

Calendar No. 707111TH CONGRESS
2^D 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, Mr. NELSON of Florida, Mr. BAYH, and Ms. MIKULSKI) introduced the following bill; which was read twice and referred to the Committee on Commerce, Science, and Transportation

DECEMBER 17, 2010

Reported by Mr. ROCKEFELLER, with an amendment

[Strike all after the enacting clause and insert the part printed in italic]

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 eased 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 (e) 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 eants;

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

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 and
19 Technology shall establish a research program to de-
20 velop cybersecurity metrics and benchmarks that can
21 assess the economic impact of cybersecurity. These
22 metrics should measure risk reduction and the cost
23 of defense. The research shall include the develop-
24 ment automated tools to assess vulnerability and
25 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
18 government 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 estab-
12 lish a standard testing and accreditation pro-
13 tocol for software built by or for the Federal
14 Government, its contractors, and grantees, and
15 private sector owned critical infrastructure in-
16 formation systems and networks. to ensure that
17 it—

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

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

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

1 (i) software development organizations
2 comply with the protocol established under
3 subparagraph (A) during the software de-
4 velopment process; and

5 (ii) testing results showing evidence of
6 adequate testing and defect reduction are
7 provided to the Federal Government prior
8 to deployment of software.

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

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

24 (d) COMPLIANCE ENFORCEMENT.—The Director
25 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 fiscal
2 year 2008. 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 (c) 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(e)(7) of
 15 such Act (15 U.S.C. 7404(e)(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 entifie 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 (k) COMPLIANCE WITH EXISTING LAW.—The Fed-
9 eral Government shall not, by virtue of offering or pro-
10 viding a prize under this section, be responsible for compli-
11 ance by registered participants in a prize competition with
12 Federal law, including licensing, export control, and non-
13 proliferation laws and related regulations.

14 (l) 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 Gov-
6 ernment 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 (8) 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 infrastruc-
23 ture information systems or networks, and shall de-
24 velop metrics to measure the effectiveness of the
25 mapping 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 (e) **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)).

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

16 (a) *SHORT TITLE.*—This Act may be cited as the “Cy-
17 bersecurity Act of 2010”.

18 (b) *TABLE OF CONTENTS.*—The table of contents for
19 this Act is as follows:

Sec. 1. Short title; table of contents.

Sec. 2. Findings.

Sec. 3. Definitions.

Sec. 4. Procedure for designation of critical infrastructure information systems.

TITLE I—WORKFORCE DEVELOPMENT

Sec. 101. Certification and training of cybersecurity professionals.

Sec. 102. Federal Cyber Scholarship-for-Service Program.

Sec. 103. Cybersecurity competition and challenge.

Sec. 104. Cybersecurity workforce plan.

Sec. 105. Measures of cybersecurity hiring effectiveness.

TITLE II—PLANS AND AUTHORITY

- Sec. 201. *Cybersecurity responsibilities and authorities.*
 Sec. 202. *Biennial cyber review.*
 Sec. 203. *Cybersecurity dashboard pilot project.*
 Sec. 204. *NIST cybersecurity guidance.*
 Sec. 205. *Legal framework review and report.*
 Sec. 206. *Joint intelligence threat and vulnerability assessment.*
 Sec. 207. *International norms and cybersecurity deterrence measures.*
 Sec. 208. *Federal secure products and services acquisitions.*
 Sec. 209. *Private sector access to classified information.*
 Sec. 210. *Authentication and civil liberties report.*
 Sec. 211. *Report on evaluation of certain identity authentication functionalities.*

TITLE III—CYBERSECURITY KNOWLEDGE DEVELOPMENT

- Sec. 301. *Promoting cybersecurity awareness and education.*
 Sec. 302. *Federal cybersecurity research and development.*
 Sec. 303. *Development of curricula for incorporating cybersecurity into educational programs for future industrial control system designers.*

TITLE IV—PUBLIC-PRIVATE COLLABORATION

- Sec. 401. *Cybersecurity Advisory Panel.*
 Sec. 402. *State and regional cybersecurity enhancement program.*
 Sec. 403. *Public-private clearinghouse.*
 Sec. 404. *Cybersecurity risk management report.*

1 **SEC. 2. FINDINGS.**

2 *The Congress finds the following:*

3 (1) *As a fundamental principle, cyberspace is a*
 4 *vital asset for the nation and the United States*
 5 *should protect it using all instruments of national*
 6 *power, in order to ensure national security, public*
 7 *safety, economic prosperity, and the delivery of crit-*
 8 *ical services to the American public.*

9 (2) *President Obama has rightfully determined*
 10 *that “our digital infrastructure—the networks and*
 11 *computers we depend on every day—will be treated .*
 12 *. . as a strategic national asset”.*

1 (3) *According to the Obama Administration*
2 *Cyberspace Policy Review, “the architecture of the*
3 *Nation’s digital infrastructure is not secure or resil-*
4 *ient. Without major advances in the security of these*
5 *systems or significant change in how they are con-*
6 *structed or operated, it is doubtful that the United*
7 *States can protect itself from the growing threat of*
8 *cybercrime and state-sponsored intrusions and oper-*
9 *ations.”.*

10 (4) *With more than 85 percent of the Nation’s*
11 *critical infrastructure owned and operated by the pri-*
12 *vate sector, it is vital that the public and private sec-*
13 *tors cooperate to protect this strategic national asset.*

14 (5) *According to the 2010 Annual Threat Assess-*
15 *ment, that “sensitive information is stolen daily from*
16 *both government and private sector networks” and*
17 *that “we cannot protect cyberspace without a coordi-*
18 *nated and collaborative effort that incorporates both*
19 *the US private sector and our international part-*
20 *ners.”.*

21 (6) *The Director of National Intelligence testified*
22 *before the Congress on February 2, 2010, that intru-*
23 *sions are a stark reminder of the importance of these*
24 *cyber assets and should serve as “a wake-up call to*
25 *those who have not taken this problem seriously.”.*

1 (7) *The National Cybersecurity Coordinator,*
2 *Howard Schmidt, stated on March 2, 2010, “we will*
3 *not defeat our cyber adversaries because they are*
4 *weakening, we will defeat them by becoming collec-*
5 *tively stronger, through stronger technology, a strong-*
6 *er cadre of security professionals, and stronger part-*
7 *nerships.”.*

8 (8) *According to the National Journal, Mike*
9 *McConnell, the former Director of National Intel-*
10 *ligence, told President Bush in May 2007 that if the*
11 *9/11 attackers had chosen computers instead of air-*
12 *planes as their weapons and had waged a massive as-*
13 *sault on a United States bank, the economic con-*
14 *sequences would have been “an order of magnitude*
15 *greater” than those caused by the physical attack on*
16 *the World Trade Center. Mike McConnell has subse-*
17 *quently referred to cybersecurity as the “soft under-*
18 *belly of this country”.*

19 (9) *Paul Kurtz, a partner and chief operating*
20 *officer of Good Harbor Consulting as well as a senior*
21 *advisor to the Obama Transition Team for cybersecu-*
22 *rity, has stated that the United States is unprepared*
23 *to respond to a “cyber-Katrina” and that “a massive*
24 *cyber disruption could have a cascading, long-term*

1 *impact without adequate co-ordination between gov-*
2 *ernment and the private sector”.*

3 (10) *According to the February 2003 National*
4 *Strategy to Secure Cyberspace, “our nation’s critical*
5 *infrastructures are composed of public and private in-*
6 *stitutions in the sectors of agriculture, food, water,*
7 *public health, emergency services, government, defense*
8 *industrial base, information and telecommunications,*
9 *energy, transportation, banking finance, chemicals*
10 *and hazardous materials, and postal and shipping.*
11 *Cyberspace is their nervous system the control system*
12 *of our country” and that “the cornerstone of Amer-*
13 *ica’s cyberspace security strategy is and will remain*
14 *a public-private partnership”.*

15 (11) *The Center for Strategic and International*
16 *Studies report on Cybersecurity for the 44th Presi-*
17 *dency concluded that (A) cybersecurity is now a*
18 *major national security problem for the United*
19 *States, (B) decisions and actions must respect privacy*
20 *and civil liberties, and (C) only a comprehensive na-*
21 *tional security strategy that embraces both the domes-*
22 *tic and international aspects of cybersecurity will*
23 *make us more secure. The report continued, stating*
24 *that the United States faces “a long-term challenge in*
25 *cyberspace from foreign intelligence agencies and*

1 *militaries, criminals, and others, and that losing this*
2 *struggle will wreak serious damage on the economic*
3 *health and national security of the United States”.*

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

11 (13) *The Cyber Strategic Inquiry 2008, spon-*
12 *sored by Business Executives for National Security*
13 *and executed by Booz Allen Hamilton, recommended*
14 *to “establish a single voice for cybersecurity within*
15 *government” concluding that the “unique nature of*
16 *cybersecurity requires a new leadership paradigm”.*

