

[STAFF WORKING DRAFT]

MARCH 31, 2009

111TH CONGRESS
1ST SESSION

S. _____

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

MARCH _____, 2009

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

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 cy-

bersecurity 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,*

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

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

6 (b) TABLE OF CONTENTS.—The table of contents for
7 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.

8 **SEC. 2. FINDINGS.**

9 The Congress finds the following:

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

1 (2) Since intellectual property is now often
2 stored in digital form, industrial espionage that ex-
3 ploits weak cybersecurity dilutes our investment in
4 innovation while subsidizing the research and devel-
5 opment efforts of foreign competitors. In the new
6 global competition, where economic strength and
7 technological leadership are vital components of na-
8 tional power, failing to secure cyberspace puts us at
9 a disadvantage.

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

21 (4) The Director of National Intelligence testi-
22 fied before the Congress on February 19, 2009 that
23 “a growing array of state and non-state adversaries
24 are increasingly targeting-for exploitation and poten-
25 tially disruption or destruction-our information in-

1 frastructure, including the Internet, telecommuni-
2 cations networks, computer systems, and embedded
3 processors and controllers in critical industries” and
4 these trends are likely to continue.

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

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

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

1 (8) Alan Paller, the Director of Research at the
2 SANS Institute, testified before the Congress that
3 “the fight against cybercrime resembles an arms
4 race where each time the defenders build a new wall,
5 the attackers create new tools to scale the wall.
6 What is particularly important in this analogy is
7 that, unlike conventional warfare where deployment
8 takes time and money and is quite visible, in the
9 cyber world, when the attackers find a new weapon,
10 they can attack millions of computers, and success-
11 fully infect hundreds of thousands, in a few hours or
12 days, and remain completely hidden.”

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

1 (10) According to the National Journal, Mike
2 McConnell, the former Director of National Intel-
3 ligence, told President Bush in May 2007 that if the
4 9/11 attackers had chosen computers instead of air-
5 planes as their weapons and had waged a massive
6 assault on a U.S. bank, the economic consequences
7 would have been “an order of magnitude greater”
8 than those caused by the physical attack on the
9 World Trade Center. Mike McConnell has subse-
10 quently referred to cybersecurity as the “soft under-
11 belly of this country.”

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

1 on the economic health and national security of the
2 United States.”

3 (12) James Lewis, Director and Senior Fellow,
4 Technology and Public Policy Program, Center for
5 Strategic and International Studies, testified on be-
6 half of the Center for Strategic and International
7 Studies that “the United States is not organized and
8 lacks a coherent national strategy for addressing”
9 cybersecurity.

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

1 (14) The President’s Information Technology
2 Advisory Committee reported in 2005 that software
3 is a major vulnerability and that “software develop-
4 ment methods that have been the norm fail to pro-
5 vide the high-quality, reliable, and secure software
6 that the IT infrastructure requires. . . . Today, as
7 with cancer, vulnerable software can be invaded and
8 modified to cause damage to previously healthy soft-
9 ware, and infected software can replicate itself and
10 be carried across networks to cause damage in other
11 systems.”

12 **SEC. 3. CYBERSECURITY ADVISORY PANEL.**

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

15 (b) QUALIFICATIONS.—The President—

16 (1) shall appoint as members of the panel rep-
17 resentatives of industry, academic, non-profit organi-
18 zations, interest groups and advocacy organizations,
19 and State and local governments who are qualified
20 to provide advice and information on cybersecurity
21 research, development, demonstrations, education,
22 technology transfer, commercial application, or soci-
23 etal and civil liberty concerns; and

24 (2) may seek and give consideration to rec-
25 ommendations from the Congress, industry, the cy-

1 bersecurity community, the defense community,
2 State and local governments, and other appropriate
3 organizations.

4 (c) DUTIES.—The panel shall advise the President on
5 matters relating to the national cybersecurity program
6 and strategy and shall assess—

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

9 (2) progress made in implementing the strat-
10 egy;

11 (3) the need to revise the strategy;

12 (4) the balance among the components of the
13 national strategy, including funding for program
14 components;

15 (5) whether the strategy, priorities, and goals
16 are helping to maintain United States leadership
17 and defense in cybersecurity;

18 (6) the management, coordination, implementa-
19 tion, and activities of the strategy; and

20 (7) whether societal and civil liberty concerns
21 are adequately addressed.

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

1 (e) TRAVEL EXPENSES OF NON-FEDERAL MEM-
2 BERS.—Non-Federal members of the panel, while attend-
3 ing meetings of the panel or while otherwise serving at
4 the request of the head of the panel while away from their
5 homes or regular places of business, may be allowed travel
6 expenses, including per diem in lieu of subsistence, as au-
7 thorized by section 5703 of title 5, United States Code,
8 for individuals in the government serving without pay.
9 Nothing in this subsection shall be construed to prohibit
10 members of the panel who are officers or employees of the
11 United States from being allowed travel expenses, includ-
12 ing per diem in lieu of subsistence, in accordance with law.

