

**[DISCUSSION DRAFT]**

SEPTEMBER 18, 2009

111TH CONGRESS  
1ST SESSION

**H. R.** \_\_\_\_\_

To authorize activities for support of cybersecurity research and development  
and for other purposes.

---

IN THE HOUSE OF REPRESENTATIVES

M. \_\_\_\_\_ introduced the following bill; which was referred to the  
Committee on \_\_\_\_\_

---

**A BILL**

To authorize activities for support of cybersecurity research  
and development and for other purposes.

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

3 **SECTION 1. SHORT TITLE.**

4 This Act may be cited as the “Cybersecurity Re-  
5 search and Development Amendments Act of 2009”.

6 **SEC. 2. DEFINITIONS.**

7 In this Act:

1           (1) NATIONAL COORDINATION OFFICE.—The  
2           term National Coordination Office means the Na-  
3           tional Coordination Office for the Networking and  
4           Information Technology Research and Development  
5           program.

6           (2) PROGRAM.—The term Program means the  
7           Networking and Information Technology Research  
8           and Development program which has been estab-  
9           lished under section 101 of the High-Performance  
10          Computing Act of 1991 (15 U.S.C. 5511).

11 **SEC. 3. FINDINGS.**

12          Section 2 of the Cyber Security Research and Devel-  
13          opment Act (15 U.S.C. 7401) is amended—

14                 (1) by amending paragraph (1) to read as fol-  
15          lows:

16                 “(1) Advancements in information and commu-  
17                 nications technology have resulted in a globally-  
18                 interconnected network of government, commercial,  
19                 scientific, and education infrastructures, including  
20                 critical infrastructures for electric power, natural  
21                 gas and petroleum production and distribution, tele-  
22                 communications, transportation, water supply, bank-  
23                 ing and finance, and emergency and government  
24                 services.”;

1           (2) in paragraph (2), by striking “Exponential  
2           increases in interconnectivity have facilitated en-  
3           hanced communications, economic growth,” and in-  
4           serting “These advancements have significantly con-  
5           tributed to the growth of the United States econ-  
6           omy”;

7           (3) by amending paragraph (3) to read as fol-  
8           lows:

9           “(3) The Cyberspace Policy Review published  
10          by the President in May, 2009, concluded that our  
11          information technology and communications infra-  
12          structure is vulnerable and has ‘suffered intrusions  
13          that have allowed criminals to steal hundreds of mil-  
14          lions of dollars and nation-states and other entities  
15          to steal intellectual property and sensitive military  
16          information’.”;

17          (4) by redesignating paragraphs (4) through  
18          (6) as paragraphs (5) through (7), respectively;

19          (5) by inserting after paragraph (3) the fol-  
20          lowing new paragraph:

21          “(4) In a series of hearings held before Con-  
22          gress in 2009 experts testified that the Federal cy-  
23          bersecurity research and development portfolio was  
24          too focused on short-term, incremental research and  
25          that it lacked the prioritization and coordination

1 necessary to address the long-term challenge of en-  
2 suring a secure and reliable information technology  
3 and communications infrastructure.”; and

4 (6) by amending paragraph (7), as so redesign-  
5 nated by paragraph (4) of this section, to read as  
6 follows:

7 “(7) While African-Americans, Hispanics, and  
8 Native Americans constitute 33 percent of the col-  
9 lege-age population, members of these minorities  
10 comprise less than 20 percent of bachelor degree re-  
11 cipients in the field of computer sciences.”.

12 **SEC. 4. CYBERSECURITY STRATEGIC RESEARCH AND DE-**  
13 **VELOPMENT PLAN.**

14 (a) IN GENERAL.—Not later than 12 months after  
15 the date of enactment of this Act, the agencies identified  
16 in subsection 101(a)(3)(B)(i) through (x) of the High-Per-  
17 formance Computing Act of 1991 (15 U.S.C.  
18 5511(a)(3)(B)(i) through (x)) or designated under section  
19 101(a)(3)(B)(xi) of such Act, working through the Na-  
20 tional Science and Technology Council and with the assist-  
21 ance of the National Coordination Office, shall transmit  
22 to Congress a strategic plan based on an assessment of  
23 cybersecurity risk to guide the overall direction of Federal  
24 cybersecurity and information assurance research and de-  
25 velopment for information technology and networking sys-

1 tems. Once every 3 years after the initial strategic plan  
2 is transmitted to Congress under this section, such agen-  
3 cies shall prepare and transmit to Congress an update of  
4 such plan.