17 (14) *Alan Paller, the Director of Research at the*
18 *SANS Institute, testified before the Congress that*
19 *“Congress can reduce the threat of damage from these*
20 *new cyber attacks both against government and*
21 *against the critical infrastructure by shifting the gov-*
22 *ernment’s cyber security emphasis from report writ-*
23 *ing to automated, real-time defenses” and that “only*
24 *active White House leadership will get the job done”.*

1 (15) *A 2009 Partnership for Public Service*
2 *study and analysis reports concluded that “the Fed-*
3 *eral government will be unable to combat cyber*
4 *threats without a more coordinated, sustained effort*
5 *to increase cybersecurity expertise in the federal work-*
6 *force” and that “the President’s success in combating*
7 *these threats . . . must include building a vibrant,*
8 *highly trained and dedicated cybersecurity workforce*
9 *in this country”.*

10 **SEC. 3. DEFINITIONS.**

11 *In this Act:*

12 (1) *ADVISORY PANEL.*—*The term “Advisory*
13 *Panel” means the Cybersecurity Advisory Panel es-*
14 *tablished or designated under section 401.*

15 (2) *CYBERSECURITY.*—*The term “cybersecurity”*
16 *means information security (as defined in section*
17 *3532(b)(1) of title 44, United States Code).*

18 (3) *CYBERSECURITY PROFESSIONAL.*—*The term*
19 *“cybersecurity professional” means a person who*
20 *maintains a certification under section 101 of this*
21 *Act.*

22 (4) *INFORMATION SYSTEM.*—*The term “informa-*
23 *tion system” has the meaning given that term by sec-*
24 *tion 3532(b)(4) of title 44, United States Code, and*

1 *includes industrial control systems that are used for*
2 *purposes described in that section.*

3 (5) *INTERNET.*—*The term “Internet” has the*
4 *meaning given that term by section 4(4) of the High-*
5 *Performance Computing Act of 1991 (15 U.S.C.*
6 *5503(4)).*

7 (6) *UNITED STATES CRITICAL INFRASTRUCTURE*
8 *INFORMATION SYSTEM.*—*The term “United States*
9 *critical infrastructure information system” means an*
10 *information system designated under section 4 of this*
11 *Act.*

12 **SEC. 4. PROCEDURE FOR DESIGNATION OF CRITICAL IN-**
13 **FRASTRUCTURE INFORMATION SYSTEMS.**

14 (a) *ESTABLISHMENT OF DESIGNATION PROCEDURE.*—
15 *Within 90 days after the date of enactment of this Act, or*
16 *as soon thereafter as may be practicable, the President, in*
17 *consultation with sector coordinating councils, relevant gov-*
18 *ernment agencies, and regulatory entities, shall initiate a*
19 *rulemaking in accordance with the requirements of chapter*
20 *5 of title 5, United States Code, to establish a procedure*
21 *for the designation of any information system the infiltra-*
22 *tion, incapacitation, or disruption of which would have a*
23 *debilitating impact on national security, including na-*
24 *tional economic security and national public health or safe-*

1 *ty, as a critical infrastructure information system under*
 2 *this Act.*

3 (b) *THRESHOLD REQUIREMENTS.—The final rule, at*
 4 *a minimum, shall—*

5 (1) *set forth objective criteria that meet the*
 6 *standard in section (a) for such designations gen-*
 7 *erally;*

8 (2) *provide for emergency and temporary des-*
 9 *ignations when necessary and in the public interest;*

10 (3) *ensure the protection of confidential and pro-*
 11 *prietary information associated with nongovern-*
 12 *mental systems from disclosure;*

13 (4) *ensure the protection of classified and sen-*
 14 *sitive security information; and*

15 (5) *establish a procedure, in accordance with*
 16 *chapter 7 of title 5, United States Code, by which the*
 17 *owner or operator of an information system may ap-*
 18 *peal, or request modification of, the designation of*
 19 *that system or network as a critical infrastructure in-*
 20 *formation system under this Act.*

21 **TITLE I—WORKFORCE**

22 **DEVELOPMENT**

23 **SEC. 101. CERTIFICATION AND TRAINING OF CYBERSECU-**
 24 **RITY PROFESSIONALS.**

25 (a) *STUDY.—*

1 (1) *IN GENERAL.*—*The President shall enter into*
2 *an agreement with the National Academies to conduct*
3 *a comprehensive study of government, academic, and*
4 *private-sector accreditation, training, and certifi-*
5 *cation programs for personnel working in cybersecu-*
6 *rity. The agreement shall require that the National*
7 *Academies consult with sector coordinating councils*
8 *and relevant governmental agencies, regulatory enti-*
9 *ties, and nongovernmental organizations in the course*
10 *of the study.*

11 (2) *SCOPE.*—*The study shall include—*

12 (A) *an evaluation of the body of knowledge*
13 *and various skills that specific categories of per-*
14 *sonnel working in cybersecurity should possess in*
15 *order to secure information systems;*

16 (B) *an assessment of whether existing gov-*
17 *ernment, academic, and private-sector accredita-*
18 *tion, training, and certification programs pro-*
19 *vide the body of knowledge and skills described*
20 *in subparagraph (A); and*

21 (C) *any other factors that should be consid-*
22 *ered for any accreditation, training, and certifi-*
23 *cation programs.*

24 (3) *REPORT.*—*Not later than 1 year after the*
25 *date of enactment of this Act, the National Academies*

1 *shall submit to the President and the Congress a re-*
2 *port on the results of the study required by this sub-*
3 *section. The report shall include—*

4 *(A) findings regarding the state of cyberse-*
5 *curity accreditation, training, and certification*
6 *programs, including specific areas of deficiency*
7 *and demonstrable progress; and*

8 *(B) recommendations for the improvement*
9 *of cybersecurity accreditation, training, and cer-*
10 *tification programs.*

11 *(b) FEDERAL INFORMATION SYSTEMS.—Beginning no*
12 *later than 6 months after receiving the report under sub-*
13 *section (a)(3), the President, in close and regular consulta-*
14 *tion with sector coordinating councils and relevant govern-*
15 *mental agencies, regulatory entities, industry sectors, and*
16 *nongovernmental organizations, shall—*

17 *(1) develop and annually review and update—*

18 *(A) guidance for the identification and cat-*
19 *egorization of positions for personnel conducting*
20 *cybersecurity functions within the Federal gov-*
21 *ernment; and*

22 *(B) requirements for certification of per-*
23 *sonnel for categories identified under subpara-*
24 *graph (A); and*

1 (2) *annually evaluate compliance with the re-*
2 *quirements in paragraph (1)(B).*

3 (c) *UNITED STATES CRITICAL INFRASTRUCTURE IN-*
4 *FORMATION SYSTEMS.—*

5 (1) *IDENTIFICATION, CATEGORIZATION, AND CER-*
6 *TIFICATION OF POSITIONS.—Not later than 6 months*
7 *after receiving the report under section (a)(3), the*
8 *President, in close and regular consultation with sec-*
9 *tor coordinating councils and relevant governmental*
10 *agencies, regulatory entities, and nongovernmental or-*
11 *ganizations, shall require owners and operators of*
12 *United States critical infrastructure information sys-*
13 *tems to develop and annually review and update—*

14 (A) *guidance for the identification and cat-*
15 *egorization of positions for personnel conducting*
16 *cybersecurity functions within their respective*
17 *information systems; and*

18 (B) *requirements for certification of per-*
19 *sonnel for categories identified under subpara-*
20 *graph (A).*

21 (2) *ACCREDITATION, TRAINING, AND CERTIFI-*
22 *CATION PROGRAMS.—Not later than 6 months after*
23 *receiving the certification requirements submitted*
24 *under paragraph (1)(B), the President, in consulta-*
25 *tion with sector coordinating councils, relevant gov-*

1 *ernmental agencies, regulatory entities, and non-*
2 *governmental organizations, shall convene sector spe-*
3 *cific working groups to establish auditable private-*
4 *sector developed accreditation, training, and certifi-*
5 *cation programs for critical infrastructure informa-*
6 *tion system personnel working in cybersecurity.*

7 (3) *POSITIVE RECOGNITION.—Beginning no later*
8 *than 1 year after the President first convenes sector*
9 *specific working groups under paragraph (2), the*
10 *President shall—*

11 (A) *recognize and promote auditable pri-*
12 *vate-sector developed accreditation, training, and*
13 *certification programs established in subsection*
14 *(b); and*

15 (B) *on an ongoing basis, but not less fre-*
16 *quently than annually, review and reconsider*
17 *recognitions under subparagraph (A) in order to*
18 *account for advances in accreditation, training,*
19 *and certification programs for personnel working*
20 *in cybersecurity.*

21 (4) *UNITED STATES CRITICAL INFRASTRUCTURE*
22 *INFORMATION SYSTEMS COMPLIANCE.—*

23 (A) *IN GENERAL.—Beginning no later than*
24 *1 year after the President first recognizes a pro-*
25 *gram under paragraph (3)(A), and on a semi-*