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

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

17 The Secretary of Commerce shall—

18 (1) in consultation with the Office of Manage-
19 ment and Budget, develop a plan within 90 days
20 after the date of enactment of this Act to implement
21 a system to provide dynamic, comprehensive, real-
22 time cybersecurity status and vulnerability informa-
23 tion of all Federal government information systems
24 and networks managed by the Department of Com-
25 merce; and

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

3 **SEC. 5. STATE AND REGIONAL CYBERSECURITY ENHANCE-**
4 **MENT PROGRAM.**

5 (a) CREATION AND SUPPORT OF CYBERSECURITY
6 CENTERS.—The Secretary of Commerce shall provide as-
7 sistance for the creation and support of Regional Cyberse-
8 curity Centers for the promotion and implementation of
9 cybersecurity standards. Each Center shall be affiliated
10 with a United States-based nonprofit institution or organi-
11 zation, or consortium thereof, that applies for and is
12 awarded financial assistance under this section.

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

16 (1) the transfer of cybersecurity standards,
17 processes, technology, and techniques developed at
18 the National Institute of Standards and Technology
19 to Centers and, through them, to small- and me-
20 dium-sized companies throughout the United States;

21 (2) the participation of individuals from indus-
22 try, universities, State governments, other Federal
23 agencies, and, when appropriate, the Institute in co-
24 operative technology transfer activities;

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

4 (4) the active dissemination of scientific, engi-
5 neering, technical, and management information
6 about cybersecurity to industrial firms, including
7 small- and medium-sized companies; and

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

11 (c) ACTIVITIES.—The Centers shall—

12 (1) disseminate cybersecurity technologies,
13 standard, and processes based on research by the In-
14 stitute for the purpose of demonstrations and tech-
15 nology transfer;

16 (2) actively transfer and disseminate cybersecu-
17 rity strategies, best practices, standards, and tech-
18 nologies to protect against and mitigate the risk of
19 cyber attacks to a wide range of companies and en-
20 terprises, particularly small- and medium-sized busi-
21 nesses; and

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

1 (c) DURATION AND AMOUNT OF SUPPORT; PROGRAM
2 DESCRIPTIONS; APPLICATIONS; MERIT REVIEW; EVALUA-
3 TIONS OF ASSISTANCE.—

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

9 (2) PROGRAM DESCRIPTION.—Within 90 days
10 after the date of enactment of this Act, the Sec-
11 retary shall publish in the Federal Register a draft
12 description of a program for establishing Centers
13 and, after a 30-day comment period, shall publish a
14 final description of the program. The description
15 shall include—

16 (A) a description of the program;

17 (B) procedures to be followed by appli-
18 cants;

19 (C) criteria for determining qualified appli-
20 cants;

21 (D) criteria, including those described in
22 paragraph (4), for choosing recipients of finan-
23 cial assistance under this section from among
24 the qualified applicants; and

1 (E) maximum support levels expected to be
2 available to Centers under the program in the
3 fourth through sixth years of assistance under
4 this section.

5 (3) APPLICATIONS; SUPPORT COMMITMENT.—

6 Any nonprofit institution, or consortia of nonprofit
7 institutions, may submit to the Secretary an applica-
8 tion for financial support under this section, in ac-
9 cordance with the procedures established by the Sec-
10 retary. In order to receive assistance under this sec-
11 tion, an applicant shall provide adequate assurances
12 that it will contribute 50 percent or more of the pro-
13 posed Center's annual operating and maintenance
14 costs for the first 3 years and an increasing share
15 for each of the next 3 years.

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

21 (A) the merits of the application, particu-
22 larly those portions of the application regarding
23 technology transfer, training and education, and
24 adaptation of cybersecurity technologies to the
25 needs of particular industrial sectors;

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

2 (C) geographical diversity and extent of
3 service area; and

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

6 (5) THIRD YEAR EVALUATION.—

7 (A) IN GENERAL.—Each Center which re-
8 ceives financial assistance under this section
9 shall be evaluated during its third year of oper-
10 ation by an evaluation panel appointed by the
11 Secretary.

12 (B) EVALUATION PANEL.—Each evalua-
13 tion panel shall be composed of private experts,
14 none of whom shall be connected with the in-
15 volved Center, and Federal officials. An official
16 of the Institute shall chair the panel. Each eval-
17 uation panel shall measure the Center's per-
18 formance against the objectives specified in this
19 section.

20 (C) POSITIVE EVALUATION REQUIRED FOR
21 CONTINUED FUNDING.—The Secretary may not
22 provide funding for the fourth through the sixth
23 years of a Center's operation unless the evalua-
24 tion by the evaluation panel is positive. If the
25 evaluation is positive, the Secretary may pro-

1 vide continued funding through the sixth year
2 at declining levels.

