declining levels.

19 (D) FUNDING AFTER SIXTH YEAR.—After
20 the sixth year, the Secretary may provide addi-
21 tional financial support to a Center if it has re-
22 ceived a positive evaluation through an inde-
23 pendent review, under procedures established by
24 the Institute. An additional independent review
25 shall be required at least every 2 years after the

1 sixth year of operation. Funding received for a
2 fiscal year under this section after the sixth
3 year of operation may not exceed one third of
4 the annual operating and maintenance costs of
5 the Center.

6 (6) PATENT RIGHTS TO INVENTIONS.—The pro-
7 visions of chapter 18 of title 35, United States Code,
8 shall (to the extent not inconsistent with this sec-
9 tion) apply to the promotion of technology from re-
10 search by Centers under this section except for con-
11 tracts for such specific technology extension or
12 transfer services as may be specified by statute or
13 by the President, or the President’s designee.

14 (d) ACCEPTANCE OF FUNDS FROM OTHER FEDERAL
15 DEPARTMENTS AND AGENCIES.—In addition to such
16 sums as may be authorized and appropriated to the Sec-
17 retary and President, or the President’s designee, to oper-
18 ate the Centers program, the Secretary and the President,
19 or the President’s designee, also may accept funds from
20 other Federal departments and agencies for the purpose
21 of providing Federal funds to support Centers. Any Center
22 which is supported with funds which originally came from
23 other Federal departments and agencies shall be selected
24 and operated according to the provisions of this section.

1 **SEC. 6. NIST STANDARDS DEVELOPMENT AND COMPLI-**
2 **ANCE.**

3 (a) IN GENERAL.—Within 1 year after the date of
4 enactment of this Act, the National Institute of Standards
5 and Technology shall establish measurable and auditable
6 cybersecurity standards for all Federal Government, gov-
7 ernment contractor, or grantee critical infrastructure in-
8 formation systems and networks in the following areas:

9 (1) CYBERSECURITY METRICS RESEARCH.—The
10 Director of the National Institute of Standards and
11 Technology shall establish a research program to de-
12 velop cybersecurity metrics and benchmarks that can
13 assess the economic impact of cybersecurity. These
14 metrics should measure risk reduction and the cost
15 of defense. The research shall include the develop-
16 ment automated tools to assess vulnerability and
17 compliance.

18 (2) SECURITY CONTROLS.—The Institute shall
19 establish standards for continuously measuring the
20 effectiveness of a prioritized set of security controls
21 that are known to block or mitigate known attacks.

22 (3) SOFTWARE SECURITY.—The Institute shall
23 establish standards for measuring the software secu-
24 rity using a prioritized list of software weaknesses
25 known to lead to exploited and exploitable
26 vulnerabilities. The Institute will also establish a

1 separate set of such standards for measuring secu-
2 rity in embedded software such as that found in in-
3 dustrial control systems.

4 (4) SOFTWARE CONFIGURATION SPECIFICATION
5 LANGUAGE.—The Institute shall, establish standard
6 computer-readable language for completely speci-
7 fying the configuration of software on computer sys-
8 tems widely used in the Federal Government, by
9 government contractors and grantees, and in private
10 sector owned critical infrastructure information sys-
11 tems and networks.

12 (5) STANDARD SOFTWARE CONFIGURATION.—
13 The Institute shall establish standard configurations
14 consisting of security settings for operating system
15 software and software utilities widely used in the
16 Federal Government, by government contractors and
17 grantees, and in private sector owned critical infra-
18 structure information systems and networks.

19 (6) VULNERABILITY SPECIFICATION LAN-
20 GUAGE.—The Institute shall establish standard com-
21 puter-readable language for specifying vulnerabilities
22 in software to enable software vendors to commu-
23 nicate vulnerability data to software users in real
24 time.

1 (7) NATIONAL COMPLIANCE STANDARDS FOR
2 ALL SOFTWARE.—

3 (A) PROTOCOL.—The Institute shall estab-
4 lish a standard testing and accreditation pro-
5 tocol for software built by or for the Federal
6 Government, its contractors, and grantees, and
7 private sector owned critical infrastructure in-
8 formation systems and networks. to ensure that
9 it—

10 (i) meets the software security stand-
11 ards of paragraph (2); and

12 (ii) does not require or cause any
13 changes to be made in the standard con-
14 figurations described in paragraph (4).

15 (B) COMPLIANCE.—The Institute shall de-
16 velop a process or procedure to verify that—

17 (i) software development organizations
18 comply with the protocol established under
19 subparagraph (A) during the software de-
20 velopment process; and

21 (ii) testing results showing evidence of
22 adequate testing and defect reduction are
23 provided to the Federal Government prior
24 to deployment of software.

1 (b) CRITERIA FOR STANDARDS.—Notwithstanding
2 any other provision of law (including any Executive
3 Order), rule, regulation, or guideline, in establishing
4 standards under this section, the Institute shall disregard
5 the designation of an information system or network as
6 a national security system or on the basis of presence of
7 classified or confidential information, and shall establish
8 standards based on risk profiles.

