107TH CONGRESS
2d Session
HOUSE OF REPRESENTATIVES
REPT. 107–355
Part I

CYBER SECURITY RESEARCH AND DEVELOPMENT ACT

FEBRUARY 4, 2002.—Committed to the Committee of the Whole House on the State of the Union and ordered to be printed

Mr. BOEHLERT, from the Committee on Science, submitted the following

R E P O R T

[To accompany H.R. 3394]

[Including cost estimate of the Congressional Budget Office]

The Committee on Science, to whom was referred the bill (H.R. 3394) to authorize funding for computer and network security research and development and research fellowship programs, and for other purposes, having considered the same, report favorably thereon without amendment and recommend that the bill do pass.

CONTENTS

99–006

I. PURPOSE OF THE BILL

The purpose of the bill is to authorize funding for computer and network security education, research and development.

II. BACKGROUND AND NEED FOR LEGISLATION

The terrorist attacks of September 11, 2001 brought into stark relief the Nation's physical and economic vulnerability to an attack within our borders. The relative case with which terrorists were able to implement their plans serves as a pointed reminder of the need to identify critical "soft sports" in the nation's defenses. Among the Nation's vulnerabilities are our computer and communications networks, on which the country's finance, transportation, energy and water distribution systems, and health and emergency services depend. These vulnerabilities have called into question whether the Nation's technological research programs, educational system, and interconnected operations are prepared to meet the challenge of cyber warfare in the 21st century. The Los Angeles Times in a recent editorial emphasized the importance of meeting this challenge: "A cyberterrorist attack would not carry the same shock and carnage of September 11. But in this information age . . . [a cyberterrorist attack] could be more widespread and just as economically destructive."

We will not be able to address these vulnerabilities without conducting more research on cybersecurity. H.R. 3394 is designed to address four inadequacies with current research efforts:

(1) The Federal Government has chronically underinvested in cybersecurity, an area in which the private sector has little incentive to invest.

(2) This is true, in part, because no Federal agency has the responsibility of ensuring that the Nation has a robust cybersecurity research enterprise;

(3) As a result, what little research has been done on cybersecurity has been incremental, leaving the basic approaches to cybersecurity unchanged for decades; and

(4) As a field with relatively little money, few researchers and minimal attention, cybersecurity fails to attract the interest of students, perpetuating the problems in the field.

VULNERABILITIES OF THE NATIONAL INFORMATION INFRASTRUCTURE

The Internet has been a tremendous success—connecting more than 100 million computers and growing—far outstripping its designers' wildest expectations. Yet the Internet was not originally designed to control power systems, connect massive databases of medical records or connect millions of home appliances or automobiles, yet today it serves these functions. It was not designed to run critical safety systems but it now does that as well. We now heavily rely on an open network of networks, so complex that no one person, group or entity can describe it, model its behavior or predict its reaction to adverse events.

The porous fabric of the U.S.'s network infrastructure leaves the Nation open to the constant possibility of cyber attack. Attacks can take several forms, including: defacement of web sites and other electronically stored information in the United States and other countries to spread disinformation and propaganda; distributed de-

nial of service attacks that overwhelm a server with access requests; use of unprotected "zombie" computers (located anywhere) as conduits for wide-scale distribution of destructive worms and viruses throughout the computer network; and unauthorized intrusions and sabotage of systems and networks belonging to the U.S. and allied countries, potentially resulting in critical infrastructure outages and corruption of vital data.

The wide-scale attack by the so-called "Nimda" worm is one example of these techniques; the virus modified web documents and certain executable files found on the systems it infected, and then created numerous copies of itself under various file names. This followed the "Code Red," "Code Red II" and "SirCam" attacks which affected millions of personal, commercial and government computers, shut down web sites, slowed Internet service, and disrupted business and government operations, causing billions of dollars of damage.

These attacks no longer represent isolated or infrequent events. Carnegie Mellon University's CERT® Coordination Center, which serves as a reporting center for Internet security problems, received 2,437 vulnerability reports in calendar year 2001, almost 6 times the number in 1999. Similarly, the number of specific incidents reported to CERT grew enormously—from 9,859 in 1999 to 52,658 in 2001. yet CERT estimates that this may represent only about 20 percent of the incidents that actually have occurred.

INTERDEPENDENCE OF CRITICAL INFRASTRUCTURES

To better understand our vulnerabilities to cyber terrorism and the potential consequences of cyber attacks, the Internet must no longer be studied solely as a separate system but also as a network of interdependent critical infrastructures. It also has links to many ostensibly private networks, such as those used by the financial services industry. While some research is being done to better understand the threats to the Internet itself, little has been done to assess and project the dramatic or subtle impact that these threats may have on other critical infrastructures. These problems are not hypothetical. While not the result of a cyber attack, the 1998 failure of the Galaxy 4 communications satellite disrupted the use of 90 percent of the Nation's pagers and disrupted credit card purchases and ATM transactions. The failure also disrupted the communications of health care providers and emergency workers.

INFORMATION WARFARE SIMULATIONS—"ELIGIBLE RECEIVER"

In 1997, the Pentagon conducted an information warfare exercise that illustrated some of the implications of infrastructure interdependence. Known as Eligible Receiver, the exercise simulated a rogue state attempting to attack vulnerable U.S. information systems. A "Red Team" comprising 35 National Security Agency computer specialists used off-the-self technology and software to simulate attacks against power and communications networks in Oahu, Los Angeles, Colorado Springs, St. Louis, Chicago, Detroit, Washington, D.C., Fayetteville, and Tampa. According to the Congressional Research Service, it is generally believed that government (including unclassified military computer networks) and commercial sites were easily attacked and penetrated. Air Force Major General John H. Campbell, commander of the DoD Joint Task

Force—Computer Network Defense, wrote that the exercise "clearly demonstrated our lack of preparation for a coordinated cyber and physical attack on our critical military and civilian infrastructure." Officials familiar with the exercise later said that Eligible Receiver showed in "real terms how vulnerable the transportation grid, the electricity grid, and others are to an attack by people using conventional equipment." The National Security Agency subsequently recommended that all Federal Internet accessible computer networks that process or provide access to classified, confidential, or sensitive data should have mandatory access controls.

UNDERLYING CAUSES OF THE NATION'S VULNERABILITY TO CYBER ATTACK

Weaknesses in research and development in the cyber security arena contribute significantly to the vulnerability of the Nation's information infrastructure. While a number of information technology companies support R&D on network security, security inadequacies cannot be addressed solely through short-term industry-based applied research, which is underfunded in any event. Industry relies on the fundamental research supported by the Federal Government and on the training of future researchers—computer scientists, mathematicians, and many others—that these federally funded research programs support.

Unfortunately, with the possible exception of encryption related research, cyber security research has been chronically underfunded, and basis research into fundamental cyber security challenges is not robust enough to meet the Nation's needs. Simply put, when it comes to computer security, too few people are paying too little attention and coming up with too few ideas.

Cyber security has been a neglected field. Although numbers are difficult to come by, federally funded cyber security research may amount to less than $60 million per year. Experts believe that fewer than 100 U.S. researchers have the experience and expertise to conduct cutting edge research in cyber security. This is true even though a computer science department at a single research university may have 60 or more faculty members.

This chronic under-investment does not merely pose problems for the academic and research community. Federal agencies are finding it increasingly difficult to recruit and hire professional staff to manage and secure their own computer networks. The National Science Foundation (NSF), in consultation with the National Security Council, the National Security Agency, the Critical Infrastructure Assurance Office, and the Office of Personnel Management established in July 2000 a scholarship-for-service program designed to train students who would then help ensure the security of the Federal information infrastructure. This program was funded at the level of $1.2 million for FY 2001 and was expected to provide scholarship funds for approximately 180 undergraduate and graduate students. The National Aeronautics and Space Administration has requested similar scholarship-for-service authority to recruit students with expertise in computer science and other technical fields. Other agencies are likely to follow. NSF has also recently established another program designed to enhance research in information assurance and build a well-trained cyber security workforce. NSF's Trusted Computing program, established in FY 2001,

will award between $4 million and $6 million in FY 2002 to support research on computer and network security.

In addition, The National Institute of Standards and Technology (NIST) within the Department of Commerce provides grants for research to develop commercial solutions to IT security problems central to critical infrastructure protection. NIST recently announced the award of grants under its Critical Infrastructure Protection Grants Program aimed at improving the security of the computer and telecommunications systems that support essential services.

While private industry has rapidly advanced many aspects of information technology, it has had little incentive to focus on the development of cyber security. The market demands faster, cheaper, more powerful products, not more secure ones. In the wake of the September 11th attacks, security has a slightly higher profile in the private sector, but real advances in information assurance will still rely on efforts by the Federal Government.

Two studies conducted by the firm Metricnet suggest that 80 percent of companies spent less than 5 percent of their information technology budget on information security prior to September 11th. In November that was still true of two-thirds of the companies.

Yet the Federal Government has not been filling the research gap left by the private sector. The Federal Government has chronically under-invested in this area. As a result, too little cyber security research is being conducted and too few researchers are prepared to meet our current and projected cyber security research needs. In addition, the research that is funded is incremental and unlikely to lead to the development of breakthrough approaches to cyber security.

This lack of Federal focus has also limited the number of undergraduate and graduate students pursuing studies in cyber security. Despite these problems and the inadequate coordination between government, academia, and industry, no Federal agency has stepped forward to take the lead in supporting cyber security research. The Cyber Security Research and Development Act responds to these challenges by authorizing a focused, long-term Federal investment in cyber security research, designed to increase the cadre of researchers in this field over the long-term and to yield innovative new approaches to cyber security.

III. Summary of Hearings

On Tuesday, July 31, 2001, the House Science Committee's Subcommittee on Research held a hearing to examine the impact Federal investment has had on promoting innovation in information technology and fostering a variety of sophisticated applications that infuse information technology into areas such as education, scientific research, and the delivery of public services. Witnesses described the increasing reliance on information technology by all sectors of the research community and the general public, and specifically discussed applications of information technology to pharmaceutical research, biotechnology, education, emergency management, air and ground traffic coordination, and predictive weather and climate modeling. Witnesses discussed the need for new information tools and technologies to be available to all sectors of the community and emphasized the increasing need for system reliability and security given the increasing dependence on informa-

tion technology for even the most basic human services. Witnesses agreed, however, that there has been a lack of focus and effort in the areas of computer and network security, privacy, and information assurance, and that the ability to protect key infrastructures lags behind their development and implementation.

On Wednesday, October 10, 2001, the House Committee on Science held a hearing to examine the vulnerability of our Nation's computer infrastructure and related research needs. Witnesses described the vulnerability of our Nation's critical infrastructure to cyber attacks, the lack of market incentives for the development and inclusion of robust information assurance software in commercial applications, and the consequences of chronic underfunding of cyber security research by the Federal Government. Witnesses called for: the designation of a lead Federal research agency that would take primary responsibility for supporting cyber security research and development; the development of innovative new approaches to cyber security and cyber security research; and for significant increases in the number of researchers capable of doing world-class cyber security research.

On Wednesday, October 17, 2001, the House Committee on Science held a second hearing to examine the vulnerability of our Nation's computer infrastructure. In this hearing the Honorable James S. Gilmore, III, Governor of the Commonwealth of Virginia and Chairman of the Advisory Panel to Assess Domestic Response Capabilities for Terrorism Involving Weapons of Mass destruction, stated that, "Critical information and communication infrastructures are targets for terrorists because of the broad economic and operational consequences a shutdown can inflict." Governor Gilmore called for "a comprehensive plan for research, development, test and evaluation of processes to enhance cyber security in the same manner as we must do for other potential terrorist attacks."

IV. Committee Action

On December 4, 2001, Science Committee Chairman Sherwood Boehlert and Ranking Minority Member Ralph Hall introduced H.R. 3394, the Cyber Security Research and Development Act, a bill to authorize appropriations for computer and network security education, research and development for Fiscal years 2003 through 2007. The bill incorporates major provisions of H.R. 3316, the Computer Security Enhancement and Research Act, introduced by Rep. Brian Baird.