3 (D) FUNDING AFTER SIXTH YEAR.—After
4 the sixth year, the Secretary may provide addi-
5 tional financial support to a Center if it has re-
6 ceived a positive evaluation through an inde-
7 pendent review, under procedures established by
8 the Institute. An additional independent review
9 shall be required at least every 2 years after the
10 sixth year of operation. Funding received for a
11 fiscal year under this section after the sixth
12 year of operation may not exceed one third of
13 the annual operating and maintenance costs of
14 the Center.

15 (6) PATENT RIGHTS TO INVENTIONS.—The pro-
16 visions of chapter 18 of title 35, United States Code,
17 shall (to the extent not inconsistent with this sec-
18 tion) apply to the promotion of technology from re-
19 search by Centers under this section except for con-
20 tracts for such specific technology extension or
21 transfer services as may be specified by statute or
22 by the President, or the President's designee,.

23 (d) ACCEPTANCE OF FUNDS FROM OTHER FEDERAL
24 DEPARTMENTS AND AGENCIES.—In addition to such
25 sums as may be authorized and appropriated to the Sec-

1 retary and President, or the President's designee, to oper-
2 ate the Centers program, the Secretary and the President,
3 or the President's designee, also may accept funds from
4 other Federal departments and agencies for the purpose
5 of providing Federal funds to support Centers. Any Center
6 which is supported with funds which originally came from
7 other Federal departments and agencies shall be selected
8 and operated according to the provisions of this section.

9 **SEC. 6. NIST STANDARDS DEVELOPMENT AND COMPLI-**
10 **ANCE.**

11 (a) IN GENERAL.—Within 1 year after the date of
12 enactment of this Act, the National Institute of Standards
13 and Technology shall establish measurable and auditable
14 cybersecurity standards for all Federal government, gov-
15 ernment contractor, or grantee critical infrastructure in-
16 formation systems and networks in the following areas:

17 (1) CYBERSECURITY METRICS RESEARCH.—The
18 Director of the National Institute of Standards shall
19 establish a research program to develop cybersecu-
20 rity metrics and benchmarks that can assess the eco-
21 nomic impact of cybersecurity. These metrics should
22 measure risk reduction and the cost of defense. The
23 research shall include the development automated
24 tools to assess vulnerability and compliance.

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

5 (3) SOFTWARE SECURITY.—The Institute shall
6 establish standards for measuring the software secu-
7 rity using a prioritized list of software weaknesses
8 known to lead to exploited and exploitable
9 vulnerabilities. The Institute will also establish a
10 separate set of such standards for measuring secu-
11 rity in embedded software such as that found in in-
12 dustrial control systems.

13 (4) SOFTWARE CONFIGURATION SPECIFICATION
14 LANGUAGE.—The Institute shall, establish standard
15 computer-readable language for completely speci-
16 fying the configuration of software on computer sys-
17 tems widely used in the Federal government, by gov-
18 ernment contractors and grantees, and in private
19 sector owned critical infrastructure information sys-
20 tems and networks.

21 (5) STANDARD SOFTWARE CONFIGURATION.—
22 The Institute shall establish standard configurations
23 consisting of security settings for operating system
24 software and software utilities widely used in the
25 Federal government, by government contractors and

1 grantees, and in private sector owned critical infra-
2 structure information systems and networks.

3 (6) VULNERABILITY SPECIFICATION LAN-
4 GUAGE.—The Institute shall establish standard com-
5 puter-readable language for specifying vulnerabilities
6 in software to enable software vendors to commu-
7 nicate vulnerability data to software users in real
8 time.

9 (7) NATIONAL COMPLIANCE STANDARDS FOR
10 ALL SOFTWARE.—

11 (A) Protocol.—The Institute shall establish
12 a standard testing and accreditation protocol
13 for software built by or for the Federal govern-
14 ment, its contractors, and grantees, and private
15 sector owned critical infrastructure information
16 systems and networks. to ensure that it—

17 (i) meets the software security stand-
18 ards of paragraph (2); and

19 (ii) does not require or cause any
20 changes to be made in the standard con-
21 figurations described in paragraph (4).

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

24 (i) software development organizations
25 comply with the protocol established under

1 subparagraph (A) during the software de-
2 velopment process; and

3 (ii) testing results showing evidence of
4 adequate testing and defect reduction are
5 provided to the Federal government prior
6 to deployment of software.

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

15 (c) INTERNATIONAL STANDARDS.—The Director,
16 through the Institute and in coordination with appropriate
17 Federal agencies, shall be responsible for United States
18 representation in all international standards development
19 related to cybersecurity, and shall develop and implement
20 a strategy to optimize the United States' position with re-
21 spect to international cybersecurity standards.