9 (c) INTERNATIONAL STANDARDS.—The Director,
10 through the Institute and in coordination with appropriate
11 Federal agencies, shall be responsible for United States
12 representation in all international standards development
13 related to cybersecurity, and shall develop and implement
14 a strategy to optimize the United States position with re-
15 spect to international cybersecurity standards.

16 (d) COMPLIANCE ENFORCEMENT.—The Director
17 shall—

18 (1) enforce compliance with the standards de-
19 veloped by the Institute under this section by soft-
20 ware manufacturers, distributors, and vendors; and

21 (2) shall require each Federal agency, and each
22 operator of an information system or network des-
23 igned by the President as a critical infrastructure
24 information system or network, periodically to dem-

1 ture information system or network, who is not licensed
2 and certified under the program.

3 **SEC. 8. REVIEW OF NTIA DOMAIN NAME CONTRACTS.**

4 (a) IN GENERAL.—No action by the Assistant Sec-
5 retary of Commerce for Communications and Information
6 after the date of enactment of this Act with respect to
7 the renewal or modification of a contract related to the
8 operation of the Internet Assigned Numbers Authority,
9 shall be final until the Advisory Panel—

10 (1) has reviewed the action;

11 (2) considered the commercial and national se-
12 curity implications of the action; and

13 (3) approved the action.

14 (b) APPROVAL PROCEDURE.—If the Advisory Panel
15 does not approve such an action, it shall immediately no-
16 tify the Assistant Secretary in writing of the disapproval
17 and the reasons therefor. The Advisory Panel may provide
18 recommendations to the Assistant Secretary in the notice
19 for any modifications the it deems necessary to secure ap-
20 proval of the action.

21 **SEC. 9. SECURE DOMAIN NAME ADDRESSING SYSTEM.**

22 (a) IN GENERAL.—Within 3 years after the date of
23 enactment of this Act, the Assistant Secretary of Com-
24 merce for Communications and Information shall develop
25 a strategy to implement a secure domain name addressing

1 system. The Assistant Secretary shall publish notice of the
2 system requirements in the Federal Register together with
3 an implementation schedule for Federal agencies and in-
4 formation systems or networks designated by the Presi-
5 dent, or the President's designee, as critical infrastructure
6 information systems or networks.

7 (b) COMPLIANCE REQUIRED.—The President shall
8 ensure that each Federal agency and each such system
9 or network implements the secure domain name address-
10 ing system in accordance with the schedule published by
11 the Assistant Secretary.

12 **SEC. 10. PROMOTING CYBERSECURITY AWARENESS.**

13 The Secretary of Commerce shall develop and imple-
14 ment a national cybersecurity awareness campaign that—

15 (1) is designed to heighten public awareness of
16 cybersecurity issues and concerns;

17 (2) communicates the Federal Government's
18 role in securing the Internet and protecting privacy
19 and civil liberties with respect to Internet-related ac-
20 tivities; and

21 (3) utilizes public and private sector means of
22 providing information to the public, including public
23 service announcements.

1 **SEC. 11. FEDERAL CYBERSECURITY RESEARCH AND DE-**
2 **VELOPMENT.**

3 (a) **FUNDAMENTAL CYBERSECURITY RESEARCH.—**

4 The Director of the National Science Foundation shall
5 give priority to computer and information science and en-
6 gineering research to ensure substantial support is pro-
7 vided to meet the following challenges in cybersecurity:

8 (1) How to design and build complex software-
9 intensive systems that are secure and reliable when
10 first deployed.

11 (2) How to test and verify that software,
12 whether developed locally or obtained from a third
13 party, is free of significant known security flaws.

14 (3) How to test and verify that software ob-
15 tained from a third party correctly implements stat-
16 ed functionality, and only that functionality.

17 (4) How to guarantee the privacy of an individ-
18 ual's identity, information, or lawful transactions
19 when stored in distributed systems or transmitted
20 over networks.

21 (5) How to build new protocols to enable the
22 Internet to have robust security as one of its key ca-
23 pabilities.

24 (6) How to determine the origin of a message
25 transmitted over the Internet.

1 (7) How to support privacy in conjunction with
2 improved security.

3 (8) How to address the growing problem of in-
4 sider threat.

5 (b) SECURE CODING RESEARCH.—The Director shall
6 support research that evaluates selected secure coding
7 education and improvement programs. The Director shall
8 also support research on new methods of integrating se-
9 cure coding improvement into the core curriculum of com-
10 puter science programs and of other programs where grad-
11 uates have a substantial probability of developing software
12 after graduation.