1 *annual basis thereafter, the President shall re-*
2 *quire each owner or operator of a United States*
3 *critical infrastructure information system to re-*
4 *port the results of independent audits that evalu-*
5 *ate compliance with the accreditation, training,*
6 *and certification programs recognized under*
7 *paragraph (3).*

8 *(B) POSITIVE RECOGNITION.—The Presi-*
9 *dent, in consultation with sector coordinating*
10 *councils, relevant governmental agencies, and*
11 *regulatory entities, and with the consent of indi-*
12 *vidual companies, may publicly recognize those*
13 *owners and operators of United States critical*
14 *infrastructure information systems whose inde-*
15 *pendent audits demonstrate compliance with the*
16 *accreditation, training, and certification pro-*
17 *grams recognized under paragraph (3).*

18 *(C) COLLABORATIVE REMEDIATION.—The*
19 *President shall require owners or operators of*
20 *United States critical infrastructure information*
21 *systems that fail to demonstrate substantial com-*
22 *pliance with the accreditation, training, and cer-*
23 *tification programs recognized under paragraph*
24 *(3) through 2 consecutive independent audits, in*
25 *consultation with sector coordinating councils,*

1 *relevant governmental agencies, and regulatory*
2 *entities, to collaboratively develop and imple-*
3 *ment a remediation plan.*

4 *(d) REFERENCE LIST FOR CONSUMERS.—The Presi-*
5 *dent, in close and regular consultation with sector coordi-*
6 *nating councils and relevant governmental agencies, regu-*
7 *latory entities, and nongovernmental organizations, shall*
8 *annually—*

9 *(1) evaluate the cybersecurity accreditation,*
10 *training, and certification programs identified in this*
11 *section;*

12 *(2) identify those cybersecurity accreditation,*
13 *training, and certification programs whose rigor and*
14 *effectiveness are beneficial to cybersecurity; and*

15 *(3) publish a noncompulsory reference list of*
16 *those programs identified under paragraph (2).*

17 **SEC. 102. FEDERAL CYBER SCHOLARSHIP-FOR-SERVICE**
18 **PROGRAM.**

19 *(a) IN GENERAL.—The Director of the National*
20 *Science Foundation shall establish a Federal Cyber Schol-*
21 *arship-for-Service program to recruit and train the next*
22 *generation of information technology professionals and se-*
23 *curity managers for Federal, State, local, and tribal govern-*
24 *ments.*

1 **(b) PROGRAM DESCRIPTION AND COMPONENTS.**—*The*
2 *program shall—*

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

7 (2) *require scholarship recipients, as a condition*
8 *of receiving a scholarship under the program, to agree*
9 *to serve in a Federal, State, local, or tribal informa-*
10 *tion technology workforce for a period equal to the*
11 *length of the scholarship following graduation if of-*
12 *fered employment in that field by a Federal, State,*
13 *local, or tribal agency;*

14 (3) *provide a procedure by which the Foundation*
15 *or a Federal agency may, consistent with regulations*
16 *of the Office of Personnel Management, request and*
17 *fund security clearances for scholarship recipients;*

18 (4) *provide opportunities for students to receive*
19 *temporary appointments for meaningful employment*
20 *in the Federal information technology workforce dur-*
21 *ing school vacation periods and for internships;*

22 (5) *provide a procedure for identifying prom-*
23 *ising K–12 students for participation in summer*
24 *work and internship programs that would lead to cer-*

1 *tification of Federal information technology workforce*
2 *standards and possible future employment; and*

3 (6) *examine and develop, if appropriate, pro-*
4 *grams to promote computer security awareness in sec-*
5 *ondary and high school classrooms.*

6 (c) *HIRING AUTHORITY.—For purposes of any law or*
7 *regulation governing the appointment of individuals in the*
8 *Federal civil service, upon the successful completion of their*
9 *studies, students receiving a scholarship under the program*
10 *shall be hired under the authority provided for in section*
11 *213.3102(r) of title 5, Code of Federal Regulations, and be*
12 *exempt from competitive service. Upon satisfactory fulfill-*
13 *ment of the service term, such individuals may be converted*
14 *to a competitive service position without competition if the*
15 *individual meets the requirements for that position.*

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

18 (1) *be a citizen of the United States;*

19 (2) *demonstrate a commitment to a career in*
20 *improving the Nation’s cyber defenses; and*

21 (3) *have demonstrated a level of proficiency in*
22 *math or computer sciences.*

23 (e) *EVALUATION AND REPORT.—The Director shall*
24 *evaluate and report periodically to the Congress on the suc-*
25 *cess of recruiting individuals for the scholarships and on*

1 *hiring and retaining those individuals in the public sector*
2 *workforce.*

3 (f) *AUTHORIZATION OF APPROPRIATIONS.—There are*
4 *authorized to be appropriated to the National Science*
5 *Foundation to carry out this section—*

6 (1) *\$50,000,000 for fiscal year 2010;*

7 (2) *\$55,000,000 for fiscal year 2011;*

8 (3) *\$60,000,000 for fiscal year 2012;*

9 (4) *\$65,000,000 for fiscal year 2013; and*

10 (5) *\$70,000,000 for fiscal year 2014.*

11 **SEC. 103. CYBERSECURITY COMPETITION AND CHALLENGE.**

12 (a) *IN GENERAL.—The Director of the National Insti-*
13 *tute of Standards and Technology, directly or through ap-*
14 *propriate Federal entities, shall establish cybersecurity com-*
15 *petitions and challenges with cash prizes, and promulgate*
16 *rules for participation in such competitions and challenges,*
17 *in order to—*

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

21 (2) *stimulate innovation in basic and applied*
22 *cybersecurity research, technology development, and*
23 *prototype demonstration that has the potential for ap-*
24 *plication to the information technology activities of*
25 *the Federal Government.*

1 (b) *TYPES OF COMPETITIONS AND CHALLENGES.*—The
2 *Director shall establish different competitions and chal-*
3 *lenges targeting the following groups:*

4 (1) *Middle school students.*

5 (2) *High school students.*

6 (3) *Undergraduate students.*

7 (4) *Graduate students.*

8 (5) *Academic and research institutions.*

9 (c) *TOPICS.*—*In selecting topics for prize competitions,*
10 *the Director shall consult widely both within and outside*
11 *the Federal Government, and may empanel advisory com-*
12 *mittees.*

13 (d) *ADVERTISING.*—*The Director shall widely adver-*
14 *tise prize competitions, in coordination with the awareness*
15 *campaign under section 301, to encourage participation.*

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

22 (f) *ELIGIBILITY.*—*To be eligible to win a prize under*
23 *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 (a);

4 (2) shall have complied with all the requirements
5 under this section;

6 (3) in the case of a public or private entity, shall
7 be incorporated in and maintain a primary place of
8 business in the United States, and in the case of an
9 individual, whether participating singly or in a
10 group, 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 (h),
17 shall assemble a panel of qualified judges to select the win-
18 ner or winners of the prize competition. Judges for each
19 competition shall include individuals from the private sec-
20 tor. 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
25 with an individual who is a registered participant.

1 (h) *ADMINISTERING THE COMPETITION.*—*The Director*
2 *may enter into an agreement with a private, nonprofit enti-*
3 *ty to administer the prize competition, subject to the provi-*
4 *sions of this section.*

5 (i) *FUNDING.*—

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

13 (2) *FUNDING REQUIRED BEFORE PRIZE AN-*
14 *NOUNCED.*—*No prize may be announced until all the*
15 *funds needed to pay out the announced amount of the*
16 *prize have been appropriated or committed in writing*
17 *by a private source. The Director may increase the*
18 *amount of a prize after an initial announcement is*
19 *made under subsection (d) if—*

20 (A) *notice of the increase is provided in the*
21 *same manner as the initial notice of the prize;*
22 *and*

23 (B) *the funds needed to pay out the an-*
24 *nounced amount of the increase have been appro-*

1 *priated or committed in writing by a private*
2 *source.*

3 (3) *NOTICE REQUIRED FOR LARGE AWARDS.*—No
4 *prize competition under this section may offer a prize*
5 *in an amount greater than \$5,000,000 unless 30 days*
6 *have elapsed after written notice has been transmitted*
7 *to the Senate Committee on Commerce, Science, and*
8 *Transportation and the House of Representatives*
9 *Committee on Science and Technology.*

10 (4) *DIRECTOR'S APPROVAL REQUIRED FOR CER-*
11 *TAIN AWARDS.*—No prize competition under this sec-
12 *tion may result in the award of more than \$1,000,000*
13 *in cash prizes without the approval of the Director.*

14 (j) *USE OF FEDERAL INSIGNIA.*—A registered partici-
15 *pant in a competition under this section may use any Fed-*
16 *eral agency's name, initials, or insignia only after prior*
17 *review and written approval by the Director.*