22 (d) COMPLIANCE ENFORCEMENT.—The Director
23 shall—

1 (b) MANDATORY LICENSING.—Beginning 3 years
2 after the date of enactment of this Act, it shall be unlawful
3 for any individual to engage in business in the United
4 States, or to be employed in the United States, as a pro-
5 vider of cybersecurity services to any Federal agency or
6 an information system or network designated by the Presi-
7 dent, or the President’s designee, as a critical infrastruc-
8 ture information system or network, who is not licensed
9 and certified under the program.

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

11 (a) IN GENERAL.—No action by the Assistant Sec-
12 retary of Commerce for Communications and Information
13 after the date of enactment of this Act with respect to
14 the renewal or modification of a contract related to the
15 operation of the Internet Assigned Numbers Authority,
16 shall be final until the Advisory Panel—

- 17 (1) has reviewed the action;
18 (2) considered the commercial and national se-
19 curity implications of the action; and
20 (3) approved the action.

21 (b) APPROVAL PROCEDURE.—If the Advisory Panel
22 does not approve such an action, it shall immediately no-
23 tify the Assistant Secretary in writing of the disapproval
24 and the reasons therefor. The Advisory Panel may provide
25 recommendations to the Assistant Secretary in the notice

1 for any modifications the it deems necessary to secure ap-
2 proval of the action.

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

4 (a) IN GENERAL.—Within 3 years after the date of
5 enactment of this Act, the Assistant Secretary of Com-
6 merce for Communications and Information shall develop
7 a strategy to implement a secure domain name addressing
8 system. The Assistant Secretary shall publish notice of the
9 system requirements in the Federal Register together with
10 an implementation schedule for Federal agencies and in-
11 formation systems or networks designated by the Presi-
12 dent, or the President’s designee, as critical infrastructure
13 information systems or networks.

14 (b) COMPLIANCE REQUIRED.—The President shall
15 ensure that each Federal agency and each such system
16 or network implements the secure domain name address-
17 ing system in accordance with the schedule published by
18 the Assistant Secretary.

19 **SEC. 10. PROMOTING CYBERSECURITY AWARENESS.**

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

22 (1) is designed to heighten public awareness of
23 cybersecurity issues and concerns;

24 (2) communicates the Federal government’s
25 role in securing the Internet and protecting privacy

1 and civil liberties with respect to Internet-related ac-
2 tivities; and

3 (3) utilizes public and private sector means of
4 providing information to the public, including public
5 service announcements.

6 **SEC. 11. FEDERAL CYBERSECURITY RESEARCH AND DE-**
7 **VELOPMENT.**

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

9 The Director of the National Science Foundation shall
10 give priority to computer and information science and en-
11 gineering research to ensure substantial support is pro-
12 vided to meet the following challenges in cybersecurity:

13 (1) How to design and build complex software-
14 intensive systems that are secure and reliable when
15 first deployed.

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

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

22 (4) How to guarantee the privacy of an individ-
23 ual's identity, information, or lawful transactions
24 when stored in distributed systems or transmitted
25 over networks.

1 (5) How to build new protocols to enable the
2 Internet to have robust security as one of its key ca-
3 pabilities.

4 (6) How to determine the origin of a message
5 transmitted over the Internet.

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

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

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

18 (c) ASSESSMENT OF SECURE CODING EDUCATION IN
19 COLLEGES AND UNIVERSITIES.—Within one year after
20 the date of enactment of this Act, the Director shall sub-
21 mit to the Senate Committee on Commerce, Science, and
22 Transportation and the House of Representatives Com-
23 mittee on Science and Technology a report on the state
24 of secure coding education in America’s colleges and uni-
25 versities for each school that received National Science

1 Foundation funding in excess of \$1,000,000 during
2 FY2008. The report shall include—

3 (1) the number of students who earned under-
4 graduate degrees in computer science or in each
5 other program where graduates have a substantial
6 probability of being engaged in software design or
7 development after graduation;

8 (2) the percentage of those students who com-
9 pleted substantive secure coding education or im-
10 provement programs during their undergraduate ex-
11 perience; and

12 (3) descriptions of the length and content of the
13 education and improvement programs, and a meas-
14 ure of the effectiveness of those programs in ena-
15 bling the students to master secure coding and de-
16 sign.

17 (d) CYBERSECURITY MODELING AND TESTBEDS.—

18 The Director shall establish a program to award grants
19 to institutions of higher education to establish cybersecu-
20 rity testbeds capable of realistic modeling of real-time
21 cyber attacks and defenses. The purpose of this program
22 is to support the rapid development of new cybersecurity
23 defenses, techniques, and processes by improving under-
24 standing and assessing the latest technologies in a real-
25 world environment. The testbeds shall be sufficiently large

1 in order to model the scale and complexity of real world
2 networks and environments.