13 (c) ASSESSMENT OF SECURE CODING EDUCATION IN
14 COLLEGES AND UNIVERSITIES.—Within one year after
15 the date of enactment of this Act, the Director shall sub-
16 mit to the Senate Committee on Commerce, Science, and
17 Transportation and the House of Representatives Com-
18 mittee on Science and Technology a report on the state
19 of secure coding education in America’s colleges and uni-
20 versities for each school that received National Science
21 Foundation funding in excess of \$1,000,000 during fiscal
22 year 2008. The report shall include—

23 (1) the number of students who earned under-
24 graduate degrees in computer science or in each
25 other program where graduates have a substantial

1 probability of being engaged in software design or
2 development after graduation;

3 (2) the percentage of those students who com-
4 pleted substantive secure coding education or im-
5 provement programs during their undergraduate ex-
6 perience; and

7 (3) descriptions of the length and content of the
8 education and improvement programs, and a meas-
9 ure of the effectiveness of those programs in ena-
10 bling the students to master secure coding and de-
11 sign.

12 (d) CYBERSECURITY MODELING AND TESTBEDS.—
13 The Director shall establish a program to award grants
14 to institutions of higher education to establish cybersecu-
15 rity testbeds capable of realistic modeling of real-time
16 cyber attacks and defenses. The purpose of this program
17 is to support the rapid development of new cybersecurity
18 defenses, techniques, and processes by improving under-
19 standing and assessing the latest technologies in a real-
20 world environment. The testbeds shall be sufficiently large
21 in order to model the scale and complexity of real world
22 networks and environments.

23 (e) NSF COMPUTER AND NETWORK SECURITY RE-
24 SEARCH GRANT AREAS.—Section 4(a)(1) of the Cyberse-

1 curity Research and Development Act (15 U.S.C.
2 7403(a)(1)) is amended—

3 (1) by striking “and” after the semicolon in
4 subparagraph (H);

5 (2) by striking “property.” in subparagraph (I)
6 and inserting “property;”; and

7 (3) by adding at the end the following:

8 “(J) secure fundamental protocols that are at
9 the heart of inter-network communications and data
10 exchange;

11 “(K) secure software engineering and software
12 assurance, including—

13 “(i) programming languages and systems
14 that include fundamental security features;

15 “(ii) portable or reusable code that re-
16 mains secure when deployed in various environ-
17 ments;

18 “(iii) verification and validation tech-
19 nologies to ensure that requirements and speci-
20 fications have been implemented; and

21 “(iv) models for comparison and metrics to
22 assure that required standards have been met;

23 “(L) holistic system security that—

24 “(i) addresses the building of secure sys-
25 tems from trusted and untrusted components;

1 “(ii) proactively reduces vulnerabilities;
 2 “(iii) addresses insider threats; and
 3 “(iv) supports privacy in conjunction with
 4 improved security;
 5 “(M) monitoring and detection; and
 6 “(N) mitigation and rapid recovery methods.”.

7 (f) NSF COMPUTER AND NETWORK SECURITY
 8 GRANTS.—Section 4(a)(3) of the Cybersecurity Research
 9 and Development Act (15 U.S.C. 7403(a)(3)) is amend-
 10 ed—

11 (1) by striking “and” in subparagraph (D);
 12 (2) by striking “2007” in subparagraph (E)
 13 and inserting “2007;”; and
 14 (3) by adding at the end of the following:

15 “(F) \$150,000,000 for fiscal year 2010;
 16 “(G) \$155,000,000 for fiscal year 2011;
 17 “(H) \$160,000,000 for fiscal year 2012;
 18 “(I) \$165,000,000 for fiscal year 2013;
 19 and
 20 “(J) \$170,000,000 for fiscal year 2014.”.

21 (g) COMPUTER AND NETWORK SECURITY CEN-
 22 TERS.—Section 4(b)(7) of such Act (15 U.S.C.
 23 7403(b)(7)) is amended—

24 (1) by striking “and” in subparagraph (D);

1 (2) by striking “2007” in subparagraph (E)
2 and inserting “2007;”; and

3 (3) by adding at the end of the following:

4 “(F) \$50,000,000 for fiscal year 2010;

5 “(G) \$52,000,000 for fiscal year 2011;

6 “(H) \$54,000,000 for fiscal year 2012;

7 “(I) \$56,000,000 for fiscal year 2013; and

8 “(J) \$58,000,000 for fiscal year 2014.”.

9 (h) COMPUTER AND NETWORK SECURITY CAPACITY
10 BUILDING GRANTS.—Section 5(a)(6) of such Act (15
11 U.S.C. 7404(a)(6)) is amended—

12 (1) by striking “and” in subparagraph (D);

13 (2) by striking “2007” in subparagraph (E)
14 and inserting “2007;”; and

15 (3) by adding at the end of the following:

16 “(F) \$40,000,000 for fiscal year 2010;

17 “(G) \$42,000,000 for fiscal year 2011;

18 “(H) \$44,000,000 for fiscal year 2012;

19 “(I) \$46,000,000 for fiscal year 2013; and

20 “(J) \$48,000,000 for fiscal year 2014.”.