18 (k) *COMPLIANCE WITH EXISTING LAW.*—The Federal
19 *Government shall not, by virtue of offering or providing a*
20 *prize under this section, be responsible for compliance by*
21 *registered participants in a prize competition with Federal*
22 *law, including licensing, export control, and non-prolifera-*
23 *tion laws and related regulations.*

24 (l) *AUTHORIZATION OF APPROPRIATIONS.*—There are
25 *authorized to be appropriated to the National Institute of*

1 *Standards and Technology to carry out this section*
2 *\$15,000,000 for each of fiscal years 2010 through 2014.*

3 **SEC. 104. CYBERSECURITY WORKFORCE PLAN.**

4 *(a) DEVELOPMENT OF PLAN.—Not later than 180 days*
5 *after the date of enactment of this Act and in every subse-*
6 *quent year, the head of each Federal agency, based on guid-*
7 *ance from the President, the Office of Personnel Manage-*
8 *ment, the Chief Human Capital Officers Council, and the*
9 *Chief Information Officers Council, shall develop a strategic*
10 *cybersecurity workforce plan as part of the agency perform-*
11 *ance plan required under section 1115 of title 31, United*
12 *States Code. The plan shall include—*

13 *(1) cybersecurity hiring projections, including*
14 *occupation and grade level, over a 2-year period;*

15 *(2) long-term and short-term strategic planning*
16 *to address critical skills deficiencies, including anal-*
17 *ysis of the numbers of and reasons for cybersecurity*
18 *employee attrition;*

19 *(3) recruitment strategies, including the use of*
20 *student internships, to attract highly qualified can-*
21 *didates from diverse backgrounds;*

22 *(4) an assessment of the sources and availability*
23 *of talent with needed expertise;*

24 *(5) streamlining the hiring process;*

1 (6) *a specific analysis of the capacity of the*
2 *agency workforce to manage contractors who are per-*
3 *forming cybersecurity work on behalf of the Federal*
4 *government;*

5 (7) *an analysis of the barriers to recruiting and*
6 *hiring cybersecurity talent, including compensation,*
7 *classification, hiring flexibilities, and the hiring proc-*
8 *ess, and recommendations to overcome those barriers;*
9 *and,*

10 (8) *a cybersecurity-related training and develop-*
11 *ment plan to enhance or keep current the knowledge*
12 *level of employees.*

13 (b) *HIRING PROJECTIONS.—Each Federal agency shall*
14 *make hiring projections made under its strategic cybersecu-*
15 *rity workforce plan available to the public, including on*
16 *its website.*

17 (c) *CLASSIFICATION.—Based on the agency analyses*
18 *and recommendations made under subsection (a)(7) of this*
19 *section and other relevant information, the President or the*
20 *President’s designee, in consultation with affected Federal*
21 *agencies and councils, shall coordinate the establishment of*
22 *new job classifications for cybersecurity functions in gov-*
23 *ernment and certification requirements for each job cat-*
24 *egory.*

1 **SEC. 105. MEASURES OF CYBERSECURITY HIRING EFFEC-**
2 **TIVENESS.**

3 (a) *IN GENERAL.*—Each agency shall measure and col-
4 lect information on cybersecurity hiring effectiveness with
5 respect to the following:

6 (1) *RECRUITING AND HIRING.*—

7 (A) *Ability to reach and recruit well-quali-*
8 *fied talent from diverse talent pools.*

9 (B) *Use and impact of special hiring au-*
10 *thorities and flexibilities to recruit most quali-*
11 *fied applicants, including the use of student in-*
12 *ternship and scholarship programs as a talent*
13 *pool for permanent hires.*

14 (C) *Use and impact of special hiring au-*
15 *thorities and flexibilities to recruit diverse can-*
16 *didates, including veteran, minority, and dis-*
17 *abled candidates.*

18 (D) *The age, educational level, and source of*
19 *applicants.*

20 (2) *HIRING MANAGER ASSESSMENT.*—

21 (A) *Manager satisfaction with the quality of*
22 *the applicants interviewed and new hires.*

23 (B) *Manager satisfaction with the match be-*
24 *tween the skills of newly hired individuals and*
25 *the needs of the agency.*

1 (C) *Manager satisfaction with the hiring*
2 *process and hiring outcomes.*

3 (D) *Mission-critical deficiencies closed by*
4 *new hires and the connection between mission-*
5 *critical deficiencies and annual agency perform-*
6 *ance.*

7 (E) *Manager satisfaction with the length of*
8 *time to fill a position.*

9 (3) *APPLICANT ASSESSMENT.—Applicant satis-*
10 *faction with the hiring process (including clarity of*
11 *job announcement, reasons for withdrawal of applica-*
12 *tion should that apply, user-friendliness of the appli-*
13 *cation process, communication regarding status of ap-*
14 *plication, and timeliness of job offer).*

15 (4) *NEW HIRE ASSESSMENT.—*

16 (A) *New hire satisfaction with the hiring*
17 *process (including clarity of job announcement,*
18 *user-friendliness of the application process, com-*
19 *munication regarding status of application, and*
20 *timeliness of hiring decision).*

21 (B) *Satisfaction with the onboarding expe-*
22 *rience (including timeliness of onboarding after*
23 *the hiring decision, welcoming and orientation*
24 *processes, and being provided with timely and*

1 *useful new employee information and assist-*
2 *ance).*

3 *(C) New hire attrition, including by per-*
4 *formance level and occupation.*

5 *(D) Investment in training and develop-*
6 *ment for employees during their first year of em-*
7 *ployment.*

8 *(E) Exit interview results.*

9 *(F) Other indicators and measures as re-*
10 *quired by the Office of Personnel Management.*

11 ***(b) REPORTS.—***

12 *(1) IN GENERAL.—Each agency shall submit the*
13 *information collected under subsection (a) to the Of-*
14 *ice of Personnel Management annually in accordance*
15 *with the regulations prescribed under subsection (c).*

16 ***(2) AVAILABILITY OF RECRUITING AND HIRING***
17 ***INFORMATION.—Each year the Office of Personnel***
18 ***Management shall provide the information received***
19 ***under paragraph (1) in a consistent format to allow***
20 ***for a comparison of hiring effectiveness and experi-***
21 ***ence across demographic groups and agencies to—***

22 ***(A) the Congress before that information is***
23 ***made publicly available; and***

1 (B) the public on the website of the Office
2 within 90 days after receipt of the information
3 under subsection (b)(1).

4 (c) *REGULATIONS.*—Not later than 180 days after the
5 date of enactment of this Act, the Director of the Office of
6 Personnel Management shall prescribe regulations estab-
7 lishing the methodology, timing, and reporting of the data
8 described in subsection (a).

9 **TITLE II—PLANS AND**
10 **AUTHORITY**

11 **SEC. 201. CYBERSECURITY RESPONSIBILITIES AND AU-**
12 **THORITIES.**

13 (a) *IN GENERAL.*—The President shall—

14 (1) within 180 days after the date of enactment
15 of this Act, after notice and opportunity for public
16 comment, develop and implement a comprehensive
17 national cybersecurity strategy, which shall include—

18 (A) a long-term vision of the Nation’s cyber-
19 security future; and

20 (B) a plan that addresses all aspects of na-
21 tional security, as it relates to cybersecurity, in-
22 cluding the proactive engagement of, and collabo-
23 ration between, the Federal government and the
24 private sector;

1 (2) *in consultation with sector coordinating*
2 *councils and relevant governmental agencies, regu-*
3 *latory entities, and nongovernmental organizations,*
4 *review critical functions likely to be impacted by a*
5 *cyber attack and develop a strategy for the acquisi-*
6 *tion, storage, and periodic replacement of assets to*
7 *support those functions;*

8 (3) *through the Office of Science and Technology*
9 *Policy, direct an annual review of all Federal cyber*
10 *technology research and development investments; and*

11 (4) *through the Office of Personnel Management,*
12 *promulgate rules for Federal professional responsibil-*
13 *ities regarding cybersecurity, and provide to the Con-*
14 *gress an annual report on Federal agency compliance*
15 *with those rules.*

16 (b) *COLLABORATIVE EMERGENCY RESPONSE AND RES-*
17 *TORATION.—The President—*

18 (1) *shall, in collaboration with owners and oper-*
19 *ators of United States critical infrastructure informa-*
20 *tion systems, sector coordinating councils and rel-*
21 *evant governmental agencies, regulatory entities, and*
22 *nongovernmental organizations, develop and rehearse*
23 *detailed response and restoration plans that clarify*
24 *specific roles, responsibilities, and authorities of gov-*
25 *ernment and private sector actors during cybersecu-*

1 *rity emergencies, and that identify the types of events*
2 *and incidents that would constitute a cybersecurity*
3 *emergency;*

4 *(2) may, in the event of an immediate threat to*
5 *strategic national interests involving compromised*
6 *Federal Government or United States critical infra-*
7 *structure information systems—*