The House Committee on Science met on December 6, 2001, to consider the bill. With a quorum present, Mr. Hall moved that the Committee favorably report the bill to the House with the recommendation that it pass, and that the staff be instructed to make technical and conforming changes to the bill and prepare the legislative report, and that the Chairman take all necessary steps to bring the bill before the House for consideration. The motion was agreed to by a voice vote.

V. Summary of Major Provisions of the Bill

• Authorizes the NSF to award grants to institutions of higher education for basic research on innovative approaches to enhancing computer and network security through hardware and software so-

lutions. Includes research in a variety of areas including authentication and cryptography, computer forensics and intrusion detection, reliability of computer and network applications, middleware, operating systems and communications infrastructure, and privacy and confidentiality. This program is authorized at $35 million for FY 2003, $40 million for FY 2004, $46 million for FY 2005, $52 million for FY 2006, and $60 million for FY 2007.

• Authorizes NSF to award grants to institutions of higher education to establish multidisciplinary Centers for Computer and Network Security Research. Applicants may partner with government laboratories and/or for-profit institutions. These centers are designed to advance the research agenda and to train additional qualified computer and network security researchers and professionals. Instructs NSF to convene an annual meeting of Center investigators to facilitate information exchange. This program is authorized at $12 million for FY 2003, $24 million for FY 2004, $36 million for each of fiscal years 2005 through 2007.

• Authorizes NSF to establish a program to award grants to institutions of higher education to establish or improve undergraduate and master's degree programs in computer and network security, to increase the number of students who pursue undergraduate or master's degrees in fields related to computer and network security, and to provide students with experience in government or industry related to their computer and network security studies. Funds may be used for curriculum development, faculty development, equipment acquisition, student recruitment and/or the establishment of bridge programs with two-year colleges and industry internship programs for students. This program is authorized at $15 million for FY 2003 and $20 million for each year from FY 2004 through FY 2007.

• Authorizes NSF to expand the activities of the Advanced Technological Education Program, established under the Scientific and Advanced Technology Act of 1992, to support improved education and technical training in fields related to computer and network security. This program is authorized at $1 million for FY 2003, and $1.25 million for each of fiscal years 2003 through FY 2007.

• Authorizes NSF to establish a program to support graduate traineeships in computer and network security at institutions of higher education. Grant awards can be used to provide student fellowship support, to pay tuition and fees for students who are fellowship recipients, to establish internship programs for students in computer and network security at for-profit institutions or government laboratories, and to administer the program. This program is authorized at $10 million for FY 2003, and $20 million for each of fiscal years 2005 through FY 2007.

• Authorizes NSF to list computer and network security as a field of specialization under the NSF Graduate Research Fellowships program established by the National Science Foundation Act of 1950.

• Amends the National Science Foundation Act of 1950 to charge NSF with taking a lead role in fostering and supporting research and education activities to improve the security of networked information systems.

• Authorizes NIST to establish a program of assistance for institutions of higher education that enter into partnerships with for-

profit entities (which may also include government laboratories), to support long-term, high-risk research to improve the security of computer systems. Instructs NIST to include research directed toward addressing needs identified through the activities of the Computer System Security and Privacy Advisory Board. This program is authorized at $25 million for FY 2003, $40 million for FY 2004, $55 million for FY 2005, $70 million for FY 2006, and $85 million for FY 2007.

• Authorizes NIST to establish a program to award post-doctoral research fellowships to citizens, nationals, or lawfully admitted permanent resident aliens of the U.S. who are seeking research positions at an institution, including the Institute, engaged in cyber security research. Also authorizes NIST to establish a similar program to provide research fellowships to senior researchers who wish to change research fields and pursue studies related to the security of computer systems. Authorizes $6 million for FY 2003, $6.2 million for FY 2004, $6.4 million for FY 2005, $6.6 for FY 2006, and $6.8 for FY 2007.

• Authorizes NIST to recruit existing NIST employees or identify additional individuals who will serve as program managers to administer the activities established under this Act.

• Instructs NIST to periodically review the portfolio of research awards funded under this Act, in consultation with the Computer System Security and Privacy Advisory Board, to ensure that appropriateness of the research goals and the quality and utility of the research projects funded under this Act.

• Directs NIST to enter an arrangement with the National Research Council for a comprehensive review of the research program established by this Act. This review shall occur during the fifth year of the program, the results of which shall be reported to Congress no later than six years after the initiation of the program.

• Authorizes the Computer System Security and Privacy Advisory Board to identify emerging issues, including research needs, related to computer security, privacy, and cryptography and to convene public meetings and distribute reports on those subjects. Authorizes $1.06 million for FY 2003 and $1.09 million for FY 2004 for these purposes.

• Amends the National Institute of Standards and Technology Act to explicitly allow intramural research on the security of networked computer systems, including those systems integral to process control and essential infrastructure.

• Directs NIST to enter into an arrangement with the National Research Council of the National Academy of Sciences to conduct a study of the vulnerabilities of the Nation's network infrastructure and make recommendations for appropriate improvements, and to transmit a report of the findings to Congress within 21 months of the enactment of this Act. Prohibits the Director from including classified or sensitive information regarding vulnerabilities in any publicly released version of this report. Authorizes appropriations of $700,000 for this study and report.

VI. SECTION-BY-SECTION ANALYSIS (BY SECTION)

SEC. 1. SHORT TITLE

"Cyber Security Research and Development Act".

SEC. 2. FINDINGS

Discuss the interdependent nature of critical infrastructures brought about by advancements in computing and communications technology; the increased consequences of failure of communications and other critical services caused by exponential increases in interconnectivity; the Nation's lack of preparedness for a coordinated cyber and physical attack; the lack of sufficient long-term research funding and the shortage of outstanding researchers in the field of cyber security; and the lack of coordination among government, academia, and industry for computer security; and the need to significantly increase the Federal investment in computer and network security research and development.

SEC. 3. DEFINITIONS

Defines the term "Director" as the Director of the National Science Foundation (Note that where the term 'Director' is used in section 8 it refers to the Director of the National Institute for Standards and Technology). Uses the definition for 'institution of higher education' found in the Higher Education Act of 1965.

SEC. 4. NATIONAL SCIENCE FOUNDATION RESEARCH

(a) Establishes an NSF program to award merit-based grants for basic research on innovative approaches to enhance computer security. Research areas for which grants can be used include authentication and cryptography, computer forensics and intrusion detection, reliability of computer and network applications, and privacy. Authorizes appropriations of $35 million for FY 2003, $40 million for FY 2004, $46 million for 2005, $52 million for FY 2006, and $60 million for FY 2007.

(b) Establishes an NSF program to award multi-year grants to institutions of higher education (or consortia thereof) to establish multidisciplinary Centers for Computer and Network Security Research. Consortia applying for grants may include one or more government laboratories or for-profit institutions. Applications for Center grants are to be reviewed on the basis of criteria that include: the ability of the institution (or consortium) to generate innovative approaches to computer and network security research; the applicant's support for students pursuing research in computer and network security; and the extent to which government laboratories or industry partners will participate in the Center's research activities. Requires the Director to convene an annual meeting of Centers to foster greater collaboration and communication. Authorizes appropriations of $12 million for FY 2003, $24 million for FY 2004, and $36 million for each of fiscal years 2005 through 2007.

SEC. 5. NATIONAL SCIENCE FOUNDATION COMPUTER AND NETWORK SECURITY PROGRAMS

(a) Establishes a competitive, merit-based NSF program to award grants to institutions of higher education (or consortia thereof) to create or improve undergraduate and master's degree programs in computer security. Allowable uses of grants include curriculum development, equipment acquisition, faculty enhancement, and student internship programs in government or industry. Requires applicants to describe the plan for building increased capacity in com-

puter and network security, to specify the roles and responsibilities of each partnering institution or collaborative group, and to provide evidence of high potential for success in educating and placing students in relevant jobs or graduate programs. Instructs the Director to evaluate the impact of the program on increasing the quality and quantity of computer and network security professionals. Authorizes $15 million for FY 2003 and $20 million for each of fiscal years 2004 through 2007.

(b) Expands NSF's existing program for community colleges (established by the Scientific and Advanced Technology Act of 1992) to include grants to improve education in fields related to computer and network security. Authorizes $1 million for FY 2003 and $1.25 million for each of fiscal years 2004 through 2007.

(c) Establishes a competitive, merit-based NSF program to award grants to institutions of higher education to establish programs for students pursuing studies in computer and network security research leading to a doctorate degree. Grant funds are to be used to support student fellowships of at least $25,000 per year, to pay student tuition and fees, and to support students in scientific internship programs. Authorizes appropriations of $10 million for FY 2003, and $20 million for of each fiscal years 2004 through 2007.

(d) Directs NSF to include computer and network security as an approved field of specialization under its current Graduate Research Fellowships program.

SEC. 6. CONSULTATION

Requires the NSF Director to consult with other Federal agencies in carrying out the programs described in Sections 4 and 5.

SEC. 7. FOSTERING RESEARCH AND EDUCATION IN COMPUTER AND NETWORK SECURITY

Amends the National Science Foundation Act of 1950 to require NSF to take a lead role in fostering and supporting research and education in computer and network security.

SEC. 8. NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY RESEARCH PROGRAM

Amends the National Institute of Standards and Technology Act to establish a program of assistance to institutions of higher education that partner with for-profit entities to support multidisciplinary, long-term, high-risk research to improve the security of computer systems. Partnerships may also include government laboratories. Authorizes the Director to award research fellowships to post-doctoral researchers engaged in computer security research and to senior researchers who wish to move from other research fields to computer security research. Instructs the NIST Director to select Program Managers who are responsible for establishing the research goals for the program, soliciting applications for specific research projects to address these goals, and selecting research projects for funding. Calls for the NIST Director to periodically review the portfolio of research awards in consultation with NIST's existing Computer System Security and Privacy Advisory Board. Also instructs the Director to enter into an arrangement with the

National Research Council to conduct a formal review of the program and to submit a report of this review to Congress.

SEC. 9. COMPUTER SECURITY REVIEW, PUBLIC MEETINGS, AND INFORMATION

Authorizes $1,060,000 for FY 2003 and $1,090,000 for FY 2004 to enable NIST's Computer System Security and Privacy Advisory Board to identify emerging issues, including research needs related to computer security, privacy, and cryptography and, as appropriate, to convene public meetings on those subjects, receive presentations, and generate reports for public distribution.

SEC. 10. INTRAMURAL SECURITY RESEARCH

Amends the National Institute of Standards and Technology Act to authorize NIST to pursue, as part of the agency's in-house research program, research related to computer security, including the development of emerging technologies to ensure security of networked systems assembled from components, improved security of real-time computing and communications systems used in industrial and critical infrastructure operations, and improved security of computer systems.

SEC. 11 AUTHORIZATION OF APPROPRIATIONS

Authorizes appropriations for sections 8 and 10 of the bill. For the research programs in section 8, provides $25 million for FY 2003, $40 million for FY 2004, $55 million for FY 2005, $70 million for FY 2006, $85 million for FY 2007, and such sums as may be necessary for fiscal years 2008 through 2012. Authorizes appropriations for section 10 at $6 million for FY 2003, $6.2 million for FY 2004, $6.4 million for FY 2005, $6.6 million for FY 2006, and $6.8 million for FY 2007.

SEC. 12. NATIONAL ACADEMY OF SCIENCES STUDY ON COMPUTER AND NETWORK SECURITY IN CRITICAL INFRASTRUCTURES

Directs the Director of NIST to enter into an agreement with the National Research Council to conduct a study of the vulnerabilities of the Nation's critical infrastructure networks and make recommendations for appropriate improvements. The study requires the NRC to review existing data to identify gaps in the security of critical infrastructure networks, make recommendations for research priorities to address these gaps, and review the security of network-related infrastructure including industrial process controls. A report of the study results is to be submitted to Congress. Authorizes $700,000 for the purpose of carrying out the study.