21 (i) SCIENTIFIC AND ADVANCED TECHNOLOGY ACT
22 GRANTS.—Section 5(b)(2) of such Act (15 U.S.C.
23 7404(b)(2)) is amended—

24 (1) by striking “and” in subparagraph (D);

1 (2) by striking “2007” in subparagraph (E)
2 and inserting “2007;”; and

3 (3) by adding at the end of the following:

4 “(F) \$5,000,000 for fiscal year 2010;

5 “(G) \$6,000,000 for fiscal year 2011;

6 “(H) \$7,000,000 for fiscal year 2012;

7 “(I) \$8,000,000 for fiscal year 2013; and

8 “(J) \$9,000,000 for fiscal year 2014.”.

9 (j) GRADUATE TRAINEESHIPS IN COMPUTER AND
10 NETWORK SECURITY RESEARCH.—Section 5(c)(7) of
11 such Act (15 U.S.C. 7404(c)(7)) is amended—

12 (1) by striking “and” in subparagraph (D);

13 (2) by striking “2007” in subparagraph (E)
14 and inserting “2007;”; and

15 (3) by adding at the end of the following:

16 “(F) \$20,000,000 for fiscal year 2010;

17 “(G) \$22,000,000 for fiscal year 2011;

18 “(H) \$24,000,000 for fiscal year 2012;

19 “(I) \$26,000,000 for fiscal year 2013; and

20 “(J) \$28,000,000 for fiscal year 2014.”.

21 (k) CYBERSECURITY FACULTY DEVELOPMENT
22 TRAINEESHIP PROGRAM.—Section 5(e)(9) of such Act (15
23 U.S.C. 7404(e)(9)) is amended by striking “2007.” and
24 inserting “2007 and for each of fiscal years 2010 through
25 2014.”.

1 (l) NETWORKING AND INFORMATION TECHNOLOGY
2 RESEARCH AND DEVELOPMENT PROGRAM.—Section
3 204(a)(1) of the High-Performance Computing Act of
4 1991 (15 U.S.C. 5524(a)(1)) is amended—

5 (1) by striking “and” after the semicolon in
6 subparagraph (B); and

7 (2) by inserting after subparagraph (C) the fol-
8 lowing:

9 “(D) develop and propose standards and
10 guidelines, and develop measurement techniques
11 and test methods, for enhanced cybersecurity
12 for computer networks and common user inter-
13 faces to systems; and”.

14 **SEC. 12. FEDERAL CYBER SCHOLARSHIP-FOR-SERVICE**
15 **PROGRAM.**

16 (a) IN GENERAL.—The Director of the National
17 Science Foundation shall establish a Federal Cyber Schol-
18 arship-for-Service program to recruit and train the next
19 generation of Federal information technology workers and
20 security managers.

21 (b) PROGRAM DESCRIPTION AND COMPONENTS.—
22 The program—

23 (1) shall provide scholarships, that provide full
24 tuition, fees, and a stipend, for up to 1,000 students

1 per year in their pursuit of undergraduate or grad-
2 uate degrees in the cybersecurity field;

3 (2) shall require scholarship recipients, as a
4 condition of receiving a scholarship under the pro-
5 gram, to agree to serve in the Federal information
6 technology workforce for a period equal to the length
7 of the scholarship following graduation if offered em-
8 ployment in that field by a Federal agency;

9 (3) shall provide opportunities for students to
10 receive temporary appointments for meaningful em-
11 ployment in the Federal information technology
12 workforce during school vacation periods and for in-
13 ternships;

14 (4) shall provide a procedure for identifying
15 promising K–12 students for participation in sum-
16 mer work and internship programs that would lead
17 to certification of Federal information technology
18 workforce standards and possible future employ-
19 ment; and

20 (5) shall examine and develop, if appropriate,
21 programs to promote computer security awareness in
22 secondary and high school classrooms.

23 (c) HIRING AUTHORITY.—For purposes of any law
24 or regulation governing the appointment of individuals in
25 the Federal civil service, upon the successful completion

1 of their studies, students receiving a scholarship under the
2 program shall be hired under the authority provided for
3 in section 213.3102(r) of title 5, Code of Federal Regula-
4 tions, and be exempt from competitive service. Upon ful-
5 fillment of the service term, such individuals shall be con-
6 verted to a competitive service position without competi-
7 tion if the individual meets the requirements for that posi-
8 tion.

9 (d) ELIGIBILITY.—To be eligible to receive a scholar-
10 ship under this section, an individual shall—

- 11 (1) be a citizen of the United States; and
- 12 (2) demonstrate a commitment to a career in
13 improving the Nation’s cyber defenses.

14 (e) CONSIDERATION AND PREFERENCE.—In making
15 selections for scholarships under this section, the Director
16 shall—

- 17 (1) consider, to the extent possible, a diverse
18 pool of applicants whose interests are of an inter-
19 disciplinary nature, encompassing the social sci-
20 entific as well as the technical dimensions of cyber
21 security; and
- 22 (2) give preference to applicants that have par-
23 ticipated in the competition and challenge described
24 in section 13.