8 *(A) declare a cybersecurity emergency; and*

9 *(B) implement the collaborative emergency*
10 *response and restoration plans developed under*
11 *paragraph (1);*

12 *(3) shall, in the event of a declaration of a cyber-*
13 *security emergency—*

14 *(A) within 48 hours submit to Congress a*
15 *report in writing setting forth—*

16 *(i) the circumstances necessitating the*
17 *emergency declaration; and*

18 *(ii) the estimated scope and duration*
19 *of the emergency; and*

20 *(B) so long as the cybersecurity emergency*
21 *declaration remains in effect, report to the Con-*
22 *gress periodically, but in no event less frequently*
23 *than once every 30 days, on the status of emer-*
24 *gency as well as on the scope and duration of the*
25 *emergency.*

1 (c) *RULE OF CONSTRUCTION.*—*This section does not*
2 *authorize, and shall not be construed to authorize, an ex-*
3 *pansion of existing Presidential authorities.*

4 **SEC. 202. BIENNIAL CYBER REVIEW.**

5 (a) *IN GENERAL.*—*Beginning with 2010 and in every*
6 *second year thereafter, the President, or the President’s des-*
7 *ignee, shall complete a review of the cyber posture of the*
8 *United States, including an unclassified summary of roles,*
9 *missions, accomplishments, plans, and programs. The re-*
10 *view shall include a comprehensive examination of the cyber*
11 *strategy, force structure, personnel, modernization plans,*
12 *infrastructure, budget plan, the Nation’s ability to recover*
13 *from a cyber emergency, 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 estab-*
16 *lishing a revised cyber program for the next 2 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 estab-*
21 *lished or designated under section 401, on an ongoing*
22 *basis, of the work undertaken in the conduct of the re-*
23 *view.*

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 President's*
2 *designee, the Panel's assessment of work undertaken*
3 *in the conduct of the review as of that date and shall*
4 *include in the assessment the recommendations of the*
5 *Panel for improvements to the review, including rec-*
6 *ommendations for additional matters to be covered in*
7 *the review.*

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

14 *(d) REPORT.—Not later than September 30, 2010, and*
15 *every 2 years thereafter, the President, or the President's*
16 *designee, shall submit to the relevant congressional Commit-*
17 *tees a comprehensive report on the review. The report shall*
18 *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 pub-*
22 *lic and private sectors best suited to implement that*
23 *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. 203. CYBERSECURITY DASHBOARD PILOT PROJECT.**

9 *The Secretary of Commerce shall—*

10 (1) *in consultation with the Office of Manage-*
11 *ment and Budget, develop a plan within 90 days*
12 *after the date of enactment of this Act to implement*
13 *a system to provide dynamic, comprehensive, real-*
14 *time cybersecurity status and vulnerability informa-*
15 *tion of all Federal Government information systems*
16 *managed by the Department of Commerce, including*
17 *an inventory of such, vulnerabilities of such systems,*
18 *and corrective action plans for those vulnerabilities;*

19 (2) *implement the plan within 1 year after the*
20 *date of enactment of this Act; and*

21 (3) *submit a report to the Congress on the imple-*
22 *mentation of the plan.*

23 **SEC. 204. NIST CYBERSECURITY GUIDANCE.**

24 (a) *IN GENERAL.—Beginning no later than 1 year*
25 *after the date of enactment of this Act, the National Insti-*

1 *tute of Standards and Technology, in close and regular con-*
2 *sultation with sector coordinating councils and relevant*
3 *governmental agencies, regulatory entities, and nongovern-*
4 *mental organizations, shall—*

5 (1) *recognize and promote auditable, private sec-*
6 *tor developed cybersecurity risk measurement tech-*
7 *niques, risk management measures and best practices*
8 *for all Federal Government and United States critical*
9 *infrastructure information systems; and*

10 (2) *on an ongoing basis, but not less frequently*
11 *than semi-annually, review and reconsider its rec-*
12 *ognitions under paragraph (1) in order to account for*
13 *advances in cybersecurity risk measurement tech-*
14 *niques, risk management measures, and best prac-*
15 *tices.*

16 (b) *FEDERAL INFORMATION SYSTEMS.—Within 1 year*
17 *after the National Institute of Standards and Technology*
18 *issues guidance under subsection (a)(1), the President shall*
19 *require all Federal departments and agencies to measure*
20 *their risk in each operating unit using the techniques recog-*
21 *nized under subsection (a) and to comply with or exceed*
22 *the cybersecurity risk management measures and best prac-*
23 *tices recognized under subsection (a).*

24 (c) *UNITED STATES CRITICAL INFRASTRUCTURE IN-*
25 *FORMATION SYSTEMS.—*

1 (1) *IN GENERAL.*—*On the earlier of the date on*
2 *which the final rule in the rulemaking required by*
3 *section 4 is promulgated, or 1 year after the President*
4 *first recognizes the cybersecurity risk measurement*
5 *techniques, risk management measures and best prac-*
6 *tices under subsection (a), and on a semi-annual*
7 *basis thereafter, the President shall require each*
8 *owner or operator of a United States critical infra-*
9 *structure information system to report the results of*
10 *independent audits that evaluate compliance with cy-*
11 *bersecurity risk measurement techniques, risk man-*
12 *agement measures, and best practices recognized*
13 *under subsection (a).*

14 (2) *POSITIVE RECOGNITION.*—*The President, in*
15 *consultation with sector coordinating councils, rel-*
16 *evant governmental agencies, and regulatory entities,*
17 *and with the consent of individual companies, may*
18 *publicly recognize those owners and operators of*
19 *United States critical infrastructure information sys-*
20 *tems whose independent audits demonstrate compli-*
21 *ance with cybersecurity risk measurement techniques,*
22 *risk management measures, and best practices recog-*
23 *nized under subsection (a);*

24 (3) *COLLABORATIVE REMEDIATION.*—*The Presi-*
25 *dent shall require owners or operators of United*

1 *States critical infrastructure information systems*
2 *that fail to demonstrate substantial compliance with*
3 *cybersecurity risk measurement techniques, risk man-*
4 *agement measures, and best practices recognized*
5 *under subsection (a) through 2 consecutive inde-*
6 *pendent audits, in consultation with sector coordi-*
7 *nating councils, relevant governmental agencies, and*
8 *regulatory entities, to collaboratively develop and im-*
9 *plement a remediation plan.*

10 (d) *INTERNATIONAL STANDARDS DEVELOPMENT.*—

11 *Within 1 year after the date of enactment of this Act, the*
12 *Director, in coordination with the Department of State and*
13 *other relevant governmental agencies and regulatory enti-*
14 *ties, and in consultation with sector coordinating councils*
15 *and relevant nongovernmental organizations, shall—*

16 (1) *direct United States cybersecurity efforts be-*
17 *fore all international standards development bodies*
18 *related to cybersecurity;*

19 (2) *develop and implement a strategy to engage*
20 *international standards bodies with respect to the de-*
21 *velopment of technical standards related to cybersecu-*
22 *rity; and*

23 (3) *submit the strategy to the Congress.*

24 (e) *CRITERIA FOR FEDERAL INFORMATION SYS-*
25 *TEMS.*—*Notwithstanding any other provision of law (in-*

1 *cluding any Executive Order), rule, regulation, or guideline*
 2 *pertaining to the distinction between national security sys-*
 3 *tems and civilian agency systems, the Institute shall adopt*
 4 *a risk-based approach in the development of Federal cyber-*
 5 *security guidance for Federal information systems.*

6 *(f) FCC BROADBAND CYBERSECURITY REVIEW.—*
 7 *Within 1 year after the date of enactment of this Act, the*
 8 *Federal Communications Commission shall report to Con-*
 9 *gress on effective and efficient means to ensure the cyberse-*
 10 *curity of commercial broadband networks as related to pub-*
 11 *lic safety, consumer welfare, healthcare, education, energy,*
 12 *government, security and other national purposes. This re-*
 13 *port should also consider consumer education and outreach*
 14 *programs to assist individuals in protecting their home and*
 15 *personal computers and other devices.*

16 *(g) ELIMINATION OF DUPLICATIVE REQUIREMENTS.—*
 17 *The President shall direct the National Institute of Stand-*
 18 *ards and Technology and other appropriate Federal agen-*
 19 *cies to identify private sector entities already required to*
 20 *report their compliance with cybersecurity laws, directives,*
 21 *and regulations to streamline compliance with duplicative*
 22 *reporting requirements.*

23 **SEC. 205. LEGAL FRAMEWORK REVIEW AND REPORT.**

24 *(a) IN GENERAL.—Within 1 year after the date of en-*
 25 *actment of this Act, the Comptroller General shall complete*

1 *a comprehensive review of the Federal statutory and legal*
2 *framework applicable to cybersecurity-related activities in*
3 *the United States, including—*