5 (b) CONTENTS OF PLAN.—The strategic plan re-  
6 quired under subsection (a) shall—

7 (1) specify and prioritize near-term, mid-term  
8 and long-term research objectives, including objec-  
9 tives associated with the research areas identified in  
10 section 4(a)(1) of the Cyber Security Research and  
11 Development Act (15 U.S.C. 7403(a)(1)) and how  
12 the near-term objectives complement research and  
13 development areas in which the private sector is ac-  
14 tively engaged;

15 (2) describe how the Program will focus on in-  
16 novative, transformational technologies with the po-  
17 tential to enhance the security, reliability, resilience,  
18 and trustworthiness of the digital infrastructure;

19 (3) describe how the Program will foster the  
20 transfer of research and development results into  
21 new cybersecurity technologies and applications for  
22 the benefit of society and the national interest, in-  
23 cluding through the dissemination of best practices  
24 and other outreach activities;

1           (4) describe how the Program will establish and  
2           maintain a national research infrastructure for cre-  
3           ating, testing, and evaluating the next generation of  
4           secure networking and information technology sys-  
5           tems; and

6           (5) describe how the Program will facilitate ac-  
7           cess by academic researchers to the infrastructure  
8           described in paragraph (4), as well as to event data.

9           (c) DEVELOPMENT OF ROADMAP.—The agencies de-  
10          scribed in subsection (a) shall develop and annually update  
11          an implementation roadmap for the strategic plan re-  
12          quired in this section. Such roadmap shall—

13           (1) specify the role of each Federal agency in  
14           carrying out or sponsoring research and development  
15           to meet the research objectives of the strategic plan,  
16           including a description of how progress toward the  
17           research objectives will be evaluated;

18           (2) specify the funding allocated to each major  
19           research objective of the strategic plan and the  
20           source of funding by agency for the current fiscal  
21           year; and

22           (3) estimate the funding required for each  
23           major research objective of the strategic plan for the  
24           following 3 fiscal years.

1 (d) RECOMMENDATIONS.—In developing and updat-  
2 ing the strategic plan under subsection (a), the agencies  
3 involved shall solicit recommendations and advice from—

4 (1) the advisory committee established under  
5 section 101(b)(1) of the High-Performance Com-  
6 puting Act of 1991 (15 U.S.C. 5511(b)(1)); and

7 (2) a wide range of stakeholders, including in-  
8 dustry, academia, and other relevant organizations  
9 and institutions.

10 (e) APPENDING TO REPORT.—The implementation  
11 roadmap required under subsection (c), and its annual up-  
12 dates, shall be appended to the report required under sec-  
13 tion 101(a)(2)(D) of the High-Performance Computing  
14 Act of 1991 (15 U.S.C. 5511(a)(2)(D)).

15 **SEC. 5. SOCIAL AND BEHAVIORAL RESEARCH IN CYBERSE-**  
16 **CURITY.**

17 Section 4(a)(1) of the Cyber Security Research and  
18 Development Act (15 U.S.C. 7403(a)(1)) is amended—

19 (1) by inserting “and usability” after “to the  
20 structure”;

21 (2) in subparagraph (H), by striking “and”  
22 after the semicolon;

23 (3) in subparagraph (I), by striking the period  
24 at the end and inserting “; and”; and

1 (4) by adding at the end the following new sub-  
2 paragraph:

3 “(J) social and behavioral factors, includ-  
4 ing human-computer interactions, usability,  
5 user motivations, and organizational cultures.”.

6 **SEC. 6. NATIONAL SCIENCE FOUNDATION CYBERSECURITY**  
7 **RESEARCH AND DEVELOPMENT PROGRAMS.**

8 (a) COMPUTER AND NETWORK SECURITY RESEARCH  
9 AREAS.—Section 4(a) of the Cyber Security Research and  
10 Development Act (15 U.S.C. 7403(a)(1)) is amended in  
11 subparagraph (A) by inserting “identity management,”  
12 after “cryptography,”.

13 (b) COMPUTER AND NETWORK SECURITY RESEARCH  
14 GRANTS.—Section 4(a)(3) of such Act (15 U.S.C.  
15 7403(a)(3)) is amended by striking subparagraphs (A)  
16 through (E) and inserting the following new subpara-  
17 graphs:

18 “(A) \$68,700,000 for fiscal year 2010;

19 “(B) \$73,500,000 for fiscal year 2011;

20 “(C) \$78,600,000 for fiscal year 2012;

21 “(D) \$84,200,000 for fiscal year 2013;

22 and

23 “(E) \$90,000,000 for fiscal year 2014.”.