1 (f) EVALUATION AND REPORT.—The Director shall
2 evaluate and report to the Senate Committee on Com-
3 merce, Science, and Transportation and the House of Rep-
4 resentatives Committee on Science and Technology on the
5 success of recruiting individuals for the scholarships.

6 (g) AUTHORIZATION OF APPROPRIATIONS.—There
7 are authorized to be appropriated to the National Science
8 Foundation to carry out this section—

9 (1) \$50,000,000 for fiscal year 2010;

10 (2) \$55,000,000 for fiscal year 2011;

11 (3) \$60,000,000 for fiscal year 2012;

12 (4) \$65,000,000 for fiscal year 2013; and

13 (5) \$70,000,000 for fiscal year 2014.

14 **SEC. 13. CYBERSECURITY COMPETITION AND CHALLENGE.**

15 (a) IN GENERAL.—The Director of the National In-
16 stitute of Standards and Technology, directly or through
17 appropriate Federal entities, shall establish cybersecurity
18 competitions and challenges with cash prizes in order to—

19 (1) attract, identify, evaluate, and recruit tal-
20 ented individuals for the Federal information tech-
21 nology workforce; and

22 (2) stimulate innovation in basic and applied
23 cybersecurity research, technology development, and
24 prototype demonstration that have the potential for

1 application to the Federal information technology
2 activities of the Federal Government.

3 (b) TYPES OF COMPETITIONS AND CHALLENGES.—

4 The Director shall establish different competitions and
5 challenges targeting the following groups:

6 (1) High school students.

7 (2) Undergraduate students.

8 (3) Graduate students.

9 (4) Academic and research institutions.

10 (c) TOPICS.—In selecting topics for prize competi-
11 tions, the Director shall consult widely both within and
12 outside the Federal Government, and may empanel advi-
13 sory committees.

14 (d) ADVERTISING.—The Director shall widely adver-
15 tise prize competitions, in coordination with the awareness
16 campaign under section 10, to encourage participation.

17 (e) REQUIREMENTS AND REGISTRATION.—For each
18 prize competition, the Director shall publish a notice in
19 the Federal Register announcing the subject of the com-
20 petition, the rules for being eligible to participate in the
21 competition, the amount of the prize, and the basis on
22 which a winner will be selected.

23 (f) ELIGIBILITY.—To be eligible to win a prize under
24 this section, an individual or entity—

1 (1) shall have registered to participate in the
2 competition pursuant to any rules promulgated by
3 the Director under subsection (d);

4 (2) shall have complied with all the require-
5 ments under this section;

6 (3) in the case of a private entity, shall be in-
7 corporated in and maintain a primary place of busi-
8 ness in the United States, and in the case of an in-
9 dividual, whether participating singly or in a group,
10 shall be a citizen or permanent resident of the
11 United States; and

12 (4) shall not be a Federal entity or Federal em-
13 ployee acting within the scope of his or her employ-
14 ment.

15 (g) JUDGES.—For each competition, the Director, ei-
16 ther directly or through an agreement under subsection
17 (h), shall assemble a panel of qualified judges to select
18 the winner or winners of the prize competition. Judges for
19 each competition shall include individuals from the private
20 sector. A judge may not—

21 (1) have personal or financial interests in, or be
22 an employee, officer, director, or agent of any entity
23 that is a registered participant in a competition; or

24 (2) have a familial or financial relationship with
25 an individual who is a registered participant.

1 (h) ADMINISTERING THE COMPETITION.—The Direc-
2 tor may enter into an agreement with a private, nonprofit
3 entity to administer the prize competition, subject to the
4 provisions of this section.

5 (i) FUNDING.—

6 (1) PRIZES.—Prizes under this section may
7 consist of Federal appropriated funds and funds
8 provided by the private sector for such cash prizes.
9 The Director may accept funds from other Federal
10 agencies for such cash prizes. The Director may not
11 give special consideration to any private sector entity
12 in return for a donation.

13 (2) USE OF UNEXPENDED FUNDS.—Notwith-
14 standing any other provision of law, funds appro-
15 priated for prize awards under this section shall re-
16 main available until expended, and may be trans-
17 ferred, reprogrammed, or expended for other pur-
18 poses only after the expiration of 10 fiscal years
19 after the fiscal year for which the funds were origi-
20 nally appropriated. No provision in this section per-
21 mits obligation or payment of funds in violation of
22 the Anti-Deficiency Act (31 U.S.C. 1341).

23 (3) FUNDING REQUIRED BEFORE PRIZE AN-
24 NOUNCED.—No prize may be announced until all the
25 funds needed to pay out the announced amount of

1 the prize have been appropriated or committed in
2 writing by a private source. The Director may in-
3 crease the amount of a prize after an initial an-
4 nouncement is made under subsection (d) if—

5 (A) notice of the increase is provided in
6 the same manner as the initial notice of the
7 prize; and

8 (B) the funds needed to pay out the an-
9 nounced amount of the increase have been ap-
10 propriated or committed in writing by a private
11 source.