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

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

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

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

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

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

16 (7) *section 552 of title 5, United States Code;*

17 (8) *the Federal Advisory Committee Act (5*
18 *U.S.C. App.);*

19 (9) *any other Federal law bearing upon cyberse-*
20 *curity-related activities; and*

21 (10) *any applicable Executive Order or agency*
22 *rule, regulation, or guideline.*

23 (b) *REPORT.—Upon completion of the review the*
24 *Comptroller General shall submit a report to the Congress*
25 *containing the Comptroller General’s, findings, conclusions,*

1 *and recommendations regarding changes needed to advance*
2 *cybersecurity and protect civil liberties in light of new cy-*
3 *bersecurity measures.*

4 **SEC. 206. JOINT INTELLIGENCE THREAT AND VULNER-**
5 **ABILITY ASSESSMENT.**

6 *The Director of National Intelligence, the Secretary of*
7 *Commerce, the Secretary of Homeland Security, the Attor-*
8 *ney General, the Secretary of Defense, and the Secretary*
9 *of State shall submit to the Congress a joint assessment of,*
10 *and report on, cybersecurity threats to and vulnerabilities*
11 *of Federal information systems and United States critical*
12 *infrastructure information systems.*

13 **SEC. 207. INTERNATIONAL NORMS AND CYBERSECURITY**
14 **DETERRENCE MEASURES.**

15 *The President shall—*

16 *(1) work with representatives of foreign govern-*
17 *ments, private sector entities, and nongovernmental*
18 *organizations—*

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 *States critical infrastructure information systems and sub-*
2 *mit a report to the Congress on the evaluation.*

3 (b) *SECURITY CLEARANCES.—To the extent deter-*
4 *mined by the President to be necessary to enhance public-*
5 *private information sharing and cybersecurity collabora-*
6 *tion, the President may—*

7 (1) *grant additional security clearances to own-*
8 *ers and operators of United States critical infrastruc-*
9 *ture information systems; and*

10 (2) *delegate original classification authority to*
11 *appropriate Federal officials on matters related to cy-*
12 *bersecurity.*

13 **SEC. 210. AUTHENTICATION AND CIVIL LIBERTIES REPORT.**

14 *Within 1 year after the date of enactment of this Act,*
15 *the President, or the President’s designee, in consultation*
16 *with sector coordinating councils, relevant governmental*
17 *agencies, regulatory entities, and nongovernmental organi-*
18 *zations, shall review, and report to Congress, on the feasi-*
19 *bility of an identity management and authentication pro-*
20 *gram, with the appropriate civil liberties and privacy pro-*
21 *tections, for Federal government and United States critical*
22 *infrastructure information systems.*

1 **SEC. 211. REPORT ON EVALUATION OF CERTAIN IDENTITY**
 2 **AUTHENTICATION FUNCTIONALITIES.**

3 (a) *IN GENERAL.*—Not later than 90 days after the
 4 date of enactment of this Act, the National Institute of
 5 Standards and Technology shall issue a public report evalu-
 6 ating identity authentication solutions to determine the
 7 necessary level of functionality and privacy protection,
 8 based on risk, commensurate with the level of data assur-
 9 ance and sensitivity, as defined by OMB e-Authentication
 10 Guidance Memorandum 04-04 (OMB 04-04).

11 (b) *CONTENTS.*—The report shall—

12 (1) assess strategies and best practices for map-
 13 ping the 4 authentication levels with authentication
 14 functionalities appropriate for each level; and

15 (2) address specifically authentication levels and
 16 appropriate functionalities necessary and available
 17 for the protection of electronic medical records and
 18 health information.

19 **TITLE III—CYBERSECURITY**
 20 **KNOWLEDGE DEVELOPMENT**

21 **SEC. 301. PROMOTING CYBERSECURITY AWARENESS AND**
 22 **EDUCATION.**

23 (a) *IN GENERAL.*—The Secretary of Commerce, in con-
 24 sultation with sector coordinating councils, relevant govern-
 25 mental agencies, regulatory entities, and nongovernmental

1 organizations, shall develop and implement a national cy-
2 bersecurity awareness campaign that—

3 (1) calls a new generation of Americans to serv-
4 ice in the field of cybersecurity;

5 (2) heightens public awareness of cybersecurity
6 issues and concerns;

7 (3) communicates the Federal Government's role
8 in securing the Internet and protecting privacy and
9 civil liberties with respect to Internet-related activi-
10 ties; and

11 (4) utilizes public and private sector means of
12 providing information to the public, including public
13 service announcements.

14 (b) *EDUCATIONAL PROGRAMS.*—The Secretary of Edu-
15 cation, in consultation with State school superintendents,
16 relevant Federal agencies, industry sectors, and nongovern-
17 mental organizations, shall identify and promote age ap-
18 propriate information and programs for grades K-12 re-
19 garding cyber safety, cybersecurity, and cyber ethics.

20 **SEC. 302. FEDERAL CYBERSECURITY RESEARCH AND DE-**
21 **VELOPMENT.**

22 (a) *FUNDAMENTAL CYBERSECURITY RESEARCH.*—The
23 Director of the National Science Foundation, in coordina-
24 tion with the Office of Science and Technology Policy, and
25 drawing on the recommendations of the Office of Science

1 *and Technology Policy's annual review of all Federal cyber*
2 *technology research and development investments required*
3 *by section 201(a)(3), shall develop a national cybersecurity*
4 *research and development plan. The plan shall encourage*
5 *computer and information science and engineering research*
6 *to meet the following challenges in cybersecurity:*

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

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

13 (3) *How to test and verify that software obtained*
14 *from a third party correctly implements stated*
15 *functionality, and only that functionality.*

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

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

23 (6) *How to determine the origin of a message*
24 *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 (9) *How improved consumer education and dig-*
6 *ital literacy initiatives can address human factors*
7 *that contribute to cybersecurity.*

8 (b) *SECURE CODING RESEARCH.*—*The Director shall*
9 *support research that evaluates selected secure coding edu-*
10 *cation and improvement programs. The Director shall also*
11 *support research on new methods of integrating secure cod-*
12 *ing improvement into the core curriculum of computer*
13 *science programs and of other programs where graduates*
14 *have a substantial probability of developing software after*
15 *graduation.*

16 (c) *ASSESSMENT OF SECURE CODING EDUCATION IN*
17 *COLLEGES AND UNIVERSITIES.*—*Within 1 year after the*
18 *date of enactment of this Act, the Director shall submit to*
19 *the Senate Committee on Commerce, Science, and Trans-*
20 *portation and the House of Representatives Committee on*
21 *Science and Technology a report on the state of secure cod-*
22 *ing education in America's colleges and universities for*
23 *each school that received National Science Foundation*
24 *funding in excess of \$1,000,000 during fiscal year 2008. The*
25 *report shall include—*

1 (1) *the number of students who earned under-*
2 *graduate degrees in computer science or in each other*
3 *program where graduates have a substantial prob-*
4 *ability of being engaged in software design or develop-*
5 *ment after graduation;*

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

10 (3) *descriptions of the length and content of the*
11 *education and improvement programs and an evalua-*
12 *tion of the effectiveness of those programs based on the*
13 *students' scores on standard tests of secure coding and*
14 *design skills.*

15 (d) *CYBERSECURITY MODELING AND TESTBEDS.—*
16 *Within 1 year after the date of enactment of this Act, the*
17 *Director shall conduct a review of existing cybersecurity*
18 *testbeds. Based on the results of that review, the Director*
19 *shall establish a program to award grants to institutions*
20 *of higher education to establish cybersecurity testbeds capa-*
21 *ble of realistic modeling of real-time cyber attacks and de-*
22 *fenses. The purpose of this program is to support the rapid*
23 *development of new cybersecurity defenses, techniques, and*
24 *processes by improving understanding and assessing the*
25 *latest technologies in a real-world environment. The testbeds*

1 *shall be sufficiently large in order to model the scale and*
2 *complexity of real world networks and environments.*

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

7 *(1) by striking “and” after the semicolon in sub-*
8 *paragraph (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*
13 *at the heart of inter-network communications*
14 *and data exchange;*

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

17 *“(i) programming languages and sys-*
18 *tems that include fundamental security fea-*
19 *tures;*

20 *“(ii) portable or reusable code that re-*
21 *mains secure when deployed in various en-*
22 *vironments;*

23 *“(iii) verification and validation tech-*
24 *nologies to ensure that requirements and*
25 *specifications have been implemented; and*

1 “(iv) models for comparison and
2 metrics to assure that required standards
3 have been met;

4 “(L) holistic system security that—

5 “(i) addresses the building of secure
6 systems from trusted and untrusted compo-
7 nents;

8 “(ii) proactively reduces
9 vulnerabilities;

10 “(iii) addresses insider threats; and

11 “(iv) supports privacy in conjunction
12 with improved security;

13 “(M) monitoring and detection; and

14 “(N) mitigation and rapid recovery meth-
15 ods.”.