3 (e) NSF COMPUTER AND NETWORK SECURITY RE-
4 SEARCH GRANT AREAS.—Section 4(a)(1) of the Cyberse-
5 curity Research and Development Act (15 U.S.C.
6 7403(a)(1)) is amended—

7 (1) by striking “and” after the semicolon in
8 subparagraph (H);

9 (2) by striking “property.” in subparagraph (I)
10 and inserting “property;”; and

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

12 “(J) secure fundamental protocols that are at
13 the heart of inter-network communications and data
14 exchange;

15 “(K) secure software engineering and software
16 assurance, including—

17 “(i) programming languages and systems
18 that include fundamental security features;

19 “(ii) portable or reusable code that re-
20 mains secure when deployed in various environ-
21 ments;

22 “(iii) verification and validation tech-
23 nologies to ensure that requirements and speci-
24 fications have been implemented; and

1 “(iv) models for comparison and metrics to
2 assure that required standards have been met;
3 “(L) holistic system security that—
4 “(i) addresses the building of secure sys-
5 tems from trusted and untrusted components;
6 “(ii) proactively reduces vulnerabilities;
7 “(iii) addresses insider threats; and
8 “(iv) supports privacy in conjunction with
9 improved security;
10 “(M) monitoring and detection; and
11 “(N) mitigation and rapid recovery methods.”.

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

- 16 (1) by striking “and” in subparagraph (D);
17 (2) by striking “2007” in subparagraph (E)
18 and inserting “2007;”; and
19 (3) by adding at the end of the following:
20 “(F) \$150,000,000 for fiscal year 2010;
21 “(G) \$155,000,000 for fiscal year 2011;
22 “(H) \$160,000,000 for fiscal year 2012;
23 “(I) \$165,000,000 for fiscal year 2013;
24 and
25 “(J) \$170,000,000 for fiscal year 2014.”.

1 (g) COMPUTER AND NETWORK SECURITY CEN-
2 TERS.—Section 4(b)(7) of such Act (15 U.S.C.
3 7403(b)(7)) is amended—

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

1 (i) SCIENTIFIC AND ADVANCED TECHNOLOGY ACT
2 GRANTS.—Section 5(b)(2) of such Act (15 U.S.C.
3 7404(b)(2)) is amended—

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

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

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

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

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

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

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

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

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

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

17 (2) by striking “2007” in subparagraph (E)

18 and inserting “2007;”; and

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

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

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

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

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

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

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

6 (l) NETWORKING AND INFORMATION TECHNOLOGY
7 RESEARCH AND DEVELOPMENT PROGRAM.—Section
8 204(a)(1) of the High-Performance Computing Act of
9 1991 (15 U.S.C. 5524(a)(1)) is amended—

10 (1) by striking “and” after the semicolon in
11 subparagraph (B); and

12 (2) by inserting after subparagraph (C) the fol-
13 lowing:

14 “(D) develop and propose standards and
15 guidelines, and develop measurement techniques
16 and test methods, for enhanced cybersecurity
17 for computer networks and common user inter-
18 faces to systems; and”.

19 **SEC. 12. FEDERAL CYBER SCHOLARSHIP-FOR-SERVICE**
20 **PROGRAM.**

21 (a) IN GENERAL.—The Director of the National
22 Science Foundation shall establish a Federal Cyber Schol-
23 arship-for-Service program to recruit and train the next
24 generation of Federal information technology workers and
25 security managers.

1 (b) PROGRAM DESCRIPTION AND COMPONENTS.—

2 The program—

3 (1) shall provide scholarships, that provide full
4 tuition, fees, and a stipend, for up to 1,000 students
5 per year in their pursuit of undergraduate or grad-
6 uate degrees in the cybersecurity field;

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

13 (3) shall provide opportunities for students to
14 receive temporary appointments for meaningful em-
15 ployment in the Federal information technology
16 workforce during school vacation periods and for in-
17 ternships;

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

1 (5) shall examine and develop, if appropriate,
2 programs to promote computer security awareness in
3 secondary and high school classrooms.

4 (c) HIRING AUTHORITY.—For purposes of any law
5 or regulation governing the appointment of individuals in
6 the Federal civil service, upon the successful completion
7 of their studies, students receiving a scholarship under the
8 program shall be hired under the authority provided for
9 in section 213.3102(r) of title 5, Code of Federal Regula-
10 tions, and be exempt from competitive service. Upon ful-
11 fillment of the service term, such individuals shall be con-
12 verted to a competitive service position without competi-
13 tion if the individual meets the requirements for that posi-
14 tion.

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

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

20 (e) CONSIDERATION AND PREFERENCE.—In making
21 selections for scholarships under this section, the Director
22 shall—

- 23 (1) consider, to the extent possible, a diverse
24 pool of applicants whose interests are of an inter-
25 disciplinary nature, encompassing the social sci-

1 entific as well as the technical dimensions of cyber
2 security; and

3 (2) give preference to applicants that have par-
4 ticipated in the competition and challenge described
5 in section 13.