12 (4) NOTICE REQUIRED FOR LARGE AWARDS.—

13 No prize competition under this section may offer a
14 prize in an amount greater than \$5,000,000 unless
15 30 days have elapsed after written notice has been
16 transmitted to the Senate Committee on Commerce,
17 Science, and Transportation and the House of Rep-
18 resentatives Committee on Science and Technology.

19 (5) DIRECTOR'S APPROVAL REQUIRED FOR CER-
20 TAIN AWARDS.—No prize competition under this sec-
21 tion may result in the award of more than
22 \$1,000,000 in cash prizes without the approval of
23 the Director.

24 (j) USE OF FEDERAL INSIGNIA.—A registered partic-
25 ipant in a competition under this section may use any

1 Federal agency's name, initials, or insignia only after prior
2 review and written approval by the Director.

3 (k) COMPLIANCE WITH EXISTING LAW.—The Fed-
4 eral Government shall not, by virtue of offering or pro-
5 viding a prize under this section, be responsible for compli-
6 ance by registered participants in a prize competition with
7 Federal law, including licensing, export control, and non-
8 proliferation laws and related regulations.

9 (l) AUTHORIZATION OF APPROPRIATIONS.—There
10 are authorized to be appropriated to the National Institute
11 of Standards and Technology to carry out this section
12 \$15,000,000 for each of fiscal years 2010 through 2014.

13 **SEC. 14. PUBLIC-PRIVATE CLEARINGHOUSE.**

14 (a) DESIGNATION.—The Department of Commerce
15 shall serve as the clearinghouse of cybersecurity threat
16 and vulnerability information to Federal Government and
17 private sector owned critical infrastructure information
18 systems and networks.

19 (b) FUNCTIONS.—The Secretary of Commerce—

20 (1) shall have access to all relevant data con-
21 cerning such networks without regard to any provi-
22 sion of law, regulation, rule, or policy restricting
23 such access;

24 (2) shall manage the sharing of Federal Gov-
25 ernment and other critical infrastructure threat and

1 vulnerability information between the Federal Gov-
2 ernment and the persons primarily responsible for
3 the operation and maintenance of the networks con-
4 cerned; and

5 (3) shall report regularly to the Congress on
6 threat information held by the Federal Government
7 that is not shared with the persons primarily respon-
8 sible for the operation and maintenance of the net-
9 works concerned.

10 (c) INFORMATION SHARING RULES AND PROCE-
11 DURES.—Within 90 days after the date of enactment of
12 this Act, the Secretary shall publish in the Federal Reg-
13 ister a draft description of rules and procedures on how
14 the Federal Government will share cybersecurity threat
15 and vulnerability information with private sector critical
16 infrastructure information systems and networks owners.
17 After a 30 day comment period, the Secretary shall pub-
18 lish a final description of the rules and procedures. The
19 description shall include—

20 (1) the rules and procedures on how the Fed-
21 eral Government will share cybersecurity threat and
22 vulnerability information with private sector critical
23 infrastructure information systems and networks
24 owners;

1 (2) the criteria in which private sector owners
2 of critical infrastructure information systems and
3 networks shall share actionable cybersecurity threat
4 and vulnerability information and relevant data with
5 the Federal Government; and

6 (3) any other rule or procedure that will en-
7 hance the sharing of cybersecurity threat and vul-
8 nerability information between private sector owners
9 of critical infrastructure information systems and
10 networks and the Federal Government.

11 **SEC. 15. CYBERSECURITY RISK MANAGEMENT REPORT.**

12 Within 1 year after the date of enactment of this Act,
13 the President, or the President’s designee, shall report to
14 the Senate Committee on Commerce, Science, and Trans-
15 portation and the House of Representatives Committee on
16 Science and Technology on the feasibility of—

17 (1) creating a market for cybersecurity risk
18 management, including the creation of a system of
19 civil liability and insurance (including government
20 reinsurance); and

21 (2) requiring cybersecurity to be a factor in all
22 bond ratings.

23 **SEC. 16. LEGAL FRAMEWORK REVIEW AND REPORT.**

24 (a) IN GENERAL.—Within 1 year after the date of
25 enactment of this Act, the President, or the President’s

1 designee, through an appropriate entity, shall complete a
2 comprehensive review of the Federal statutory and legal
3 framework applicable to cyber-related activities in the
4 United States, including—

5 (1) the Privacy Protection Act of 1980 (42
6 U.S.C. 2000aa);

7 (2) the Electronic Communications Privacy Act
8 of 1986 (18 U.S.C. 2510 note);

9 (3) the Computer Security Act of 1987 (15
10 U.S.C. 271 et seq.; 40 U.S.C. 759);

11 (4) the Federal Information Security Manage-
12 ment Act of 2002 (44 U.S.C. 3531 et seq.);

13 (5) the E-Government Act of 2002 (44 U.S.C.
14 9501 et seq.);

15 (6) the Defense Production Act of 1950 (50
16 U.S.C. App. 2061 et seq.);

17 (7) any other Federal law bearing upon cyber-
18 related activities; and

19 (8) any applicable Executive Order or agency
20 rule, regulation, guideline.