16 (f) *NSF COMPUTER AND NETWORK SECURITY*

17 *GRANTS.*—Section 4(a)(3) of the Cybersecurity Research
18 and Development Act (15 U.S.C. 7403(a)(3)) is amended—

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

20 (2) by striking “2007.” in subparagraph (E)
21 and inserting “2007;”; and

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

23 “(F) \$150,000,000 for fiscal year 2010;

24 “(G) \$155,000,000 for fiscal year 2011;

25 “(H) \$160,000,000 for fiscal year 2012;

1 “(I) \$165,000,000 for fiscal year 2013; and
2 “(J) \$170,000,000 for fiscal year 2014.”.

3 (g) *COMPUTER AND NETWORK SECURITY CENTERS.*—
4 *Section 4(b)(7) of such Act (15 U.S.C. 7403(b)(7)) is*
5 *amended—*

6 (1) *by striking “and” in subparagraph (D);*
7 (2) *by striking “2007.” in subparagraph (E)*
8 *and inserting “2007;”; and*
9 (3) *by adding at the end of the following:*

10 “(F) \$50,000,000 for fiscal year 2010;
11 “(G) \$52,000,000 for fiscal year 2011;
12 “(H) \$54,000,000 for fiscal year 2012;
13 “(I) \$56,000,000 for fiscal year 2013; and
14 “(J) \$58,000,000 for fiscal year 2014.”.

15 (h) *COMPUTER AND NETWORK SECURITY CAPACITY*
16 *BUILDING GRANTS.*—*Section 5(a)(6) of such Act (15 U.S.C.*
17 *7404(a)(6)) is amended—*

18 (1) *by striking “and” in subparagraph (D);*
19 (2) *by striking “2007.” in subparagraph (E)*
20 *and inserting “2007;”; and*
21 (3) *by adding at the end of the following:*

22 “(F) \$40,000,000 for fiscal year 2010;
23 “(G) \$42,000,000 for fiscal year 2011;
24 “(H) \$44,000,000 for fiscal year 2012;
25 “(I) \$46,000,000 for fiscal year 2013; and

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

2 (i) *SCIENTIFIC AND ADVANCED TECHNOLOGY ACT*
3 *GRANTS*.—Section 5(b)(2) of such Act (15 U.S.C.
4 7404(b)(2)) is amended—

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

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

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

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

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

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

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

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

14 (j) *GRADUATE TRAINEESHIPS IN COMPUTER AND NET-*
15 *WORK SECURITY RESEARCH*.—Section 5(c)(7) of such Act
16 (15 U.S.C. 7404(c)(7)) is amended—

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

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

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

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

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

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

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

25 “(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 in-
 4 serting “2007 and for each of fiscal years 2010 through
 5 2014.”.

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

10 (1) by striking “and” after the semicolon in sub-
 11 paragraph (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 for
 17 computer networks and common user interfaces
 18 to systems; and”.

19 **SEC. 303. DEVELOPMENT OF CURRICULA FOR INCOR-**
 20 **PORATING CYBERSECURITY INTO EDU-**
 21 **CATIONAL PROGRAMS FOR FUTURE INDUS-**
 22 **TRIAL CONTROL SYSTEM DESIGNERS.**

23 (a) *IN GENERAL.*—The Director of the National
 24 Science Foundation shall establish a grant program to fund
 25 public and private educational institutions to develop grad-

1 uate and undergraduate level curricula that address cyber-
 2 security in modern industrial control systems. In admin-
 3 istering the program, the Director—

4 (1) shall establish such requirements for the sub-
 5 mission of applications containing such information,
 6 commitments, and assurances as the Director finds
 7 necessary and appropriate;

8 (2) shall award the grants on a competitive
 9 basis;

10 (3) shall require grant recipients to make the de-
 11 veloped curricula and related materials to other pub-
 12 lic and private educational institutions; and

13 (4) may make up to 3 grants per year.

14 (b) *AUTHORIZATION OF APPROPRIATIONS.*—There are
 15 authorized to be appropriated to the Director to carry out
 16 the grant program under this section \$2,000,000 for each
 17 of fiscal years 2011 and 2012.

18 **TITLE IV—PUBLIC-PRIVATE**
 19 **COLLABORATION**

20 **SEC. 401. CYBERSECURITY ADVISORY PANEL.**

21 (a) *IN GENERAL.*—The President shall establish or des-
 22 ignate a Cybersecurity Advisory Panel.

23 (b) *QUALIFICATIONS.*—The President—

24 (1) shall appoint as members of the panel rep-
 25 resentatives of industry, academic, non-profit organi-

1 *zations, interest groups and advocacy organizations,*
2 *and State and local governments who are qualified to*
3 *provide advice and information on cybersecurity re-*
4 *search, development, demonstrations, education, per-*
5 *sonnel, technology transfer, commercial application,*
6 *or societal and civil liberty concerns; and*

7 *(2) may seek and give consideration to rec-*
8 *ommendations from the Congress, industry, the cyber-*
9 *security community, the defense community, State*
10 *and local governments, and other appropriate organi-*
11 *zations.*

12 *(c) DUTIES.—The panel shall advise the President on*
13 *matters relating to the national cybersecurity program and*
14 *strategy and shall assess—*

15 *(1) trends and developments in cybersecurity*
16 *science research and development;*

17 *(2) progress made in implementing the strategy;*

18 *(3) the need to revise the strategy;*

19 *(4) the readiness and capacity of the Federal*
20 *and national workforces to implement the national*
21 *cybersecurity program and strategy, and the steps*
22 *necessary to improve workforce readiness and capac-*
23 *ity;*

1 (5) *the balance among the components of the na-*
2 *tional strategy, including funding for program com-*
3 *ponents;*

4 (6) *whether the strategy, priorities, and goals are*
5 *helping to maintain United States leadership and de-*
6 *fense in cybersecurity;*

7 (7) *the management, coordination, implementa-*
8 *tion, and activities of the strategy;*

9 (8) *whether the concerns of Federal, State, and*
10 *local law enforcement entities are adequately ad-*
11 *ressed; and*

12 (9) *whether societal and civil liberty concerns*
13 *are adequately addressed.*

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

18 (e) *TRAVEL EXPENSES OF NON-FEDERAL MEM-*
19 *BERS.*—*Non-Federal members of the panel, while attending*
20 *meetings of the panel or while otherwise serving at the re-*
21 *quest of the head of the panel while away from their homes*
22 *or regular places of business, may be allowed travel ex-*
23 *penses, including per diem in lieu of subsistence, as author-*
24 *ized by section 5703 of title 5, United States Code, for indi-*
25 *viduals in the government serving without pay. Nothing in*

1 *this subsection shall be construed to prohibit members of*
2 *the panel who are officers or employees of the United States*
3 *from being allowed travel expenses, including per diem in*
4 *lieu of subsistence, in accordance with law.*

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

8 **SEC. 402. STATE AND REGIONAL CYBERSECURITY EN-**
9 **HANCEMENT PROGRAM.**

10 (a) *CREATION AND SUPPORT OF CYBERSECURITY CEN-*
11 *TERS.*—The Secretary of Commerce shall provide assistance
12 *for the creation and support of Regional Cybersecurity Cen-*
13 *ters for the promotion of private sector developed cybersecu-*
14 *rity risk measurement techniques, risk management meas-*
15 *ures, and best practices. Each Center shall be affiliated with*
16 *a United States-based nonprofit institution or organiza-*
17 *tion, or consortium thereof, that applies for and is awarded*
18 *financial assistance under this section.*

19 (b) *PURPOSE.*—The purpose of the Centers is to en-
20 *hance the cybersecurity of small and medium sized busi-*
21 *nesses in the United States through—*

22 (1) *the promotion of private sector developed cy-*
23 *bersecurity risk measurement techniques, risk man-*
24 *agement measures, and best practices to small- and*

1 *medium-sized companies throughout the United*
2 *States;*

3 (2) *the voluntary participation of individuals*
4 *from industry, universities, State governments, other*
5 *Federal agencies, and, when appropriate, the Institute*
6 *in cooperative technology transfer activities in accord-*
7 *ance with existing technology transfer rules and intel-*
8 *lectual property protection measures;*

9 (3) *efforts to make new cybersecurity technology,*
10 *standards, and processes usable by United States-*
11 *based small- and medium-sized companies;*

12 (4) *the active dissemination of scientific, engi-*
13 *neering, technical, and management information*
14 *about cybersecurity to industrial firms, including*
15 *small- and medium-sized companies;*

16 (5) *the utilization, when appropriate, of the ex-*
17 *pertise and capability that exists in Federal labora-*
18 *tories other than the Institute; and*

19 (6) *the performance of these and related activi-*
20 *ties in a manner that supplements or coordinates*
21 *with, and does not compete with or duplicate, private*
22 *sector activities.*