6 (f) **EVALUATION AND REPORT.**—The Director shall
7 evaluate and report to the Senate Committee on Com-
8 merce, Science, and Transportation and the House of Rep-
9 resentatives Committee on Science and Technology on the
10 success of recruiting individuals for the scholarships.

11 (g) **AUTHORIZATION OF APPROPRIATIONS.**—There
12 are authorized to be appropriated to the National Science
13 Foundation to carry out this section—

14 (1) \$50,000,000 for fiscal year 2010;

15 (2) \$55,000,000 for fiscal year 2011;

16 (3) \$60,000,000 for fiscal year 2012;

17 (4) \$65,000,000 for fiscal year 2013; and

18 (5) \$70,000,000 for fiscal year 2014.

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

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

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

4 (2) stimulate innovation in basic and applied
5 cybersecurity research, technology development, and
6 prototype demonstration that have the potential for
7 application to the Federal information technology
8 activities of the Federal government.

9 (b) TYPES OF COMPETITIONS AND CHALLENGES.—

10 The Director shall establish different competitions and
11 challenges targeting the following groups:

12 (1) High school students.

13 (2) Undergraduate students.

14 (3) Graduate students.

15 (4) Academic and research institutions.

16 (c) TOPICS.—In selecting topics for prize competi-
17 tions, the Director shall consult widely both within and
18 outside the Federal Government, and may empanel advi-
19 sory committees.

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

23 (e) REQUIREMENTS AND REGISTRATION.—For each
24 prize competition, the Director shall publish a notice in
25 the Federal Register announcing the subject of the com-

1 petition, the rules for being eligible to participate in the
2 competition, the amount of the prize, and the basis on
3 which a winner will be selected.

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

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

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

11 (3) in the case of a private entity, shall be in-
12 corporated in and maintain a primary place of busi-
13 ness in the United States, and in the case of an in-
14 dividual, whether participating singly or in a group,
15 shall be a citizen or permanent resident of the
16 United States; and

17 (4) shall not be a Federal entity or Federal em-
18 ployee acting within the scope of his or her employ-
19 ment.

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

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

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

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

10 (i) FUNDING.—

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

18 (2) USE OF UNEXPENDED FUNDS.—Notwith-
19 standing any other provision of law, funds appro-
20 priated for prize awards under this section shall re-
21 main available until expended, and may be trans-
22 ferred, reprogrammed, or expended for other pur-
23 poses only after the expiration of 10 fiscal years
24 after the fiscal year for which the funds were origi-
25 nally appropriated. No provision in this section per-

1 mits obligation or payment of funds in violation of
2 the Anti-Deficiency Act (31 U.S.C. 1341).

3 (3) FUNDING REQUIRED BEFORE PRIZE AN-
4 NOUNCED.—No prize may be announced until all the
5 funds needed to pay out the announced amount of
6 the prize have been appropriated or committed in
7 writing by a private source. The Director may in-
8 crease the amount of a prize after an initial an-
9 nouncement is made under subsection (d) if—

10 (A) notice of the increase is provided in
11 the same manner as the initial notice of the
12 prize; and

13 (B) the funds needed to pay out the an-
14 nounced amount of the increase have been ap-
15 propriated or committed in writing by a private
16 source.

17 (4) NOTICE REQUIRED FOR LARGE AWARDS.—
18 No prize competition under this section may offer a
19 prize in an amount greater than \$5,000,000 unless
20 30 days have elapsed after written notice has been
21 transmitted to the Senate Committee on Commerce,
22 Science, and Transportation and the House of Rep-
23 resentatives Committee on Science and Technology.

24 (5) DIRECTOR'S APPROVAL REQUIRED FOR CER-
25 TAIN AWARDS.—No prize competition under this sec-

1 tion may result in the award of more than
2 \$1,000,000 in cash prizes without the approval of
3 the Director.

4 (j) USE OF FEDERAL INSIGNIA.—A registered partic-
5 ipant in a competition under this section may use any
6 Federal agency’s name, initials, or insignia only after prior
7 review and written approval by the Director.

8 (j) COMPLIANCE WITH EXISTING LAW.—The Federal
9 Government shall not, by virtue of offering or providing
10 a prize under this section, be responsible for compliance
11 by registered participants in a prize competition with Fed-
12 eral law, including licensing, export control, and non-pro-
13 liferation laws and related regulations.

14 (k) AUTHORIZATION OF APPROPRIATIONS.—There
15 are authorized to be appropriated to the National Institute
16 of Standards and Technology to carry out this section
17 \$15,000,000 for each of fiscal years 2010 through 2014.

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

19 (a) DESIGNATION.—The Department of Commerce
20 shall serve as the clearinghouse of cybersecurity threat
21 and vulnerability information to Federal government and
22 private sector owned critical infrastructure information
23 systems and networks.