1 (c) COMPUTER AND NETWORK SECURITY RESEARCH  
2 CENTERS.—Section 4(b) of such Act (15 U.S.C. 7403(b))  
3 is amended—

4 (1) in paragraph (4)—

5 (A) in subparagraph (C), by inserting  
6 “and” after the semicolon;

7 (B) in subparagraph (D), by striking the  
8 period and inserting “; and”; and

9 (C) by striking subparagraph (D); and

10 (2) by adding at the end the following new sub-  
11 paragraph:”.

12 “(E) how the center will partner with gov-  
13 ernment laboratories, for-profit entities, other  
14 institutions of higher education, or nonprofit re-  
15 search institutions.”.

16 (c) COMPUTER AND NETWORK SECURITY CAPACITY  
17 BUILDING GRANTS.—Section 5(a)(6) of such Act (15  
18 U.S.C. 7404(a)(6)) is amended to read as follows:

19 “(6) AUTHORIZATION OF APPROPRIATIONS.—

20 The are authorized to be appropriated to the Na-  
21 tional Science Foundation such sums as are nec-  
22 essary to carry out this subsection for each of the  
23 fiscal years 2010 through 2014.”.

1 (d) SCIENTIFIC AND ADVANCED TECHNOLOGY ACT  
2 GRANTS.—Section 5(b)(2) of such Act (15 U.S.C.  
3 7404(b)(2)) is amended to read as follows:

4 “(2) AUTHORIZATION OF APPROPRIATIONS.—  
5 The are authorized to be appropriated to the Na-  
6 tional Science Foundation such sums as are nec-  
7 essary to carry out this subsection for each of the  
8 fiscal years 2010 through 2014.”.

9 (e) GRADUATE TRAINEESHIPS IN COMPUTER AND  
10 NETWORK SECURITY.—Section 5(c)(7) of such Act (15  
11 U.S.C. 7404(c)(7)) is amended to read as follows:

12 “(7) AUTHORIZATION OF APPROPRIATIONS.—  
13 The are authorized to be appropriated to the Na-  
14 tional Science Foundation such sums as are nec-  
15 essary to carry out this subsection for each of the  
16 fiscal years 2010 through 2014.”.

17 (f) POSTDOCTORAL RESEARCH FELLOWSHIPS IN CY-  
18 BERSECURITY.—Section 5(e) of such Act (15 U.S.C.  
19 7404(e)) is amended to read as follows:

20 “(e) POSTDOCTORAL RESEARCH FELLOWSHIPS IN  
21 CYBERSECURITY.—

22 “(1) IN GENERAL.—The Director shall carry  
23 out a program to encourage young scientists and en-  
24 gineers to conduct postdoctoral research in the fields  
25 of cybersecurity and information assurance, includ-

1       ing the research areas described in section 4(a)(1),  
2       through the award of competitive, merit-reviewed fel-  
3       lowships.

4               “(2) AUTHORIZATION OF APPROPRIATIONS.—  
5       The are authorized to be appropriated to the Na-  
6       tional Science Foundation such sums as are nec-  
7       essary to carry out this subsection for each of the  
8       fiscal years 2010 through 2014.”.

9       **SEC. 7. FEDERAL CYBER SCHOLARSHIP FOR SERVICE PRO-**  
10               **GRAM.**

11       (a) IN GENERAL.—The Director of the National  
12       Science Foundation shall carry out a Scholarship for Serv-  
13       ice program to recruit and train the next generation of  
14       Federal cybersecurity professionals and to increase the ca-  
15       pacity of the higher education system to produce a tech-  
16       nology workforce with the skills necessary to enhance the  
17       security of the Nation’s communications and information  
18       infrastructure.

19       (b) CHARACTERISTICS OF PROGRAM.—The program  
20       under this section shall—

21               (1) provide, through qualified institutions of  
22       higher education, scholarships that provide tuition,  
23       fees, and a competitive stipend for up to 3 years to  
24       students pursuing undergraduate and graduate de-  
25       grees in cybersecurity fields;

1           (2) provide the scholarship recipients with sum-  
2 mer internship opportunities or other meaningful  
3 temporary appointments in the Federal information  
4 technology workforce; and

5           (3) increase the capacity of institutions of high-  
6 er education to produce highly qualified cybersecu-  
7 rity professionals, through the award of competitive,  
8 merit-reviewed grants that support such activities  
9 as—

10                   (A) faculty professional development, in-  
11 cluding technical, hands-on experiences in the  
12 private sector or government, workshops, semi-  
13 nars, conferences, and other professional devel-  
14 opment opportunities that will result in im-  
15 proved instructional capabilities;

16                   (B) institutional partnerships; and

17                   (C) development of cybersecurity-related  
18 courses and curricula.