23 (c) *ACTIVITIES.—The Centers shall—*

24 (1) *disseminate cybersecurity technologies, stand-*
25 *ards, and processes based on research by the Institute*

1 *for the purpose of demonstrations and technology*
2 *transfer;*

3 (2) *actively transfer and disseminate private sec-*
4 *tor developed cybersecurity risk measurement tech-*
5 *niques, risk management measures, and best practices*
6 *to protect against and mitigate the risk of cyber at-*
7 *tacks to a wide range of companies and enterprises,*
8 *particularly small- and medium-sized businesses; and*

9 (3) *make loans, on a selective, short-term basis,*
10 *of items of advanced protective cybersecurity measures*
11 *to small businesses with less than 100 employees.*

12 (c) *DURATION AND AMOUNT OF SUPPORT; PROGRAM*
13 *DESCRIPTIONS; APPLICATIONS; MERIT REVIEW; EVALUA-*
14 *TIONS OF ASSISTANCE.—*

15 (1) *FINANCIAL SUPPORT.—The Secretary may*
16 *provide financial support, not to exceed 50 percent of*
17 *the Center’s annual operating and maintenance costs,*
18 *to any Center for a period not to exceed 6 years (ex-*
19 *cept as provided in paragraph (5)(D)).*

20 (2) *PROGRAM DESCRIPTION.—Within 90 days*
21 *after the date of enactment of this Act, the Secretary*
22 *shall publish in the Federal Register a draft descrip-*
23 *tion of a program for establishing Centers and, after*
24 *a 30-day comment period, shall publish a final de-*

1 *scription of the program. The description shall in-*
2 *clude—*

3 *(A) a description of the program;*

4 *(B) procedures to be followed by applicants;*

5 *(C) criteria for determining qualified appli-*
6 *cants;*

7 *(D) criteria, including those described in*
8 *paragraph (4), for choosing recipients of finan-*
9 *cial assistance under this section from among the*
10 *qualified applicants; and*

11 *(E) maximum support levels expected to be*
12 *available to Centers under the program in the*
13 *fourth through sixth years of assistance under*
14 *this section.*

15 *(3) APPLICATIONS; SUPPORT COMMITMENT.—*

16 *Any nonprofit institution, or consortia of nonprofit*
17 *institutions, may submit to the Secretary an applica-*
18 *tion for financial support under this section, in ac-*
19 *cordance with the procedures established by the Sec-*
20 *retary. In order to receive assistance under this sec-*
21 *tion, an applicant shall provide adequate assurances*
22 *that it will contribute 50 percent or more of the pro-*
23 *posed Center's annual operating and maintenance*
24 *costs for the first 3 years and an increasing share for*
25 *each of the next 3 years.*

1 (4) *AWARD CRITERIA.*—*Awards shall be made on*
2 *a competitive, merit-based review. In making a deci-*
3 *sion whether to approve an application and provide*
4 *financial support under this section, the Secretary*
5 *shall consider, at a minimum—*

6 *(A) the merits of the application, particu-*
7 *larly those portions of the application regarding*
8 *technology transfer, training and education, and*
9 *adaptation of cybersecurity technologies to the*
10 *needs of particular industrial sectors;*

11 *(B) the quality of service to be provided;*

12 *(C) geographical diversity and extent of*
13 *service area; and*

14 *(D) the percentage of funding and amount*
15 *of in-kind commitment from other sources.*

16 (5) *THIRD YEAR EVALUATION.*—

17 *(A) IN GENERAL.*—*Each Center which re-*
18 *ceives financial assistance under this section*
19 *shall be evaluated during its third year of oper-*
20 *ation by an evaluation panel appointed by the*
21 *Secretary.*

22 *(B) EVALUATION PANEL.*—*Each evaluation*
23 *panel shall be composed of private experts and*
24 *Federal officials, none of whom shall be con-*
25 *nected with the involved Center. Each evaluation*

1 panel shall measure the Center's performance
2 against the objectives specified in this section
3 and ensure that the Center is not competing
4 with, or duplicating, private sector activities.

5 (C) *POSITIVE EVALUATION REQUIRED FOR*
6 *CONTINUED FUNDING.*—The Secretary may not
7 provide funding for the fourth through the sixth
8 years of a Center's operation unless the evalua-
9 tion by the evaluation panel is positive. If the
10 evaluation is positive, the Secretary may provide
11 continued funding through the sixth year at de-
12 clining levels.

13 (D) *FUNDING AFTER SIXTH YEAR.*—After
14 the sixth year, the Secretary may provide addi-
15 tional financial support to a Center if it has re-
16 ceived a positive evaluation through an inde-
17 pendent review, under procedures established by
18 the Institute. An additional independent review
19 shall be required at least every 2 years after the
20 sixth year of operation. Funding received for a
21 fiscal year under this section after the sixth year
22 of operation may not exceed one third of the an-
23 nual operating and maintenance costs of the
24 Center.

1 (6) *PATENT RIGHTS TO INVENTIONS.*—*The provi-*
2 *sions of chapter 18 of title 35, United States Code,*
3 *shall (to the extent not inconsistent with this section)*
4 *apply to the promotion of technology from research by*
5 *Centers under this section except for contracts for*
6 *such specific technology extension or transfer services*
7 *as may be specified by statute or by the President, or*
8 *the President’s designee.*

9 (d) *ACCEPTANCE OF FUNDS FROM OTHER FEDERAL*
10 *DEPARTMENTS AND AGENCIES.*—*In addition to such sums*
11 *as may be authorized and appropriated to the Secretary*
12 *and President, or the President’s designee, to operate the*
13 *Centers program, the Secretary and the President, or the*
14 *President’s designee, also may accept funds from other Fed-*
15 *eral departments and agencies for the purpose of providing*
16 *Federal funds to support Centers. Any Center which is sup-*
17 *ported with funds which originally came from other Federal*
18 *departments and agencies shall be selected and operated ac-*
19 *ording to the provisions of this section.*

20 **SEC. 403. PUBLIC-PRIVATE CLEARINGHOUSE.**

21 (a) *SURVEY OF EXISTING MODELS OF INTERAGENCY*
22 *AND PUBLIC-PRIVATE INFORMATION SHARING.*—*Within*
23 *180 days after the date of enactment of this Act, the Presi-*
24 *dent, or the President’s designee, in consultation with sector*
25 *coordinating councils, relevant governmental agencies and*

1 *regulatory entities, and nongovernmental organizations,*
2 *shall conduct a review and assessment of existing informa-*
3 *tion sharing models used by Federal agencies.*

4 **(b) DESIGNATION.**—*Pursuant to the results of the re-*
5 *view and assessment required by subsection (a), the Presi-*
6 *dent shall establish or designate a facility to serve as the*
7 *central cybersecurity threat and vulnerability information*
8 *clearinghouse for the Federal Government and United*
9 *States critical infrastructure information systems. The fa-*
10 *cility shall incorporate the best practices and concepts of*
11 *operations of existing information sharing models in order*
12 *to effectively promote the sharing of public-private cyberse-*
13 *curity threat and vulnerability information.*

14 **(c) INFORMATION SHARING RULES AND PROCE-**
15 **DURES.**—*The President, or the President’s designee, in con-*
16 *sultation with sector coordinating councils, relevant govern-*
17 *mental agencies and regulatory entities, and nongovern-*
18 *mental organizations, shall promulgate rules and proce-*
19 *dures regarding cybersecurity threat and vulnerability in-*
20 *formation sharing, that—*

21 **(1)** *expand the Federal Government’s sharing of*
22 *cybersecurity threat and vulnerability information*
23 *with owners and operators of United States critical*
24 *infrastructure information systems;*

1 (2) *ensure confidentiality and privacy protec-*
2 *tions for individuals and personally identifiable in-*
3 *formation;*

4 (3) *ensure confidentiality and privacy protec-*
5 *tions for private sector-owned intellectual property*
6 *and proprietary information;*

7 (4) *establish criteria under which owners or op-*
8 *erators of United States critical infrastructure infor-*
9 *mation systems share actionable cybersecurity threat*
10 *and vulnerability information and relevant data with*
11 *the Federal Government;*

12 (5) *protect against, or mitigate, civil and crimi-*
13 *nal liability implicated by information shared; and*

14 (6) *otherwise will enhance the sharing of cyberse-*
15 *curity threat and vulnerability information between*
16 *owners or operators of United States critical infra-*
17 *structure information systems and the Federal Gov-*
18 *ernment.*

19 **SEC. 404. CYBERSECURITY RISK MANAGEMENT REPORT.**

20 *Within 1 year after the date of enactment of this Act,*
21 *the President, or the President's designee, shall report to*
22 *the Congress on the feasibility of creating a market for cy-*
23 *bersecurity risk management.*

Calendar No. 707

11TH CONGRESS
2^D SESSION
S. 773

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 cyber security defenses against disruption, and for other purposes.

DECEMBER 17, 2010

Reported with an amendment