VII. COMMITTEE VIEWS

The Committee on Science believes that the Nation's cyber security research and development enterprise clearly needs strengthening. Not only is too little research in this important area being conducted, but the research that this being performed is too incremental to lead to breakthroughs. In addition, too few students are being trained in this field, perpetuating its current failings. The Cyber Security Research and Development Act raises the level of Federal funding for cyber security research significantly, investing

in two of the Federal Government's key scientific research agencies: NSF and NIST.

Building on NSF's proven capacity to mobilize the academic research community, the Act authorizes NSF to fund new academic centers and instructs NSF to fund research that is particularly innovative. Awardees selected under this program are to be selected through NSF's standard merit-review procedure. The merit-review system has been a key to NSF's success. The Committee recognizes, however, that review by outside panels has limitations, especially in underfunded fields, as the shortage of funds can lead review panels to reject research that is especially risky and lies outside the boundaries of the current paradigms.

In part for that reason, the Act also authorizes a grant program at NIST that is aimed at supporting the kind of high-risk research that might be overlooked by a system based on outside review. The Act authorizes NIST to use an administrative model that has been successfully implemented at the Defense Advanced Research Projects Agency (DARPA). In that model, talented project managers are invested with broad latitude to establish research objectives and to solicit and fund promising research proposals. This structure shortens the approval time for research proposals and allows the project manager to move quickly to invest in promising new ideas. In addition, the proposals submitted to NIST are expected to be focused on specific questions of more immediate interest to industry than are those submitted to NSF.

Recongizing that the lack of Federal leadership in the area of cyber security research has impeded progress, the Committee believes it is important that an agency assume a leadership role in the funding of computer and network security research. Thus the Act amends the NSF Organic Act—NSF's basic operating statute—to explicitly give NSF a leading role in cyber security research and education.

NATIONAL SCIENCE FOUNDATION RESEARCH

The Committee recognizes NSF's important role in computer and information science, including the agency's important contributions to the development of the Internet. The Committee also realizes that the NSF has already acknowledged the need for greater research in information assurance and has established the Trusted Computing program to fund small-scale academic research projects related to information assurance. However, the Committee believes that the expected level of funding for that program—between $4 million and $6 million—is insufficient to address the Nation's needs.

This Act provides significant additional funding—approximately $570 million for FY 2003 through FY 2007—for cyber security research. The Committee emphasizes that the list of research areas in section 4 is illustrative and not exhaustive.

While individual investigator research is needed to lay a firm foundation in information assurance, the Committee recognizes that large multidiciplinary efforts will be required to address the complex problems in this field. The Act provides funding to establish Computer and Network Security Research Centers to promote large-scale, multidisciplinary collaborations that exploit the collective knowledge of computer scientists, programmers, mathemati-

cians, cryptographers, systems engineers, software engineers, social scientists, and network architects, among others.

The Committee also recognizes the need for sustained funding over a substantial period of time to ensure that an institution has ample time to fully develop and implement high quality research programs, create technologically sophisticated facilities, attract or develop qualified faculty to support the instructional program, and recruit students. The Committee expects that the Computer and Network Security Research Centers will receive stable, long-term funding.

The Committee recognizes that the sensitive nature of some cyber security research results precludes their publication. The Committee encourages NSF to look beyond referred journal citations as proof of a particular individual's abilities and expertise or as evidence of a Center's accomplishments.

The Committee also encourages NSF to support projects and Centers with strong connections to the computer and network security user community, government laboratories, Federal agencies, and private sector companies that depend upon reliable information assurance technologies.

The Committee intends the term "governmental laboratories" to be construed in its broadest sense. It includes laboratories at both the state and Federal level, including government-owned, contractor-operated facilities.

COMPUTER AND NETWORK SECURITY CAPACITY BUILDING

The Committee firmly believes that the field of computer and network security cannot advance unless a major effort is made to prepare and recruit the Nation's best and brightest students to pursue higher education, and ultimately careers, in computer and network security. For this reason, the Act establishes several programs at the National Science Foundation to provide funds to institutions of higher education to develop and implement high-quality undergraduate and graduate programs in computer and network security and to attract students to them.

The Committee believes it is critical that institutional capacity at a number and variety of institutions have been designated by the National Security Agency as Centers of Academic Excellence in Information Assurance Education, those institutions alone cannot produce enough students to meet the projected need for 10,000 information assurance specialists by the year 2010. The Act authorizes NSF to provide merit-based Computer and Network Security Capacity Building grants to institutions of higher education, including two-year colleges, to establish or improve certificate, undergraduate and master's degree programs in computer and network security.

The Committee also believes that the computer and network security instructional programs supported through this program should be informed by the needs of the research and user communities and that students gain practical experience in the applications of security technologies in authentic settings by participating in government or industry internships.

And since computer and network security professionals with a variety of educational credentials will be required in the workforce, the program created under section 5 should fund a wide assortment

of institutions, including 2-year colleges, comprehensive colleges, and liberal arts institutions, as well as research universities.

The Committee expects that institutions applying for Capacity Building grants will provide an analysis of the potential for student enrollment as well as the potential for placement in computer and information security as part of their applications. Institutions are strongly encouraged to develop comprehensive recruitment, retention and placement strategies in partnership with K–12 schools, 2-year colleges, and local government and industry partners.

UNDERREPRESENTED GROUPS IN SCIENCE AND TECHNOLOGY

One important goal of the research and education activities by the bill is to increase the size and quality of the national research community engaged in research related to computer and network security. Applications for the NSF research center awards under section 4(b) must describe how the center will help increase the number of computer and network security researchers and other professionals. The NSF programs authorized under section 5, including the capacity building grants and the graduate traineeship program, and the NIST fellowship programs authorized under section 8 are specifically focused on enlarging the human resource base of the Nation for researchers and other specialties related to computer security.

The Committee directs NSF in managing its research and education activities authorized by the bill to ensure that active and sustained efforts are made to include the participation by individuals from groups traditionally underrepresented in science and engineering and by minority serving institutions. Further the Committee directs NSF to provide to the Committee within three years of the date of initiation of the activities authorized by this bill a report that (1) describes the actions taken by the Foundation to ensure participation by individuals from underrepresented groups and by minority serving institutions, (2) provides data on the numbers of individuals from underrepresented groups supported by fellowships, traineeships or research assistantships under activities authorized by the bill, and (3) describes the participation by minority serving institutions in activities authorized by the bill.

SCIENTIFIC AND ADVANCED TECHNOLOGY ACT OF 1992

The Committee recognizes the contributions of two-year colleges to meeting the rapidly evolving needs of the technical workforce. The Advanced Technological Education Program at NSF has contributed significantly to technician education through projects, national centers, regional centers, and articulation partnerships that bridge two-year and four-year colleges and universities. To date the NSF has funded 15 National Centers of Excellence that range in focus from biotechnology to environmental technology and information technology. The Committee feels that the growing demand for technical experts in computer and network security justifies the creation of at least one Center of Excellence focused on computer and network security. This Center should be selected through a competitive, merit-reviewed process and shall provide focus and resources for the national effort to enhance technical training in computer and information security in a variety of technical fields at two-year colleges across the U.S. The Committee also feels that a

number of project grants in computer and network security should be awarded to build the technical workforce and to develop a national network of technical training programs in computer and network security.

GRADUATE TRAINEESHIPS IN COMPUTER AND NETWORK SECURITY RESEARCH

Computer security research will not be able to move forward now or in the future unless universities increase the number of doctoral students trained in computer and network security or related areas. To accomplish that, graduate students need to receive tuition and stipend support, in addition to programs aimed at augmenting their research training.

The Committee believes that, in this case, the most effective way to provide this financial and programmatic support to graduate students is through traineeships. Traineeships, or grants to institutions of higher education for the purpose of providing support to graduate students, will enable institutions to develop focused programs that will complement and enhance the financial support given to students.

Like other NSF graduate fellowships, the fellowships available under this section will be available only to U.S. citizens, U.S. nationals, and legally admitted permanent resident aliens. However, the Committee recognizes that some foreign graduate students and post-doctoral students receive indirect support from NSF, as they are supported by funds from their research advisor's grants. Given the sensitive nature of computer and network security research, the Committee strongly encourages NSF to develop policies and procedures aimed to protect sensitive or classified information.

GRADUATE RESEARCH FELLOWSHIPS PROGRAM SUPPORT

The Committee values the Graduate Research Fellowship program at the National Science Foundation, which has helped recruit students to graduate programs in mathematics, science and engineering. While students pursuing graduate degrees in computer and network security are already eligible for fellowship awards under this program, the Committee believes that an explicit statement of this fact will enhance the student recruitment effort in computer and network security. Therefore, the Act instructs the Director to add computer and network security to the list of fields of specialization supported by the Graduate Research Fellowship program established under section 10 of the National Science Foundation Act of 1950.

FOSTERING RESEARCH AND EDUCATION IN COMPUTER AND NETWORK SECURITY

The Committee believes that the lack of a single Federal agency in a leadership role for research in cyber security is a factor that has hampered advancement of the field. Therefore, the Act amends the National Science Foundation Act of 1950 to charge NSF with a leadership role in fostering and supporting research and education activities to improve the security of networked information systems.

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY RESEARCH PROGRAM

Section 8 of the bill amends the NIST Act to establish an extramural research program centered on the security of computer systems. Awards are authorized for institutions of higher education that form partnerships with for-profit entities. The Committee expects that the research agenda of the program will be informed by the needs of industry and government.

In managing the research program, the Committee intends that NIST use the model developed by DARPA for managing its research programs. Consistent with that model, the bill specifies that the research program must be managed by program managers who have expertise in computer security research and also substantial knowledge of the vulnerabilities of existing computer systems. Ideal candidates will have a thorough knowledge of the needs of the user community as well as the capabilities of the research community that generates the basic knowledge and innovations needed to fulfill these needs.

The bill requires that program managers be given broad authority for defining the research goals of their programs, for identifying and motivating talented researchers to propose research projects to address the program goals, and for selecting specific research proposals for funding. Because of the large influence the program managers will have on the ultimate success of the research program, the Committee expects the NIST Director to carefully review the qualifications of potential program managers and to take advantage of the Intergovernmental Personnel Act and recruitment of new civil service employees, as well as current NIST employees, to ensure that highly qualified individuals are placed in these positions.

ATTRACTING NEW RESEARCHERS

While research funding is critical to ensuring advances in computer systems security research, a larger pool of talented researchers is also required to drive innovation at the necessary rate. While one way to promote the development and expansion of an able research community is by providing opportunities for junior researchers to gain post-doctoral training while initiating their own careers as independent investigators, another is to sponsor senior researchers interested in changing their research focus to problems of computer systems security. Therefore, the Act authorizes NIST to establish a program that would provide both post-doctoral research support to U.S. citizens, nationals, or permanent resident aliens in computer security research, and support for senior researchers.

DATA REQUIRED

The Committee directs NIST to include in the report required under section 22(e) of the NIST Act, as added by this bill, data on the numbers of individuals from underrepresented groups supported by fellowships or research assistantships by activities authorized by the bill, and a description of the participation by minority serving institutions in activities authorized by the bill.

VIII. Cost Estimate

Rule XIII, clause 3(d)(2) of the House of Representatives requires each committee report accompanying each bill or joint resolution of a public character to contain: (1) an estimate, made by such committee, of the costs which would be incurred in carrying out such bill or joint resolution in the fiscal year in which it is reported, and in each of the five fiscal years following such fiscal year (or for the authorized duration of any program authorized by such bill or joint resolution, if less than five years); (2) a comparison of the estimate of costs described in subparagraph (1) of this paragraph made by such committee with an estimate of such costs made by any Government agency and submitted to such committee; and (3) when practicable, a comparison of the total estimated funding level for the relevant program (or programs) with the appropriate levels under current law. However, House Rule XIII, clause 3(d)(B) provides that this requirement does not apply when a cost estimate and comparison prepared by the Director of the Congressional Budget Office under section 402 of the Congressional Budget Act of 1974 has been timely submitted prior to the filing of the report and included in the report pursuant to House Rule XIII, clause 3(c)(3). A cost estimate and comparison prepared by the Director of the Congressional Budget Office under section 402 of the Congressional Budget Act of 1974 has been timely submitted to the Committee on Science prior to the filing of this report and is included in Section IX of this report pursuant to House Rule XIII, clause 3(c)(3).