19       (c) SCHOLARSHIP REQUIREMENTS.—

20           (1) ELIGIBILITY.—Scholarships under this sec-  
21 tion shall be available only to students who—

22                   (A) are citizens or permanent residents of  
23 the United States; and

24                   (B) are full-time students in an eligible de-  
25 gree program, as determined by the Director,

1           that is focused on computer security or infor-  
2           mation assurance at an awardee institution.

3           (2) SELECTION.—Individuals shall be selected  
4           to receive scholarships primarily on the basis of aca-  
5           demic merit, with consideration given to financial  
6           need.

7           (3) SERVICE OBLIGATION.—If an individual re-  
8           ceives a scholarship under this section, as a condi-  
9           tion of receiving such scholarship, the individual  
10          upon completion of their degree must serve as a cy-  
11          bersecurity professional within the Federal workforce  
12          for a period of time equal to the length of the schol-  
13          arship. If a scholarship recipient is not offered em-  
14          ployment by a Federal agency, the service require-  
15          ment can be satisfied by —

16                   (A) serving as a cybersecurity professional  
17                   in a State or local government agency; or

18                   (B) teaching cybersecurity courses at an  
19                   institution of higher education.

20          (d) FAILURE TO COMPLETE SERVICE OBLIGATION.—

21                  (1) GENERAL RULE.—If an individual who has  
22                  received a scholarship under this section—

23                          (A) fails to maintain an acceptable level of  
24                          academic standing in the educational institution

1 in which the individual is enrolled, as deter-  
2 mined by the Director;

3 (B) is dismissed from such educational in-  
4 stitution for disciplinary reasons;

5 (C) withdraws from the program for which  
6 the award was made before the completion of  
7 such program;

8 (D) declares that the individual does not  
9 intend to fulfill the service obligation under this  
10 section; or

11 (E) fails to fulfill the service obligation of  
12 the individual under this section,

13 such individual shall be liable to the United States  
14 as provided in paragraph (3).

15 (2) MONITORING COMPLIANCE.—A qualified in-  
16 stitution of higher education receiving a grant under  
17 this section shall, as a condition of participating in  
18 the program, enter into an agreement with the Di-  
19 rector of the National Science Foundation to mon-  
20 itor the compliance of scholarship recipients with re-  
21 spect to their respective service requirements.

22 (3) AMOUNT OF REPAYMENT.—

23 (A) LESS THAN ONE YEAR OF SERVICE.—

24 If a circumstance described in paragraph (1)  
25 occurs before the completion of 1 year of a

1 service obligation under this section, the total  
2 amount of awards received by the individual  
3 under this section shall be repaid or such  
4 amount shall be treated as a loan to be repaid  
5 in accordance with subparagraph (C).

6 (B) MORE THAN ONE YEAR OF SERVICE.—  
7 If a circumstance described in subparagraph  
8 (D) or (E) of paragraph (1) occurs after the  
9 completion of 1 year of a service obligation  
10 under this section, the total amount of scholar-  
11 ship awards received by the individual under  
12 this section, reduced by the ratio of the number  
13 of years of service completed divided by the  
14 number of years of service required, shall be re-  
15 paid or such amount shall be treated as a loan  
16 to be repaid in accordance with subparagraph  
17 (C).

18 (C) REPAYMENTS.—A loan described in  
19 subparagraph (A) or (B) shall be treated as a  
20 Federal Direct Unsubsidized Stafford Loan  
21 under part D of title IV of the Higher Edu-  
22 cation Act of 1965 (20 U.S.C. 1087a and fol-  
23 lowing), and shall be subject to repayment, to-  
24 gether with interest thereon accruing from the  
25 date of the scholarship award, in accordance

1 with terms and conditions specified by the Di-  
2 rector (in consultation with the Secretary of  
3 Education) in regulations promulgated to carry  
4 out this paragraph.

5 (4) COLLECTION OF REPAYMENT.—

6 (A) IN GENERAL.—In the event that a  
7 scholarship recipient is required to repay the  
8 scholarship under this subsection, the institu-  
9 tion providing the scholarship shall—

10 (i) be responsible for determining the  
11 repayment amounts and for notifying the  
12 recipient and the Director of the amount  
13 owed; and

14 (ii) collect such repayment amount  
15 within a period of time as determined  
16 under the agreement described in para-  
17 graph (2), or the repayment amount shall  
18 be treated as a loan in accordance with  
19 paragraph (3)(C).

20 (B) RETURNED TO TREASURY.—Except as  
21 provided in subparagraph (C) of this para-  
22 graph, any such repayment shall be returned to  
23 the Treasury of the United States.