21 (b) REPORT.—Upon completion of the review, the
22 President, or the President’s designee, shall submit a re-
23 port to the Senate Committee on Commerce, Science, and
24 Transportation, the House of Representatives Committee
25 on Science and Technology, and other appropriate Con-

1 gressional Committees containing the President's, or the
2 President's designee's, findings, conclusions, and rec-
3 ommendations.

4 **SEC. 17. AUTHENTICATION AND CIVIL LIBERTIES REPORT.**

5 Within 1 year after the date of enactment of this Act,
6 the President, or the President's designee, shall review,
7 and report to Congress, on the feasibility of an identity
8 management and authentication program, with the appro-
9 priate civil liberties and privacy protections, for govern-
10 ment and critical infrastructure information systems and
11 networks.

12 **SEC. 18. CYBERSECURITY RESPONSIBILITIES AND AUTHOR-**
13 **ITY.**

14 The President—

15 (1) within 1 year after the date of enactment
16 of this Act, shall develop and implement a com-
17 prehensive national cybersecurity strategy, which
18 shall include—

19 (A) a long-term vision of the Nation's cy-
20 bersecurity future; and

21 (B) a plan that encompasses all aspects of
22 national security, including the participation of
23 the private sector, including critical infrastruc-
24 ture operators and managers;

1 (2) may declare a cybersecurity emergency and
2 order the limitation or shutdown of Internet traffic
3 to and from any compromised Federal Government
4 or United States critical infrastructure information
5 system or network;

6 (3) shall designate an agency to be responsible
7 for coordinating the response and restoration of any
8 Federal Government or United States critical infra-
9 structure information system or network affected by
10 a cybersecurity emergency declaration under para-
11 graph (2);

12 (4) shall, through the appropriate department
13 or agency, review equipment that would be needed
14 after a cybersecurity attack and develop a strategy
15 for the acquisition, storage, and periodic replace-
16 ment of such equipment;

17 (5) shall direct the periodic mapping of Federal
18 Government and United States critical infrastruc-
19 ture information systems or networks, and shall de-
20 velop metrics to measure the effectiveness of the
21 mapping process;

22 (6) may order the disconnection of any Federal
23 Government or United States critical infrastructure
24 information systems or networks in the interest of
25 national security;

1 (7) shall, through the Office of Science and
2 Technology Policy, direct an annual review of all
3 Federal cyber technology research and development
4 investments;

5 (8) may delegate original classification author-
6 ity to the appropriate Federal official for the pur-
7 poses of improving the Nation’s cybersecurity posture;
8

9 (9) shall, through the appropriate department
10 or agency, promulgate rules for Federal professional
11 responsibilities regarding cybersecurity, and shall
12 provide to the Congress an annual report on Federal
13 agency compliance with those rules;

14 (10) shall withhold additional compensation, di-
15 rect corrective action for Federal personnel, or ter-
16 minate a Federal contract in violation of Federal
17 rules, and shall report any such action to the Con-
18 gress in an unclassified format within 48 hours after
19 taking any such action; and

20 (11) shall notify the Congress within 48 hours
21 after providing a cyber-related certification of legal-
22 ity to a United States person.

23 **SEC. 19. QUADRENNIAL CYBER REVIEW.**

24 (a) IN GENERAL.—Beginning with 2013 and in every
25 fourth year thereafter, the President, or the President’s

1 designee, shall complete a review of the cyber posture of
2 the United States, including an unclassified summary of
3 roles, missions, accomplishments, plans, and programs.
4 The review shall include a comprehensive examination of
5 the cyber strategy, force structure, modernization plans,
6 infrastructure, budget plan, the Nation's ability to recover
7 from a cyberemergency, and other elements of the cyber
8 program and policies with a view toward determining and
9 expressing the cyber strategy of the United States and es-
10 tablishing a revised cyber program for the next 4 years.

11 (b) INVOLVEMENT OF CYBERSECURITY ADVISORY
12 PANEL.—

13 (1) The President, or the President's designee,
14 shall apprise the Cybersecurity Advisory Panel es-
15 tablished or designated under section 3, on an ongo-
16 ing basis, of the work undertaken in the conduct of
17 the review.

18 (2) Not later than 1 year before the completion
19 date for the review, the Chairman of the Advisory
20 Panel shall submit to the President, or the Presi-
21 dent's designee, the Panel's assessment of work un-
22 dertaken in the conduct of the review as of that date
23 and shall include in the assessment the recommenda-
24 tions of the Panel for improvements to the review,

1 including recommendations for additional matters to
2 be covered in the review.