Rule XIII, clause 3(c)(2) of the House of Representatives requires each committee report that accompanies a measure providing new budget authority (other than continuing appropriations), new spending authority, or new credit authority, or charges in revenues or tax expenditures to contain a cost estimate, as required by section 308(a)(1) of the Congressional Budget Act of 1974 and, when practicable with respect to estimate of new budget authority, a comparison of the total estimated funding level for the relevant program (or programs) to the appropriate levels under current law. H.R. 3394 does not contain any new budget authority, credit authority, or changes in revenues or tax expenditures. Assuming that the sums authorized under the bill are appropriated, H.R. 3394 does authorize additional discretionary spending, as described in the Congressional Budget Office report on the bill, which is contained in Section IX of this report.

IX. Congressional Budget Office Cost Estimate

U.S. Congress,
Congressional Budget Office,
Washington, DC, December 17, 2001.

Hon. Sherwood L. Boehlert,
Chairman, Committee on Science,
House of Representatives, Washington, DC.

Dear Mr. Chairman: The Congressional Budget Office has prepared the enclosed cost estimate for H.R. 3394, the Cyber Security Research and Development Act.

If you wish further details on this estimate, we will be pleased to provide them. The CBO staff contact is Kathleen Gramp.

Sincerely,

BARRY B. ANDERSON, (FOR DAN L. CRIPPEN,
Director).

Enclosure.

H.R. 3394—Cyber Security Research and Development Act

Summary: H.R. 3394 would authorize appropriations for several research initiatives related to computer security at two agencies—the National Science Foundation (NSF) and the National Institute of Standards and Technology (NIST). The bill would establish the terms and conditions for awarding grants, fellowships, cooperative agreements related to computer security, and would authorize NIST to conduct similar research at its laboratories. It would authorize the appropriation of $878 million over the 2002–2007 period for these activities, and any amounts necessary to continue the fellowships and cooperative agreements at NIST through 2012. This total would include funding for the ongoing activities of the Computer System Security and Privacy Advisory Board and a study by the National Academy of Sciences on the vulnerability of the nation's network infrastructure.

Assuming appropriation of the specified amounts, CBO estimates that implementing this bill would cost $420 million over the 2002–2006 period. The bill would not affect direct spending or receipts; therefore, pay-as-you-go procedures would not apply.

H.R. 3394 contains no intergovernmental or private-sector mandates as defined in the Unfunded Mandates Reform Act (UMRA) and would impose no costs on state, local, or tribal governments.

Estimated cost to the Federal Government: The estimated budgetary impact of H.R. 3394 is shown in the following table. The costs of this legislation fall within budget functions 250 (general science, space, and technology) and 376 (commerce and housing credit). For this estimate, CBO assumes that funds will be appropriated near the beginning of each fiscal year and that outlays will occur at rates similar to those for other research programs at NSF and NIST.

	By fiscal year, in million of dollars—				
	2002	2003	2004	2005	2006
CHANGES IN SPENDING SUBJECT TO APPROPRIATION					
Authorization level	1	105	152	184	206
Estimated outlays	1	30	85	134	170

Pay-as-you-go considerations: None.

Estimated impact on State, local, and tribal governments: H.R. 3394 contains no intergovernmental mandates as defined in UMRA and would impose no costs on state, local, or tribal governments. The bill would benefit state governments by authorizing the appropriation of $878 million, much would be for grant programs to institutions of higher education (including public universities) to develop programs to improve the security of computer networks.

Estimated impact on the private sector: This bill contains no new private-sector mandates as defined in UMRA.

Estimate prepared by: Federal costs: Kathleen Gramp (National Science Foundation) and Ken Johnson (NIST); impact on State, local, and tribal governments: Elyse Goldman; impact on the private sector: Jean Talarico.

Estimate approved by: Peter H. Fontaine, Deputy Assistant Director for Budget Analysis.

X. Compliance With Public Law 104–4

H.R. 3394 contains no unfunded mandates.

XI. Committee Oversight Findings and Recommendations

Rule XIII, clause 3(c)(1) of the House of Representatives requires each committee report to include oversight findings and recommendations required pursuant to clause 2(b)(1) of rule X. The Committee on Science's oversight findings and recommendations are reflected in the body of this report.

XII. Constitutional Authority Statement

Rule XII, clause 3(d)(1) of the House of Representatives requires each report of a committee on a bill or joint resolution of a public character to include a statement citing the specific powers granted to the Congress in the Constitution to enact the law proposed by the bill or joint resolution. Article I, section 8 of the Constitution of the United States grants Congress the authority to enact H.R. 3394.

XIII. Federal Advisory Committee Statement

H.R. 3394 does not establish nor authorize the establishment of any advisory committee.

XIV. Congressional Accountability Act

The Committee finds that H.R. 3394 does not relate to the terms and conditions of employment or access to public services or accommodations within the meaning of section 102(b)(3) of the Congressional Accountability Act (Public Law 104–1).

XV. Statement on Preemption of State, Local, or Tribal Law

This bill is not intended to preempt any state, local, or tribal law.

XVI. Changes in Existing Law Made by the Bill, as Reported

In compliance with clause 3(e) of rule XIII of the Rules of the House of Representatives, changes in existing law made by the bill, as reported, are shown as follows (existing law proposed to be omitted is enclosed in black brackets, new matter is printed in italic, existing law in which no change is proposed is shown in roman):

SECTION 3 OF THE NATIONAL SCIENCE FOUNDATION ACT OF 1950

* * * * * * *

FUNCTIONS OF THE FOUNDATION

Sec. 3. (a) The Foundation is authorized and directed—

(1) * * *

* * * * * * *

(6) to provide a central clearinghouse for the collection, interpretation, and analysis of data on scientific and engineering and to provide a source of information for policy formulation by other agencies of the Federal Government; [and]

(7) to initiate and maintain a program for the determination of the total amount of money for scientific and engineering research, including money allocated for the construction of the facilities wherein such research is conducted, received by each educational institution and appropriate nonprofit organization in the United States, by grant, contract, or other arrangement from agencies of the Federal Government, and to report annually thereon to the President and the Congress[.]*; and*

(8) to take a leading role in fostering and supporting research and education activities to improve the security of networked information systems.

* * * * * * *

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY ACT

* * * * * * *

SEC. 20. (a) * * *

* * * * * * *

(d) As part of the research activities conducted in accordance with subsection (b)(4), the Institute shall—

(1) conduct a research program to address emerging technologies associated with assembling a networked computer system from components while ensuring it maintains desired security properties;

(2) carry out research and support standards development activities associated with improving the security of real-time computing and communications systems for use in process control; and

(3) carry out multidisciplinary, long-term, high-risk research on ways to improve the security of computer systems.

[(d)] *(e)* As used in this section—

(1) the term "computer system"—

(A) * * *

(B) includes—

(i) computers *and computer networks*;

* * * * * * *

(f) There are authorized to be appropriated to the Secretary $1,060,000 for fiscal year 2003 and $1,090,000 for fiscal year 2004 to enable the Computer System Security and Privacy Advisory Board, established by section 21, to identify emerging issues, including research needs, related to computer security, privacy, and cryptography and, as appropriate, to convene public meetings on those

subjects, receive presentations, and publish reports, digests, and summaries for public distribution on those subjects.

* * * * * * *

RESEARCH PROGRAM ON SECURITY OF COMPUTER SYSTEMS

SEC. 22. (a) ESTABLISHMENT.—The Director shall establish a program of assistance to institutions of higher education that enter into partnerships with for-profit entities to support research to improve the security of computer systems. The partnerships may also include government laboratories. The program shall—

(1) include multidisciplinary, long-term, high-risk research;

(2) include research directed toward addressing needs identified through the activities of the Computer System Security and Privacy Advisory Board under section 20(f); and

(3) promote the development of a robust research community working at the leading edge of knowledge in subject areas relevant to the security of computer systems by providing support for graduate students, post-doctoral researchers, and senior researchers.

(b) FELLOWSHIPS.—(1) The Director is authorized to establish a program to award post-doctoral research fellowships to individuals who are citizens, nationals, or lawfully admitted permanent resident aliens of the United States and are seeking research positions at institutions, including the Institute, engaged in research activities related to the security of computer systems, including the research areas described in section 4(a)(1) of the Cyber Security Research and Development Act.

(2) The Director is authorized to establish a program to award senior research fellowships to individuals seeking research positions at institutions, including the Institute, engaged in research activities related to the security of computer systems, including the research areas described in section 4(a)(1) of the Cyber Security Research and Development Act. Senior research fellowships shall be made available for established researchers at institutions of higher education who seek to change research fields and pursue studies related to the security of computer systems.

(3)(A) To be eligible for an award under this subsection, an individual shall submit an application to the Director at such time, in such manner, and containing such information as the Director may require.

(B) Under this subsection, the Director is authorized to provide stipends for post-doctoral research fellowships at the level of the Institute's Post Doctoral Research Fellowship Program and senior research fellowships at levels consistent with support for a faculty member in a sabbatical position.

(c) AWARDS; APPLICATIONS.—The Director is authorized to award grants or cooperative agreements to institutions of higher education to carry out the program established under subsection (a). To be eligible for an award under this section, an institution of higher education shall submit an application to the Director at such time, in such manner, and containing such information as the Director may require. The application shall include, at a minimum, a description of—

(1) the number of graduate students anticipated to participate in the research project and the level of support to be provided to each;

(2) the number of post-doctoral research positions included under the research project and the level of support to be provided to each;

(3) the number of individuals, if any, intending to change research fields and pursue studies related to the security of computer systems to be included under the research project and the level of support to be provided to each; and

(4) how the for-profit entities and any other partners will participate in developing and carrying out the research and education agenda of the partnership.

(d) PROGRAM OPERATION.—(1) The program established under subsection (a) shall be managed by individuals who shall have both expertise in research related to the security of computer systems and knowledge of the vulnerabilities of existing computer systems. The Director shall designate such individuals as program managers.

(2) Program managers designated under paragraph (1) may be new or existing employees of the Institute or individuals on assignment at the Institute under the Intergovernmental Personnel Act of 1970.

(3) Program managers designated under paragraph (1) shall be responsible for—

(A) establishing and publicizing the broad research goals for the program;

(B) soliciting applications for specific research projects to address the goals developed under subparagraph (A);

(C) selecting research projects for support under the program from among applications submitted to the Institute, following consideration of—

(i) the novelty and scientific and technical merit of the proposed projects;

(ii) the demonstrated capabilities of the individual or individuals submitting the applications to successfully carry out the proposed research;

(iii) the impact the proposed projects will have on increasing the number of computer security researchers;

(iv) the nature of the participation by for-profit entities and the extent to which the proposed projects address the concerns of industry; and

(v) other criteria determined by the Director, based on information specified for inclusion in applications under subsection (c); and

(D) monitoring the progress of research projects supported under the program.

(e) REVIEW OF PROGRAM.—(1) The Director shall periodically review the portfolio of research awards monitored by each program manager designated in accordance with subsection (d). In conducting those reviews, the Director shall seek the advice of the Computer System Security and Privacy Advisory Board, established under section 21, on the appropriateness of the research goals and on the quality and utility of research projects managed by program managers in accordance with subsection (d).

(2) The Director shall also contract with the National Research Council for a comprehensive review of the program established under subsection (a) during the 5th year of the program. Such review shall include an assessment of the scientific quality of the research conducted, the relevance of the research results obtained to the goals of the program established under subsection (d)(3)(A), and the progress of the program in promoting the development of a substantial academic research community working at the leading edge of knowledge in the field. The Director shall submit to Congress a report on the results of the review under this paragraph no later than six years after the initiation of the program.