24 (C) RETAIN PERCENTAGE.—An institution  
25 of higher education may retain a percentage of



1           any repayment the institution collects under  
2           this paragraph to defray administrative costs  
3           associated with the collection. The Director  
4           shall establish a single, fixed percentage that  
5           will apply to all eligible entities.

6           (5) EXCEPTIONS.—The Director may provide  
7           for the partial or total waiver or suspension of any  
8           service or payment obligation by an individual under  
9           this section whenever compliance by the individual  
10          with the obligation is impossible or would involve ex-  
11          treme hardship to the individual, or if enforcement  
12          of such obligation with respect to the individual  
13          would be unconscionable.

14          (e) HIRING AUTHORITY.—For purposes of any law  
15          or regulation governing the appointment of individuals in  
16          the Federal civil service, upon successful completion of  
17          their degree, students receiving a scholarship under this  
18          section shall be hired under the authority provided for in  
19          section 213.3102(r) of title 5, Code of Federal Regula-  
20          tions, and be exempted from competitive service. Upon ful-  
21          fillment of the service term, such individuals shall be con-  
22          verted to a competitive service position without competi-  
23          tion if the individual meets the requirements for that posi-  
24          tion.

1 (f) AUTHORIZATION OF APPROPRIATIONS.—There  
2 are authorized to appropriated to the National Science  
3 Foundation to carry out this section—

4 (1) \$18,700,000 for fiscal year 2010;

5 (2) \$20,100,000 for fiscal year 2011;

6 (3) \$21,600,000 for fiscal year 2012;

7 (4) \$23,300,000 for fiscal year 2013; and

8 (5) \$25,000,000 for fiscal year 2014.

9 **SEC. 8. CYBERSECURITY WORKFORCE ASSESSMENT.**

10 Not later than 180 days after the date of enactment  
11 of this Act the President shall transmit to the Congress  
12 a report addressing the cybersecurity workforce needs of  
13 the Federal Government. The report shall include—

14 (1) an examination of the current state of and  
15 the projected needs of the Federal cybersecurity  
16 workforce, including a comparison of the different  
17 agencies and departments, and an analysis of the ca-  
18 pacity of such agencies and departments to meet  
19 those needs;

20 (2) an analysis of the sources and availability of  
21 cybersecurity talent, including a comparison of the  
22 Federal Government's needs with the cybersecurity  
23 skills and expertise sought by the private sector; and

24 (3) an analysis of any barriers to the Federal  
25 Government recruiting and hiring cybersecurity tal-

1 ent, including barriers relating to compensation, the  
2 hiring process, job classification, and hiring flexibili-  
3 ties, along with recommendations to overcome identi-  
4 fied barriers.

5 **SEC. 9. CYBERSECURITY UNIVERSITY-INDUSTRY TASK**  
6 **FORCE.**

7 (a) ESTABLISHMENT OF UNIVERSITY-INDUSTRY  
8 TASK FORCE.—Not later than 180 days after the date of  
9 enactment of this Act, the Director of the Office of Science  
10 and Technology Policy shall convene a task force to ex-  
11 plore mechanisms for carrying out collaborative research  
12 and development activities for cybersecurity through a  
13 consortium or other appropriate entity with participants  
14 from institutions of higher education and industry.

15 (b) FUNCTIONS.—The task force shall—

16 (1) develop options for a collaborative model  
17 and an organizational structure for such entity  
18 under which the joint research and development ac-  
19 tivities could be planned, managed, and conducted  
20 effectively, including mechanisms for the allocation  
21 of resources among the participants in such entity  
22 for support of such activities;

23 (2) propose a process for developing a research  
24 and development agenda for such entity, including  
25 guidelines to ensure an appropriate scope of work fo-

1           cused on nationally significant challenges and requir-  
2           ing collaboration;

3           (3) define the roles and responsibilities for the  
4           participants from institutions of higher education  
5           and industry in such entity;

6           (4) propose guidelines for assigning intellectual  
7           property rights and for the transfer of research and  
8           development results to the private sector; and

9           (5) make recommendations for how such entity  
10          could be funded from Federal, State, and nongovern-  
11          mental sources.

12          (c) COMPOSITION.—In establishing the task force  
13          under subsection (a), the Director of the Office of Science  
14          and Technology Policy shall appoint an equal number of  
15          individuals from institutions of higher education and from  
16          industry with knowledge and expertise in cybersecurity.

17          (d) REPORT.—Not later than 12 months after the  
18          date of enactment of this Act, the Director of the Office  
19          of Science and Technology Policy shall transmit to the  
20          Congress a report describing the findings and rec-  
21          ommendations of the task force.