3 (c) ASSESSMENT OF REVIEW.—Upon completion of
4 the review, the Chairman of the Advisory Panel, on behalf
5 of the Panel, shall prepare and submit to the President,
6 or the President’s designee, an assessment of the review
7 in time for the inclusion of the assessment in its entirety
8 in the report under subsection (d).

9 (d) REPORT.—Not later than September 30, 2013,
10 and every 4 years thereafter, the President, or the Presi-
11 dent’s designee, shall submit to the relevant congressional
12 Committees a comprehensive report on the review. The re-
13 port shall include—

14 (1) the results of the review, including a com-
15 prehensive discussion of the cyber strategy of the
16 United States and the collaboration between the
17 public and private sectors best suited to implement
18 that strategy;

19 (2) the threats examined for purposes of the re-
20 view and the scenarios developed in the examination
21 of such threats;

22 (3) the assumptions used in the review, includ-
23 ing assumptions relating to the cooperation of other
24 countries and levels of acceptable risk; and

25 (4) the Advisory Panel’s assessment.

1 **SEC. 20. JOINT INTELLIGENCE THREAT ASSESSMENT.**

2 The Director of National Intelligence and the Sec-
3 retary of Commerce shall submit to the Congress an an-
4 nual assessment of, and report on, cybersecurity threats
5 to and vulnerabilities of critical national information, com-
6 munication, and data network infrastructure.

7 **SEC. 21. INTERNATIONAL NORMS AND CYBERSECURITY**
8 **DETERRENCE MEASURES.**

9 The President shall—

10 (1) work with representatives of foreign govern-
11 ments—

12 (A) to develop norms, organizations, and
13 other cooperative activities for international en-
14 gagement to improve cybersecurity; and

15 (B) to encourage international cooperation
16 in improving cybersecurity on a global basis;
17 and

18 (2) provide an annual report to the Congress on
19 the progress of international initiatives undertaken
20 pursuant to subparagraph (A).

21 **SEC. 22. FEDERAL SECURE PRODUCTS AND SERVICES AC-**
22 **QUISITIONS BOARD.**

23 (a) ESTABLISHMENT.—There is established a Secure
24 Products and Services Acquisitions Board. The Board
25 shall be responsible for cybersecurity review and approval
26 of high value products and services acquisition and, in co-

1 ordination with the National Institute of Standards and
2 Technology, for the establishment of appropriate stand-
3 ards for the validation of software to be acquired by the
4 Federal Government. The Director of the National Insti-
5 tute of Standards and Technology shall develop the review
6 process and provide guidance to the Board. In reviewing
7 software under this subsection, the Board may consider
8 independent secure software validation and verification as
9 key factor for approval.

10 (b) ACQUISITION STANDARDS.—The Director, in co-
11 operation with the Office of Management and Budget and
12 other appropriate Federal agencies, shall ensure that the
13 Board approval is included as a prerequisite to the acquisi-
14 tion of any product or service—

15 (1) subject to review by the Board; and

16 (2) subject to Federal acquisition standards.

17 (c) ACQUISITION COMPLIANCE.—After the publica-
18 tion of the standards developed under subsection (a), any
19 proposal submitted in response to a request for proposals
20 issued by a Federal agency shall demonstrate compliance
21 with any such applicable standard in order to ensure that
22 cybersecurity products and services are designed to be an
23 integral part of the overall acquisition.

24 **SEC. 23. DEFINITIONS.**

25 In this Act:

1 (1) ADVISORY PANEL.—The term “Advisory
2 Panel” means the Cybersecurity Advisory Panel es-
3 tablished or designated under section 3.

4 (2) CYBER.—The term “cyber” means—

5 (A) any process, program, or protocol re-
6 lating to the use of the Internet or an intranet,
7 automatic data processing or transmission, or
8 telecommunication via the Internet or an
9 intranet; and

10 (B) any matter relating to, or involving the
11 use of, computers or computer networks.

12 (3) FEDERAL GOVERNMENT AND UNITED
13 STATES CRITICAL INFRASTRUCTURE INFORMATION
14 SYSTEMS AND NETWORKS.—The term “Federal Gov-
15 ernment and United States critical infrastructure in-
16 formation systems and networks” includes—

17 (A) Federal Government information sys-
18 tems and networks; and

19 (B) State, local, and nongovernmental in-
20 formation systems and networks in the United
21 States designated by the President as critical
22 infrastructure information systems and net-
23 works.

24 (4) INTERNET.—The term “Internet” has the
25 meaning given that term by section 4(4) of the

1 High-Performance Computing Act of 1991 (15
2 U.S.C. 5503(4)).

3 (5) NETWORK.—The term “network” has the
4 meaning given that term by section 4(5) of such Act
5 (15 U.S.C. 5503(5)).

○