(f) DEFINITIONS.—For purposes of this section—

(1) the term "computer system" has the meaning given that term in section 20(d)(1); and

(2) the term "institution of higher education" has the meaning given that term in section 101 of the Higher Education Act of 1965 (20 U.S.C. 1001).

* * * * * * *

SEC. [22] *32*. Appropriations to carry out the provisions of this Act may remain available for obligation and expenditure for such period or periods as may be specified in the Acts making such appropriations.

XVII. COMMITTEE RECOMMENDATIONS

On December 6, 2001, a quorum being present, the Committee on Science favorably reported the Cyber Security Research and Development Act, by a voice vote, and recommends its enactment.

XVIII. STATEMENT OF GENERAL PERFORMANCE GOALS AND OBJECTIVES

Pursuant to clause (3)(c) of House rule XIII, the goals of H.R. 3394 are (1) to increase the amount of innovative basic cyber security research being supported by the Federal Government; (2) to increase the number of world class researchers conducting cyber security research in the United States; (3) build new partnerships between industry, academia, and Federal agencies and laboratories; and (4) increase the number and quality of undergraduate and graduate students preparing for careers in information assurance research, development, and implementation.

XIX. EXCHANGE OF COMMITTEE CORRESPONDENCE

HOUSE OF REPRESENTATIVES,
COMMITTEE ON SCIENCE,
Washington, DC, January 28, 2002.

Hon. JOHN BOEHNER,
Chairman, Committee on Education and The Workforce, House of Representatives, Washington, DC.

DEAR CHAIRMAN BOEHNER: Thank you for your letter regarding the Education and the Workforce Committee's jurisdictional interest in H.R. 3394, the Cyber Security Research and Development Act.

I acknowledge your committee's jurisdiction over portions of H.R. 3394 and appreciate your cooperation in moving the bill to the

House floor expeditiously. I concur that your decision to forego further action on the bill will not prejudice the Education and Workforce Committee with respect to its jurisdictional prerogatives on H.R. 3394 or on similar or related legislation. Should a conference occur on H.R. 3394 or similar legislation, the Committee on Science will support your request to have conferees on this or similar legislation that falls within your Committee's jurisdiction. I will include a copy of your letter and this response in the Committee's report on the bill as well as in the Congressional Record when the House considers the legislation.

Once again, thank you for your cooperation in this matter.

Sincerely,

SHERWOOD L. BOEHLERT,
Chairman.

COMMITTEE ON EDUCATION
AND THE WORKFORCE,
Washington, DC, January 28, 2002.

Hon. SHERWOOD L. BOEHLERT,
Chairman, Committee on Science,
Rayburn HOB, Washington, DC.

DEAR CHAIRMAN BOEHLERT: Thank you for working with me regarding H.R. 3394, the "Cyber Security Research and Development Act", which was referred to the Committee on Science and in addition the Committee on Education and the Workforce, and ordered favorably reported by your Committee on December 6, 2001. I understand your desire to have this legislation considered expeditiously by the House; hence, I do not intend to hold a hearing or markup on this legislation.

In agreeing to waive consideration by our Committee, I would expect you to agree that this procedural route should not be construed to prejudice the Committee on Education and the Workforce's jurisdictional interest and prerogatives on this or any similar legislation and will not be considered as precedent for consideration of matters of jurisdictional interest to my Committee in the future. I would also expect your support in my request to the Speaker for the appointment of conferees from my Committee with respect to matters within the jurisdiction of my Committee should a conference with the Senate be convened on this or similar legislation.

I would appreciate your including our exchange of letters in your Committee's report to accompany H.R. 3394, which I understand you intend to file this week. Again, I thank you for working with me in developing this legislation and I look forward to working with you on these issues in the future.

Sincerely,

JOHN BOEHNER,
Chairman.

XX. PROCEEDINGS OF FULL COMMITTEE MARKUP

PROCEEDINGS OF THE FULL COMMITTEE MARKUP ON H.R. 3394, CYBER SECURITY RESEARCH AND DEVELOPMENT ACT, DECEMBER 6, 2001

The committee met, pursuant to call, at 11:10 a.m., in room 2318 of the Rayburn House Office Building, Hon. Sherwood L. Boehlert (chairman of the committee) presiding.

Chairman BOEHLERT. Good morning. The Committee on Science will be in order. Pursuant to notice, the Committee on Science is meeting today to consider the following measures, H.R. 3394, the Cyber Security Research and Development Act, and H.R. 3400, the Networking and Information Technology Research Advancement Act. I ask unanimous consent for the authority to recess the Committee at any point and, without objection, so ordered.

This morning we will mark up two important bills to boost our Nation's efforts in information technology. The first bill, H.R. 3394, which I introduced with my partner, Mr. Hall, creates new research programs to improve cyber security. The second bill, H.R. 3400, introduced by Research Subcommittee Chairman Nick Smith and Ranking Member Eddie Bernice Johnson, will augment and improve our existing interagency programs in networking and information technology.

Both bills have the hallmarks of Science Committee legislation. They promote targeted solutions to real problems that were raised by expert witnesses at Committee hearings. They are designed to solve problems over the long-run, not just temporarily; and they are bipartisan. Indeed, the majority and minority staffs of the Committee worked together on these bills from day one.

Let me say a bit more about H.R. 3394, the Cyber Security Research and Development Act, and Mr. Smith will discuss H.R. 3400 in detail when we take it up at a later time.

As I have pointed out repeatedly in recent weeks, the cyber security threat is real and potentially devastating. Experts from industry, government, and academia have told us that we simply do not have enough people conducting enough promising research on how to protect our computers and networks. And no federal agency is charged with solving that problem.

H.R. 3394 attacks those concerns head on. It creates new programs at the National Science Foundation and the National Institute of Standards and Technology to draw new researchers into the cyber security field, to promote incentives to conduct more creative research, and to encourage undergraduates, graduate students, and post-docs to study cyber security.

Right now, it's hard even to come up with a figure for how much the Federal Government is devoting to cyber security research, but the number is believed to be in the range of $60 million, a pittance, really, considering the risk. This bill authorizes almost $800 million over 5 years to build a cadre of researchers and to set them to work on the problem.

We hope to move this bill to the Floor early next year, and we are working with the Senate to develop a companion measure. This Committee must continue to lead the way in developing long-term solutions to the problems that have come to the forefront since September 11.

The Chair recognizes distinguished Ranking Member, Mr. Hall of Texas.

[Statement of Mr. Boehlert follows:]

OPENING STATEMENT OF HON. SHERWOOD BOEHLERT

This morning we will mark up two important bills to boost our nation's efforts in information technology. The first bill, H.R. 3394, which I introduced with Mr. Hall, creates new research programs to improve cybersecurity. The second, H.R. 3400, introduced by Research Subcommittee Chairman Nick Smith and Ranking Member Eddie Bernice Johnson, will augment and improve our existing interagency program in networking and information technology.

Both bills have the hallmarks of Science Committee legislation—they promote targeted solutions to real problems that were raised by expert witnesses at Committee hearings; they are designed to solve problems over the long-run, not just temporarily; and they are bipartisan. Indeed, the majority and minority staffs of the Committee worked together on these bills from day one.

Let me say a bit more about H.R. 3394, the "Cyber Security Research and Development Act," and Mr. Smith will discuss H.R. 3400 in detail when we take it up a little later.

As I've pointed out repeatedly in recent weeks, the cybersecurity threat is real and potentially devastating. Experts from industry, government and academia have told us that we simply do not have enough people conducting promising research on how to protect our computers and networks. And no federal agency is charged with solving that problem.

H.R. 3394 attacks those concerns head on. It creates new programs at the National Science Foundation and the National Institute of Standards and Technology to draw new researchers into the cyber security field, to provide incentives to conduct more creative research, and to encourage undergraduates, graduate students and post-docs to study cybersecurity.

Right now, it's hard even to come up with a figure for how much the federal government is devoting to cybersecurity research, but the number is believed to be in the range of $60 million—a pittance, really, considering the risk. This bill authorizes almost $800 million over five years to build a cadre of researchers and set them to work on the problem.

We hope to move this bill to the floor early next year, and we are working with the Senate to develop a companion measure.

This Committee must continue to lead the way in developing long-term solutions to the problems that have come to the fore since September 11th.

Mr. HALL. Mr. Chairman, thank you. And, of course, this bill just hopefully paves the way for better computer security. And when you say that, you have just about said everything you can say for the bill, and you covered it very well. As the Committee knows, in the past few years, computer virus attacks by the computer hackers and electronic identification theft have become more common, and the events this fall makes us realize how vulnerable we are.

We have had recent testimony before the Science Committee. These are too few scientists and too few engineers engaged in research on information security and too little funding for the security research, as you have pointed out.

H.R. 3394 simply establishes substantial new research programs at the National Science Foundation and the National Institute of Standards and Technology. And these programs will support graduate students, postdoctoral researchers, senior researchers, while encouraging stronger ties between universities and industry.

And the provisions pertaining to the thrust of these bills were first developed by Representative Baird and are contained in H.R. 3316, which is the bill he introduced a few weeks ago. I think that is very important and this Chairman and this Committee has given a lot of credence to that. I want to thank Congressman Baird for his important contribution to the legislation.

Mr. Chairman, if I could, I would like to yield to him for any comments he wishes to make, limited down to my 15 minutes.

[Statement of Mr. Hall follows:]

OPENING STATEMENT OF HON. RALPH M. HALL

The Cyber Security Research and Development Act, H.R. 3394, which Chairman Boehlert and I recently introduced, fills an important gap in current information technology research programs—namely, the need for better computer security.

In the past few years, computer viruses, attacks by computer hackers, and electronic identification theft have become more common. The events of this fall have made us realize just how vulnerable we are to attack and have underscored the need to enhance the protection of the Nation's physical and electronic infrastructure.

Recent testimony before the Science Committee highlighted an obstacle to achieving this goal. Currently there are too few scientists and engineers engaged in research on information security and too little funding for security research. and as federal agencies and private industry have found, there are few people with specialized computer security skills.

H.R. 3394 establishes substantial new research programs at the Nation Science Foundation and the National Institute of Standards and Technology. Programs at both agencies are multi-year and will increase the community of computer security researchers.

These programs will support graduate students, post-doctoral researchers and senior researchers, while encouraging stronger ties between universities and industry. This industry linkage will provide a reality check for the research priorities and will facilitate transfer of research results into new products and services.

The provisions pertaining to NIST were first developed by Rep. Baird and are contained in H.R. 3316, a bill he introduced a few weeks ago. I want to thank Congressman Baird for his important contribution to this legislation, and yield to him for any comments he wishes to make on the bill.

Chairman BOEHLERT. Without objection, go to.

Mr. BAIRD. Mr. Chairman, and, Ranking Member, thank you very much. I want to thank you for your leadership on this important issue. Certainly coming from the great State of Washington where technology is so important to our economy, we know these issues well. And I want to emphasize that this is not just about an economic issue. It is actually about saving human lives with our air traffic control system, emergency medical response, water production, et cetera, all governed and communicated through information technology. Making sure that technology and the infrastructure is secure is not just an economic good policy; it is about saving lives.

And I commend you for your leadership. Providing researchers and trained graduate students who can conduct research into this area is absolutely critical today and for the long-term viability of our economy. And I am privileged to be part of this. And thank you for including my statement.

Chairman BOEHLERT. Thank you very much, Mr. Baird. Without objection, all additional member opening statements will be placed in the record at this point.

[Statement of Mr. Smith of Michigan follows:]

OPENING STATEMENT OF HON. CONGRESSMAN NICK SMITH

Thank you, Mr. Chairman, for holding this markup today on two pieces of legislation that will significantly revamp our information technology and computer security research efforts. In keeping with the spirit of this Committee, I think we have put together two truly bipartisan bills will provide guidance and funding for important federal research and development challenges.