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

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

5 (2) shall manage the sharing of Federal govern-
6 ment and other critical infrastructure threat and
7 vulnerability information between the Federal gov-
8 ernment and the persons primarily responsible for
9 the operation and maintenance of the networks con-
10 cerned; and

11 (3) shall report regularly to the Congress on
12 threat information held by the Federal government
13 that is not shared with the persons primarily respon-
14 sible for the operation and maintenance of the net-
15 works concerned.

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

1 (1) the rules and procedures on how the Fed-
2 eral government will share cybersecurity threat and
3 vulnerability information with private sector critical
4 infrastructure information systems and networks
5 owners;

6 (2) the criteria in which private sector owners
7 of critical infrastructure information systems and
8 networks shall share actionable cybersecurity threat
9 and vulnerability information and relevant data with
10 the Federal government; and

11 (3) any other rule or procedure that will en-
12 hance the sharing of cybersecurity threat and vul-
13 nerability information between private sector owners
14 of critical infrastructure information systems and
15 networks and the Federal government.

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

17 Within 1 year after the date of enactment of this Act,
18 the President, or the President's designee, shall report to
19 the Senate Committee on Commerce, Science, and Trans-
20 portation and the House of Representatives Committee on
21 Science and Technology on the feasibility of—

22 (1) creating a market for cybersecurity risk
23 management, including the creation of a system of
24 civil liability and insurance (including government
25 reinsurance); and

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

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

4 (a) IN GENERAL.—Within 1 year after the date of
5 enactment of this Act, the President, or the President’s
6 designee,, through an appropriate entity, shall complete a
7 comprehensive review of the Federal statutory and legal
8 framework applicable to cyber-related activities in the
9 United States, including—

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

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

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

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

18 (5) the E-Government Act of 2002 (44 U.S.C.
19 9501 et seq.);

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

22 (7) any other Federal law bearing upon cyber-
23 related activities; and

24 (7) any applicable Executive Order or agency
25 rule, regulation, guideline.

1 (b) REPORT.—Upon completion of the review, the
2 President, or the President’s designee, shall submit a re-
3 port to the Senate Committee on Commerce, Science, and
4 Transportation, the House of Representatives Committee
5 on Science and Technology, and other appropriate Con-
6 gressional Committees containing the President’s, or the
7 President’s designee’s, findings, conclusions, and rec-
8 ommendations.

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

10 Within 1 year after the date of enactment of this Act,
11 the President, or the President’s designee, shall review,
12 and report to Congress, on the feasibility of an identity
13 management and authentication program, with the appro-
14 priate civil liberties and privacy protections, for govern-
15 ment and critical infrastructure information systems and
16 networks.

17 **SEC. 18. CYBERSECURITY RESPONSIBILITIES AND AUTHOR-**
18 **ITY.**

19 The President—

20 (1) within 1 year after the date of enactment
21 of this Act, shall develop and implement a com-
22 prehensive national cybersecurity strategy, which
23 shall include—

24 (A) a long-term vision of the nation’s cy-
25 bersecurity future; and

1 (B) a plan that encompasses all aspects of
2 national security, including the participation of
3 the private sector, including critical infrastruc-
4 ture operators and managers;

5 (2) may declare a cybersecurity emergency and
6 order the limitation or shutdown of Internet traffic
7 to and from any compromised Federal government
8 or United States critical infrastructure information
9 system or network;

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

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

21 (5) shall direct the periodic mapping of Federal
22 government and United States critical infrastructure
23 information systems or networks, and shall develop
24 metrics to measure the effectiveness of the mapping
25 process;

1 (6) may order the disconnection of any Federal
2 government or United States critical infrastructure
3 information systems or networks in the interest of
4 national security;

5 (7) shall, through the Office of Science and
6 Technology Policy, direct an annual review of all
7 Federal cyber technology research and development
8 investments;

9 (8) may delegate original classification author-
10 ity to the appropriate Federal official for the pur-
11 poses of improving the Nation's cybersecurity pos-
12 ture;

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

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

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

4 **SEC. 19. QUADRENNIAL CYBER REVIEW.**

5 (a) IN GENERAL.—Beginning with 2013 and in every
6 fourth year thereafter, the President, or the President’s
7 designee, shall complete a review of the cyber posture of
8 the United States, including an unclassified summary of
9 roles, missions, accomplishments, plans, and programs.
10 The review shall include a comprehensive examination of
11 the cyber strategy, force structure, modernization plans,
12 infrastructure, budget plan, the Nation’s ability to recover
13 from a cyberemergency, and other elements of the cyber
14 program and policies with a view toward determining and
15 expressing the cyber strategy of the United States and es-
16 tablishing a revised cyber program for the next 4 years.