I am pleased to be the sponsor of one of these bills along with my friend and colleague Congresswoman Johnson of Texas. Our bill, H.R. 3400, the Networking and Information Technology Research and Advancement Act (NITRA), will update and re-authorize federally funded basic research in information technology. The bill authorizes a multi-agency research initiative that will ensure that America stays at

the cutting edge of new information technologies that stimulate economic growth, stimulate further scientific advancements, and make all of our lives better.

Additionally, I am proud to be a cosponsor of H.R. 3394, the Cybersecurity Research and Development Act, which will establish a research plan among several agencies to shore up the security of our computer systems. While much attention has been focused on other, more tangible forms of terrorism, we must not overlook the national security threat posed to our computer systems. In this age where we are increasingly dependent on computers for daily activities, the need for computer security cannot be understated. H.R. 3394 devotes significant resources to respond to these threats.

I urge members to support both of these bills that will strengthen our research efforts to foster innovation, continued economic growth, and improve our national security from the very real threat of cyberterrorism. I am looking forward to this markup, and I am hopeful that we can pass these bills through committee and move ahead with floor preparation as expeditiously as possible.

[Statement of Ms. Eddie Bernice Johnson follows:]

OPENING STATEMENT OF HON. EDDIE BERNICE JOHNSON

Mr. Speaker, I understand and support the Cyber Security Research and Development Act's aim to support research and education activities associated with increasing network and computer security.

The events over the last few months have given America more reasons to establish and sustain research programs to stimulate the development of vigorous research enterprise in network and computer security. Also, the events have provided us with another opportunity to reevaluate our society and to appreciate the wealth of diversity in our nation.

However, this legislation can provide an opportunity, which the language of the bill does not address. We can use this legislation to reiterate our commitment to diversity by providing an opportunity for us to ensure that everyone is provided the tools to succeed.

For this reason, I would like the opportunity to work with the Majority, before this bill goes to the House floor for a vote. My aim is to place language within H.R. 3394 that will encourage participation from individuals of traditionally underrepresented groups and minority serving institutions.

So often these individuals and institutions are unable to participate in the kinds of opportunities that this legislation will provide. I believe that we must make a valiant effort to include them as we have done in several pieces of legislation this committee has passed this session.

I have provided the Majority staff with the changes I am proposing and look forward to working with you in our endless efforts to ensure opportunity to all.

[Statement of Mr. Forbes follows:]

OPENING STATEMENT OF HON. J. RANDY FORBES

Mr. Chairman, I would like to express my strong support both for the Networking and Information Technology Research Advancement Act, as well as the Cyber Security Research and Development Act. As a cosponsor of both pieces of legislation, I appreciate my colleagues' efforts to coordinate our national response to the very serious threat of cyber terrorism.

Though it won't bring the death and destruction of biological or chemical weapons, cyber terrorism holds the power to disrupt our way of life, harm people's personal interests, and cause tremendous losses for businesses. Both bills before us are necessary for updating our national ability to thwart terrorist plots to disrupt our economy and do harm to our way of life using our own computer networks. As we heard from various witnesses who have come before this Committee over the past several months, have bright and innovative minds in this nation, but they need direction and coordination to maximize their efforts to find ways to prevent cyber terrorist attacks and ameliorate their consequences.

The bills before us today will coordinate the various research and development efforts that currently exist and increase the overall federal contribution for them. In addition, they will revise the rules under which federal dollars operate to give our science and technology experts the ability to think outside the box. Our enemies use their evil cunning as a weapon. We should not be restricted in our thinking to defeat their efforts.

Mr. Chairman, I appreciate your bringing these bills to our Committee so quickly. I am hopeful that they will get such prompt treatment by the Congress as a whole so that we can begin to implement this coordinated policy. Thank you.

Chairman BOEHLERT. We will now consider H.R. 3394, the Cyber Security Research and Development Act. I ask unanimous consent that the bill be considered as read and open to amendment at any point. And I ask the members to proceed with the amendments in the order on the roster. And since we don't have a roster, I will ask, are there any amendments? Mr. Matheson.

Mr. MATHESON. I have none.

Chairman BOEHLERT. Okay. Okay. All right. Yes. Who do—do I see a hand? Ms. Johnson.

Ms. JOHNSON. Thank you, Mr. Chairman. I want to express my appreciation, and I have an amendment at the desk and would like to ask for that consideration. I have been in contact with the staff. And all it does is simply request the research dollars to keep in mind the Historically Black Universities and—Colleges and Universities, as well as the Hispanic Serving Colleges and Universities, as the money is distributed. And I would be happy to work with you and the staff with——

Chairman BOEHLERT. And I will look forward to working with you. This is a cause near and dear to your heart and to mine also. So we will work cooperatively and do something for the Floor.

Ms. JOHNSON. Thank you very much, Mr. Chairman.

Chairman BOEHLERT. Anyone else seek recognition? Any further discussion? If no, the vote occurs on the bill. Okay. I reported—we haven't got—I am just trying to count for numbers. You are worth two, Jim. All right. We are just 23, 24. We are getting there.

Mr. MATHSON. Okay.

Chairman BOEHLERT. Do I hear 25? Are we all set? Yeah. Here we are. Since there are no further discussion, no further amendments, the vote occurs on the bill. All in favor, say aye. Noes? The ayes have it. Without objection, the bill is ordered reported.

Mr. HALL. Mr. Chairman——

Chairman BOEHLERT. Yes, sir.

Mr. HALL. Mr. Chairman——

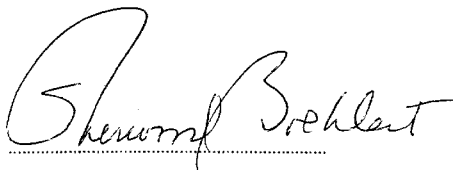
Chairman BOEHLERT. Mr. Hall.

Mr. HALL. I move that the Committee favorably report H.R. 3394 to the House with the recommendation that the bill do pass. Furthermore, I move the staff be instructed to prepare the legislative report and make the necessary and technical and conforming changes, and that the Chairman take all necessary steps to bring the bill before the House for consideration. I yield back my time.

Chairman BOEHLERT. All right. The Chair notes the presence of a reporting quorum. The question is on the motion to report the bill favorably. Those in favor of the motion will signify by saying aye. Opposed, no. The ayes appear to have it. The bill is favorably reported. Without objection, the motion to reconsider is laid upon the table. I move that members have 2 subsequent calendar days in which to submit supplemental, minority, or additional views on the measure. Without objection, so ordered.

I move, pursuant to Clause 1 of the Rule 22 of the House—Rules of the House of Representatives, that the Committee authorize the Chairman to offer such motions as may be necessary in the House to go to conference with the Senate on the bill H.R. 3394, or a similar Senate bill. Without objection, so ordered.

[H.R. 3394 follows:]



(Original Signature of Member)

107TH CONGRESS
1ST SESSION

H. R. 3394

IN THE HOUSE OF REPRESENTATIVES

Mr. BOEHLERT (for himself, Mr. HALL of Texas, Mr. SMITH of Texas, Mr. BAIRD, Mr. SMITH of Michigan, and Ms. EDDIE BERNICE JOHNSON of Texas) introduced the following bill; which was referred to the Committee on _____

A BILL

To authorize funding for computer and network security research and development and research fellowship programs, and for other purposes.

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

SECTION 1. SHORT TITLE.

This Act may be cited as the "Cyber Security Research and Development Act".

SEC. 2. FINDINGS.

The Congress finds the following:

(1) Revolutionary advancements in computing and communications technology have interconnected government, commercial, scientific, and educational infrastructures—including critical infrastructures for electric power, natural gas and petroleum production and distribution, telecommunications, transportation, water supply, banking and finance, and emergency and government services—in a vast, interdependent physical and electronic network.

(2) Exponential increases in interconnectivity have facilitated enhanced communications, economic growth, and the delivery of services critical to the public welfare, but have also increased the consequences of temporary or prolonged failure.

(3) A Department of Defense Joint Task Force concluded after a 1997 United States information warfare exercise that the results "clearly demonstrated our lack of preparation for a coordinated cyber and physical attack on our critical military and civilian infrastructure".

(4) Computer security technology and systems implementation lack—

(A) sufficient long term research funding;

(B) adequate coordination across Federal and State government agencies and among government, academia, and industry;

(C) sufficient numbers of outstanding researchers in the field; and

(D) market incentives for the design of commercial and consumer security solutions.

(5) Accordingly, Federal investment in computer and network security research and development must be significantly increased to—

(A) improve vulnerability assessment and technological and systems solutions;

(B) expand and improve the pool of information security professionals, including researchers, in the United States workforce; and

(C) better coordinate information sharing and collaboration among industry, government, and academic research projects.

SEC. 3. DEFINITIONS.

For purposes of this Act—

(1) the term "Director" means the Director of the National Science Foundation; and

(2) the term "institution of higher education" has the meaning given that term in section 101 of

the Higher Education Act of 1965 (20 U.S.C. 1001).

SEC. 4. NATIONAL SCIENCE FOUNDATION RESEARCH.

(a) COMPUTER AND NETWORK SECURITY RESEARCH GRANTS.—

(1) IN GENERAL.—The Director shall award grants for basic research on innovative approaches to the structure of computer and network hardware and software that are aimed at enhancing computer security. Research areas may include—

(A) authentication and cryptography;

(B) computer forensics and intrusion detection;

(C) reliability of computer and network applications, middleware, operating systems, and communications infrastructure; and

(D) privacy and confidentiality.

(2) MERIT REVIEW; COMPETITION.—Grants shall be awarded under this section on a merit-reviewed competitive basis.

(3) AUTHORIZATION OF APPROPRIATIONS.—There are authorized to be appropriated to the National Science Foundation to carry out this subsection—

(A) $35,000,000 for fiscal year 2003;

(B) $40,000,000 for fiscal year 2004;

(C) $46,000,000 for fiscal year 2005;

(D) $52,000,000 for fiscal year 2006; and

(E) $60,000,000 for fiscal year 2007.

(b) COMPUTER AND NETWORK SECURITY RESEARCH CENTERS.—

(1) IN GENERAL.—The Director shall award multiyear grants, subject to the availability of appropriations, to institutions of higher education (or consortia thereof) to establish multidisciplinary Centers for Computer and Network Security Research. Institutions of higher education (or consortia thereof) receiving such grants may partner with one or more government laboratories or for-profit institutions.

(2) MERIT REVIEW; COMPETITION.—Grants shall be awarded under this subsection on a merit-reviewed competitive basis.

(3) PURPOSE.—The purpose of the Centers shall be to generate innovative approaches to computer and network security by conducting cutting-edge, multidisciplinary research in computer and network security, including the research areas described in subsection (a)(1).

(4) APPLICATIONS.—An institution of higher education (or a consortium of such institutions)

seeking funding under this subsection shall submit an application to the Director at such time, in such manner, and containing such information as the Director may require. The application shall include, at a minimum, a description of—

(A) the research projects that will be undertaken by the Center and the contributions of each of the participating entities;

(B) how the Center will promote active collaboration among scientists and engineers from different disciplines, such as computer scientists, engineers, mathematicians, and social science researchers; and

(C) how the Center will contribute to increasing the number of computer and network security researchers and other professionals.

(5) CRITERIA.—In evaluating the applications submitted under paragraph (4), the Director shall consider, at a minimum—

(A) the ability of the applicant to generate innovative approaches to computer and network security and effectively carry out the research program;

(B) the experience of the applicant in conducting research on computer and network se-

curity and the capacity of the applicant to foster new multidisciplinary collaborations;

(C) the capacity of the applicant to attract and provide adequate support for undergraduate and graduate students and postdoctoral fellows to pursue computer and network security research; and

(D) the extent to which the applicant will partner with government laboratories or for-profit entities, and the role the government laboratories or for-profit entities will play in the research undertaken by the Center.

(6) ANNUAL MEETING.—The Director shall convene an annual meeting of the Centers in order to foster collaboration and communication between Center participants.

(7) AUTHORIZATION OF APPROPRIATIONS.—There are authorized to be appropriated for the National Science Foundation to carry out this subsection—

(A) $12,000,000 for fiscal year 2003;

(B) $24,000,000 for fiscal year 2004;

(C) $36,000,000 for fiscal year 2005;

(D) $36,000,000 for fiscal year 2006; and

(E) $36,000,000 for fiscal year 2007.

SEC. 5. NATIONAL SCIENCE FOUNDATION COMPUTER AND NETWORK SECURITY PROGRAMS.

(a) COMPUTER AND NETWORK SECURITY CAPACITY BUILDING GRANTS.—

(1) IN GENERAL.—The Director shall establish a program to award grants to institutions of higher education (or consortia thereof) to establish or improve undergraduate and master's degree programs in computer and network security, to increase the number of students who pursue undergraduate or master's degrees in fields related to computer and network security, and to provide students with experience in government or industry related to their computer and network security studies.

(2) MERIT REVIEW.—Grants shall be awarded under this subsection on a merit-reviewed competitive basis.

(3) USE OF FUNDS.—Grants awarded under this subsection shall be used for activities that enhance the ability of an institution of higher education (or consortium thereof) to provide high-quality undergraduate and master's degree programs in computer and network security and to recruit and retain increased numbers of students to such programs. Activities may include—

(A) revising curriculum to better prepare undergraduate and master's degree students for careers in computer and network security;

(B) establishing degree and certificate programs in computer and network security;

(C) creating opportunities for undergraduate students to participate in computer and network security research projects;

(D) acquiring equipment necessary for student instruction in computer and network security, including the installation of testbed networks for student use;

(E) providing opportunities for faculty to work with local or Federal Government agencies, private industry, or other academic institutions to develop new expertise or to formulate new research directions in computer and network security;

(F) establishing collaborations with other academic institutions or departments that seek to establish, expand, or enhance programs in computer and network security;

(G) establishing student internships in computer and network security at government agencies or in private industry;

(H) establishing or enhancing bridge programs in computer and network security between community colleges and universities; and

(I) any other activities the Director determines will accomplish the goals of this subsection.

(4) SELECTION PROCESS.—

(A) APPLICATION.—An institution of higher education (or a consortium thereof) seeking funding under this subsection shall submit an application to the Director at such time, in such manner, and containing such information as the Director may require. The application shall include, at a minimum—

(i) a description of the applicant's computer and network security research and instructional capacity, and in the case of an application from a consortium of institutions of higher education, a description of the role that each member will play in implementing the proposal;

(ii) a comprehensive plan by which the institution or consortium will build instructional capacity in computer and information security;

(iii) a description of relevant collaborations with government agencies or private industry that inform the instructional program in computer and network security;

(iv) a survey of the applicant's historic student enrollment and placement data in fields related to computer and network security and a study of potential enrollment and placement for students enrolled in the proposed computer and network security program; and

(v) a plan to evaluate the success of the proposed computer and network security program, including post-graduation assessment of graduate school and job placement and retention rates as well as the relevance of the instructional program to graduate study and to the workplace.

(B) AWARDS.—(i) The Director shall ensure, to the extent practicable, that grants are awarded under this subsection in a wide range of geographic areas and categories of institutions of higher education.

(ii) The Director shall award grants under this subsection for a period not to exceed 5 years.

(5) ASSESSMENT REQUIRED.—The Director shall evaluate the program established under this subsection no later than 6 years after the establishment of the program. At a minimum, the Director shall evaluate the extent to which the grants achieved their objectives of increasing the quality and quantity of students pursuing undergraduate or master's degrees in computer and network security.

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

(A) $15,000,000 for fiscal year 2003;

(B) $20,000,000 for fiscal year 2004;

(C) $20,000,000 for fiscal year 2005;

(D) $20,000,000 for fiscal year 2006; and

(E) $20,000,000 for fiscal year 2007.

(b) SCIENTIFIC AND ADVANCED TECHNOLOGY ACT OF 1992.—

(1) GRANTS.—The Director shall provide grants under the Scientific and Advanced Technology Act of 1992 for the purposes of section 3(a)

and (b) of that Act, except that the activities supported pursuant to this subsection shall be limited to improving education in fields related to computer and network security.

(2) AUTHORIZATION OF APPROPRIATIONS.—There are authorized to be appropriated to the National Science Foundation to carry out this subsection—

(A) $1,000,000 for fiscal year 2003;

(B) $1,250,000 for fiscal year 2004;

(C) $1,250,000 for fiscal year 2005;

(D) $1,250,000 for fiscal year 2006; and

(E) $1,250,000 for fiscal year 2007.

(c) GRADUATE TRAINEESHIPS IN COMPUTER AND NETWORK SECURITY RESEARCH.—

(1) IN GENERAL.—The Director shall establish a program to award grants to institutions of higher education to establish traineeship programs for graduate students who pursue computer and network security research leading to a doctorate degree by providing funding and other assistance, and by providing graduate students with research experience in government or industry related to the students' computer and network security studies.

(2) MERIT REVIEW.—Grants shall be provided under this subsection on a merit-reviewed competitive basis.

(3) USE OF FUNDS.—An institution of higher education shall use grant funds for the purposes of—

(A) providing fellowships to students who are citizens, nationals, or lawfully admitted permanent resident aliens of the United States and are pursuing research in computer or network security leading to a doctorate degree;

(B) paying tuition and fees for students receiving fellowships under subparagraph (A);

(C) establishing scientific internship programs for students receiving fellowships under subparagraph (A) in computer and network security at for-profit institutions or government laboratories; and

(D) other costs associated with the administration of the program.

(4) FELLOWSHIP AMOUNT.—Fellowships provided under paragraph (3)(A) shall be in the amount of $25,000 per year, or the level of the National Science Foundation Graduate Research Fellowships, whichever is greater, for up to 3 years.

(5) SELECTION PROCESS.—An institution of higher education seeking funding under this subsection shall submit an application to the Director at such time, in such manner, and containing such information as the Director may require. The application shall include, at a minimum, a description of—

(A) the instructional program and research opportunities in computer and network security available to graduate students at the applicant's institution; and

(B) the internship program to be established, including the opportunities that will be made available to students for internships at for-profit institutions and government laboratories.

(6) REVIEW OF APPLICATIONS.—In evaluating the applications submitted under paragraph (5), the Director shall consider—

(A) the ability of the applicant to effectively carry out the proposed program;

(B) the quality of the applicant's existing research and education programs;

(C) the likelihood that the program will recruit increased numbers of students to pursue

and earn doctorate degrees in computer and network security;

(D) the nature and quality of the internship program established through collaborations with government laboratories and for-profit institutions;

(E) the integration of internship opportunities into graduate students' research; and

(F) the relevance of the proposed program to current and future computer and network security needs.

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

(A) $10,000,000 for fiscal year 2003;

(B) $20,000,000 for fiscal year 2004;

(C) $20,000,000 for fiscal year 2005;

(D) $20,000,000 for fiscal year 2006; and

(E) $20,000,000 for fiscal year 2007.

(d) GRADUATE RESEARCH FELLOWSHIPS PROGRAM SUPPORT.— Computer and network security shall be included among the fields of specialization supported by the National Science Foundation's Graduate Research Fellow-

ships program under section 10 of the National Science Foundation Act of 1950 (42 U.S.C. 1869).

SEC. 6. CONSULTATION.

In carrying out sections 4 and 5, the Director shall consult with other Federal agencies.

SEC. 7. FOSTERING RESEARCH AND EDUCATION IN COMPUTER AND NETWORK SECURITY.

Section 3(a) of the National Science Foundation Act of 1950 (42 U.S.C. 1862(a)) is amended—

(1) by striking "and" at the end of paragraph (6);

(2) by striking the period at the end of paragraph (7) and inserting "; and"; and

(3) by adding at the end the following new paragraph:

"(8) to take a leading role in fostering and supporting research and education activities to improve the security of networked information systems.".

SEC. 8. NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY RESEARCH PROGRAM.

The National Institute of Standards and Technology Act is amended—

(1) by moving section 22 to the end of the Act and redesignating it as section 32;

(2) by inserting after section 21 the following new section:

"RESEARCH PROGRAM ON SECURITY OF COMPUTER SYSTEMS

"SEC. 22. (a) ESTABLISHMENT.—The Director shall establish a program of assistance to institutions of higher education that enter into partnerships with for-profit entities to support research to improve the security of computer systems. The partnerships may also include government laboratories. The program shall—

"(1) include multidisciplinary, long-term, high-risk research;

"(2) include research directed toward addressing needs identified through the activities of the Computer System Security and Privacy Advisory Board under section 20(f); and

"(3) promote the development of a robust research community working at the leading edge of knowledge in subject areas relevant to the security of computer systems by providing support for graduate students, post-doctoral researchers, and senior researchers.

"(b) FELLOWSHIPS.—(1) The Director is authorized to establish a program to award post-doctoral research fellowships to individuals who are citizens, nationals, or lawfully admitted permanent resident aliens of the United

States and are seeking research positions at institutions, including the Institute, engaged in research activities related to the security of computer systems, including the research areas described in section 4(a)(1) of the Cyber Security Research and Development Act.

"(2) The Director is authorized to establish a program to award senior research fellowships to individuals seeking research positions at institutions, including the Institute, engaged in research activities related to the security of computer systems, including the research areas described in section 4(a)(1) of the Cyber Security Research and Development Act. Senior research fellowships shall be made available for established researchers at institutions of higher education who seek to change research fields and pursue studies related to the security of computer systems.

"(3)(A) To be eligible for an award under this subsection, an individual shall submit an application to the Director at such time, in such manner, and containing such information as the Director may require.

"(B) Under this subsection, the Director is authorized to provide stipends for post-doctoral research fellowships at the level of the Institute's Post Doctoral Research Fellowship Program and senior research fellowships at levels consistent with support for a faculty member in a sabbatical position.

"(c) AWARDS; APPLICATIONS.—The Director is authorized to award grants or cooperative agreements to institutions of higher education to carry out the program established under subsection (a). To be eligible for an award under this section, an institution of higher education shall submit an application to the Director at such time, in such manner, and containing such information as the Director may require. The application shall include, at a minimum, a description of—

"(1) the number of graduate students anticipated to participate in the research project and the level of support to be provided to each;

"(2) the number of post-doctoral research positions included under the research project and the level of support to be provided to each;

"(3) the number of individuals, if any, intending to change research fields and pursue studies related to the security of computer systems to be included under the research project and the level of support to be provided to each; and

"(4) how the for-profit entities and any other partners will participate in developing and carrying out the research and education agenda of the partnership.

"(d) PROGRAM OPERATION.—(1) The program established under subsection (a) shall be managed by individuals who shall have both expertise in research related to the security of computer systems and knowledge of the vulnerabilities of existing computer systems. The Director shall designate such individuals as program managers.

"(2) Program managers designated under paragraph (1) may be new or existing employees of the Institute or individuals on assignment at the Institute under the Intergovernmental Personnel Act of 1970.

"(3) Program managers designated under paragraph (1) shall be responsible for—

"(A) establishing and publicizing the broad research goals for the program;

"(B) soliciting applications for specific research projects to address the goals developed under subparagraph (A);

"(C) selecting research projects for support under the program from among applications submitted to the Institute, following consideration of—

"(i) the novelty and scientific and technical merit of the proposed projects;

"(ii) the demonstrated capabilities of the individual or individuals submitting the applica-

tions to successfully carry out the proposed research;

"(iii) the impact the proposed projects will have on increasing the number of computer security researchers;

"(iv) the nature of the participation by for-profit entities and the extent to which the proposed projects address the concerns of industry; and

"(v) other criteria determined by the Director, based on information specified for inclusion in applications under subsection (c); and

"(D) monitoring the progress of research projects supported under the program.