17 (b) INVOLVEMENT OF CYBERSECURITY ADVISORY
18 PANEL.—

19 (1) The President, or the President’s designee,
20 shall apprise the Cybersecurity Advisory Panel es-
21 tablished or designated under section 3, on an ongo-
22 ing basis, of the work undertaken in the conduct of
23 the review.

24 (2) Not later than 1 year before the completion
25 date for the review, the Chairman of the Advisory

1 Panel shall submit to the President, or the Presi-
2 dent's designee, the Panel's assessment of work un-
3 dertaken in the conduct of the review as of that date
4 and shall include in the assessment the recommenda-
5 tions of the Panel for improvements to the review,
6 including recommendations for additional matters to
7 be covered in the review.

8 (c) ASSESSMENT OF REVIEW.—Upon completion of
9 the review, the Chairman of the Advisory Panel, on behalf
10 of the Panel, shall prepare and submit to the President,
11 or the President's designee, an assessment of the review
12 in time for the inclusion of the assessment in its entirety
13 in the report under subsection (d).

14 (d) REPORT.—Not later than September 30, 2013,
15 and every 4 years thereafter, the President, or the Presi-
16 dent's designee, shall submit to the relevant congressional
17 Committees a comprehensive report on the review. The re-
18 port shall include—

19 (1) the results of the review, including a com-
20 prehensive discussion of the cyber strategy of the
21 United States and the collaboration between the
22 public and private sectors best suited to implement
23 that strategy;

1 (2) the threats examined for purposes of the re-
2 view and the scenarios developed in the examination
3 of such threats;

4 (3) the assumptions used in the review, includ-
5 ing assumptions relating to the cooperation of other
6 countries and levels of acceptable risk; and

7 (4) the Advisory Panel's assessment.

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

9 The Director of National Intelligence and the Sec-
10 retary of Commerce shall submit to the Congress an an-
11 nual assessment of, and report on, cybersecurity threats
12 to and vulnerabilities of critical national information, com-
13 munication, and data network infrastructure.

14 **SEC. 21. INTERNATIONAL NORMS AND CYBERSECURITY**
15 **DETERRENCE MEASURES.**

16 The President shall—

17 (1) work with representatives of foreign govern-
18 ments—

19 (A) to develop norms, organizations, and
20 other cooperative activities for international en-
21 gagement to improve cybersecurity; and

22 (B) to encourage international cooperation
23 in improving cybersecurity on a global basis;
24 and

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

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

6 (a) ESTABLISHMENT.—There is established a Secure
7 Products and Services Acquisitions Board. The Board
8 shall be responsible for cybersecurity review and approval
9 of high value products and services acquisition and, in co-
10 ordination with the National Institute of Standards and
11 Technology, for the establishment of appropriate stand-
12 ards for the validation of software to be acquired by the
13 Federal government. The Director of the National Insti-
14 tute of Standards and Technology shall develop the review
15 process and provide guidance to the Board. In reviewing
16 software under this subsection, the Board may consider
17 independent secure software validation and verification as
18 key factor for approval.

19 (b) ACQUISITION STANDARDS.—The Director, in co-
20 operation with the Office of Management and Budget and
21 other appropriate Federal agencies, shall ensure that the
22 Board approval is included as a prerequisite to the acqui-
23 sition of any product or service—

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

25 (2) subject to Federal acquisition standards.

1 (c) ACQUISITION COMPLIANCE.—After the publica-
2 tion of the standards developed under subsection (a), any
3 proposal submitted in response to a request for proposals
4 issued by a Federal agency shall demonstrate compliance
5 with any such applicable standard in order to ensure that
6 cybersecurity products and services are designed to be an
7 integral part of the overall acquisition.

8 **SEC. 23. DEFINITIONS.**

9 In this Act:

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

13 (2) CYBER.—The term “cyber” means—

14 (A) any process, program, or protocol re-
15 lating to the use of the Internet or an intranet,
16 automatic data processing or transmission, or
17 telecommunication via the Internet or an
18 intranet; and

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

21 (3) FEDERAL GOVERNMENT AND UNITED
22 STATES CRITICAL INFRASTRUCTURE INFORMATION
23 SYSTEMS AND NETWORKS.—The term “Federal gov-
24 ernment and United States critical infrastructure in-
25 formation systems and networks” includes—

1 (A) Federal Government information sys-
2 tems and networks; and

3 (B) State, local, and nongovernmental in-
4 formation systems and networks in the United
5 States designated by the President as critical
6 infrastructure information systems and net-
7 works.

8 (4) INTERNET.—The term “Internet” has the
9 meaning given that term by section 4(4) of the
10 High-Performance Computing Act of 1991 (15
11 U.S.C. 5503(4)).

12 (5) NETWORK.—The term “network” has the
13 meaning given that term by section 4(5) of such Act
14 (15 U.S.C. 5503(5)).

○