"(e) REVIEW OF PROGRAM.—(1) The Director shall periodically review the portfolio of research awards monitored by each program manager designated in accordance with subsection (d). In conducting those reviews, the Director shall seek the advice of the Computer System Security and Privacy Advisory Board, established under section 21, on the appropriateness of the research goals and on the quality and utility of research projects managed by program managers in accordance with subsection (d).

"(2) The Director shall also contract with the National Research Council for a comprehensive review of the

program established under subsection (a) during the 5th year of the program. Such review shall include an assessment of the scientific quality of the research conducted, the relevance of the research results obtained to the goals of the program established under subsection (d)(3)(A), and the progress of the program in promoting the development of a substantial academic research community working at the leading edge of knowledge in the field. The Director shall submit to Congress a report on the results of the review under this paragraph no later than six years after the initiation of the program.

"(f) DEFINITIONS.—For purposes of this section—

"(1) the term 'computer system' has the meaning given that term in section 20(d)(1); and

"(2) the term 'institution of higher education' has the meaning given that term in section 101 of the Higher Education Act of 1965 (20 U.S.C. 1001)."; and

(3) in section 20(d)(1)(B)(i) (15 U.S.C. 278g–3(d)(1)(B)(i)), by inserting "and computer networks" after "computers".

SEC. 9. COMPUTER SECURITY REVIEW, PUBLIC MEETINGS, AND INFORMATION.

Section 20 of the National Institute of Standards and Technology Act (15 U.S.C. 278g–3) is amended by adding at the end the following new subsection:

"(f) There are authorized to be appropriated to the Secretary $1,060,000 for fiscal year 2003 and $1,090,000 for fiscal year 2004 to enable the Computer System Security and Privacy Advisory Board, established by section 21, to identify emerging issues, including research needs, related to computer security, privacy, and cryptography and, as appropriate, to convene public meetings on those subjects, receive presentations, and publish reports, digests, and summaries for public distribution on those subjects.".

SEC. 10. INTRAMURAL SECURITY RESEARCH.

Section 20 of the National Institute of Standards and Technology Act (15 U.S.C. 278g–3) is further amended—

(1) by redesignating subsection (d) as subsection (e); and

(2) by inserting after subsection (c) the following new subsection:

"(d) As part of the research activities conducted in accordance with subsection (b)(4), the Institute shall—

"(1) conduct a research program to address emerging technologies associated with assembling a

networked computer system from components while ensuring it maintains desired security properties;

"(2) carry out research and support standards development activities associated with improving the security of real-time computing and communications systems for use in process control; and

"(3) carry out multidisciplinary, long-term, high-risk research on ways to improve the security of computer systems.".

SEC. 11. AUTHORIZATION OF APPROPRIATIONS.

There are authorized to be appropriated to the Secretary of Commerce for the National Institute of Standards and Technology—

(1) for activities under section 22 of the National Institute of Standards and Technology Act, as added by section 8 of this Act—

(A) $25,000,000 for fiscal year 2003;

(B) $40,000,000 for fiscal year 2004;

(C) $55,000,000 for fiscal year 2005;

(D) $70,000,000 for fiscal year 2006;

(E) $85,000,000 for fiscal year 2007; and

(F) such sums as may be necessary for fiscal years 2008 through 2012; and

(2) for activities under section 20(d) of the National Institute of Standards and Technology Act, as added by section 10 of this Act—

(A) $6,000,000 for fiscal year 2003;

(B) $6,200,000 for fiscal year 2004;

(C) $6,400,000 for fiscal year 2005;

(D) $6,600,000 for fiscal year 2006; and

(E) $6,800,000 for fiscal year 2007.

SEC. 12. NATIONAL ACADEMY OF SCIENCES STUDY ON COMPUTER AND NETWORK SECURITY IN CRITICAL INFRASTRUCTURES.

(a) STUDY.—Not later than 3 months after the date of the enactment of this Act, the Director of the National Institute of Standards and Technology shall enter into an arrangement with the National Research Council of the National Academy of Sciences to conduct a study of the vulnerabilities of the Nation's network infrastructure and make recommendations for appropriate improvements. The National Research Council shall—

(1) review existing studies and associated data on the architectural, hardware, and software vulnerabilities and interdependencies in United States critical infrastructure networks;

(2) identify and assess gaps in technical capability for robust critical infrastructure network secu-

rity, and make recommendations for research priorities and resource requirements; and

(3) review any and all other essential elements of computer and network security, including security of industrial process controls, to be determined in the conduct of the study.

(b) REPORT.—The Director of the National Institute of Standards and Technology shall transmit a report containing the results of the study and recommendations required by subsection (a) to the Congress not later than 21 months after the date of enactment of this Act.

(c) SECURITY.—The Director of the National Institute of Standards and Technology shall ensure that no information that is classified is included in any publicly released version of the report required by this section.

(d) AUTHORIZATION OF APPROPRIATIONS.—There are authorized to be appropriated to the Secretary of Commerce for the National Institute of Standards and Technology for the purposes of carrying out this section, $700,000.

[The information follows:]

H.R. 3394—THE CYBER SECURITY RESEARCH AND DEVELOPMENT ACT, INTRODUCED BY MR. BOEHLERT, MR. HALL (TX), MR. SMITH (TX), MR. BAIRD, MR. SMITH (MI), AND MS. EDDIE BERNICE JOHNSON (TX)

SECTION-BY-SECTION SUMMARY

Sec. 1. Short title

"Cyber Security Research and Development Act"

Sec. 2. Findings

Discuss the interdependent nature of critical infrastructures brought about by advancements in computing and communications technology; the increased consequences of failure of communications and other critical services caused by exponential increases in interconnectivity; the nation's lack of preparedness for a coordinated cyber and physical attack; the lack of sufficient long-term research funding and the shortage of outstanding researchers in the field of cyber security; and the lack of coordination among government, academia, and industry for computer security; and the need to significantly increase the Federal investment in computer and network security research and development.

Sec. 3. Definitions

Defines the term 'Director' as the Director of the National Science Foundation (NSF) (Note that where the term 'Director' is used in section 8 it refers to the Director of the National Institute for Standards and Technology (NIST)). Uses the definition for 'institution of higher education' found in the Higher Education Act of 1965.

Sec. 4. National Science Foundation research

(1) Establishes an NSF program to award merit-based grants for basic research on innovative approaches to enhance computer security. Research areas for which grants can be used include authentication and cryptography, computer forensics and intrusion detection, reliability of computer and network applications, and privacy. Authorizes appropriations of $35 million for FY 2003, $40 million for FY 2004, $46 million for 2005, $52 million for FY 2006, and $60,000 for FY 2007.

(b) Establishes an NSF program to award multi-year grants to institutions of higher education (or consortia thereof) to establish multidisciplinary Centers for Computer and Network Security Research. Consortia applying for grants may partner with one or more government laboratories or for-profit institutions. Applications for Center grants are to be reviewed on the basis of criteria that include: the ability of the institution (or consortium) to generate innovative approaches to computer and network security research; the applicant's support for students pursuing research in computer and network security; and the extent to which government laboratories or industry partners will participate in the Center's research activities. Requires the Director to convene an annual meeting of Centers to foster greater collaboration and communication. Authorizes appropriations of $12 million for FY 2003, $24 million for FY 2004, $36 million for FY 2005, and $36 million for FY 2006 and FY 2007.

Sec. 5. National Science Foundation computer and network security programs

(a) Establishes a competitive, merit-based NSF program to award grants to institutions of higher education (or consortia thereof) to create or improve undergraduate and master's degree programs in computer security. Grants can be used for uses that include curriculum development, equipment acquisition, faculty enhancement, and the establishment of a student internship program in government or industry. Requires applicants to describe the plan for building increased capacity in computer and network security, to articulate the roles and responsibilities of each partnering institution or collaborative group, and to provide evidence of high potential for success in educating and placing students in relevant jobs or graduate programs. Instructs the Director to evaluate the impact of the program on increasing the quality and quantity of computer and network security professionals. Authorizes $15 million for FY 2003 and $20 million for each of fiscal years 2004–2007.

(b) Expands NSF's existing program for community colleges (established by the Scientific and Advanced Technology Act of 1992) to include grants to improve education in fields related to computer and network security. Authorizes $1 million for FY 2003 and $1.25 million for each of fiscal years 2004–2007.

(c) Establishes a competitive, merit-based NSF program to award grants to institutions of higher education to establish programs for students pursuing studies in computer and network security research leading to a doctorate degree. Grant funds are to be used to support student fellowships of at least $25,000 per year, to pay student tuition and fees, and to support students in scientific internship programs.

Authorizes appropriations of $10 million for FY 2003, and $20 million for each fiscal year 2004–2007.

(d) Directs NSF to include computer and network security as an approved field of specialization under its current Graduate Research Fellowships program.

Sec. 6. Consultation

Requires the NSF Director to consult with other Federal agencies in carrying out the programs described in Sections 4 and 5.

Sec. 7. Fostering research and education in computer and network security

Amends the National Science Foundation Act of 1950 to require NSF to take a leading role in fostering and supporting research and education in computer and network security.

Sec. 8. National Institute of Standards and Technology Research Program

Amends the National Institute of Standards and Technology Act to establish a program that provides assistance to institutions of higher education that partner with for-profit entities to support multidisciplinary, long-term, high-risk research to improve the security of computer systems. Partnerships may also include government laboratories. Authorizes the Director to award research fellowships to postdoctoral researchers engaged in computer security research and to senior researchers who wish to transition from other research fields to computer security research. Instructs the NIST Director to select Program Managers who are responsible for establishing the research goals for the program, soliciting applications for specific research projects to address these goals, and selecting research projects for funding. Calls for the NIST Director to periodically review the portfolio of research awards in consultation with NIST's existing Computer System Security and Privacy Advisory Board. Also instructs the Director to contract with the National Academy of Sciences to conduct a formal review of the program and to submit a report of this review to Congress.

Sec. 9. Computer security review, public meetings, and information

Authorizes funding ($1,060,000 for FY 2003 and $1,090,000 for FY 2004) to enable NIST's Computer System Security and Privacy Advisory Board to identify emerging issues, including research needs related to computer security, privacy, and cryptography and, as appropriate, to convene public meetings on those subjects, receive presentations, and generate reports for public distribution.

Sec. 10. Intramural security research

Amends the National Institute of Standards and Technology Act authorize NIST to pursue, as part of the agency's in-house research program, research related to computer security including the development of emerging technologies to ensure security of networked systems assembled from components, improved security of real-time computing and communications systems used in industrial and critical infrastructure operations, and improved security of computer systems.

Sec. 11. Authorization of appropriations

Authorizes appropriations for sections 8 and 10 of the bill. For the research programs in section 8, provides $25 million for FY 2003, $40 million for FY 2004, $55 million for FY 2005, $70 million for FY 2006, $85 million for FY 2007, and such sums as may be necessary for fiscal years 2008 through 2012. Authorizes appropriations for section 10 at $6 million for FY 2003, $6.2 million for FY 2004, $6.4 million for FY 2005, $6.6 million for FY 2006, and $6.8 million for FY 2007.

Sec. 12. National Academy of Sciences study on computer and network security in critical infrastructures

Authorizes the Director of NIST to enter into an agreement with the National Research Council (NRC) of the National Academy of Sciences to conduct a study of the vulnerabilities of the Nation's critical infrastructure networks and make recommendations for appropriate improvements. The study requires the NRC to review existing data to identify gaps in the security of critical infrastructure networks, make recommendations for research priorities to address these gaps, and review the security of network-related infrastructure including industrial process controls. A report of the study results is to be submitted to Congress. Authorizes $700,000 for the purpose of carrying out the study.

SUMMARY OF H.R. 3394—THE CYBER SECURITY RESEARCH AND DEVELOPMENT ACT—INTRODUCED BY MR. BOEHLERT, MR. HALL (TX), MR. SMITH (TX), MR. BAIRD, MR. SMITH (MI) AND MS. EDDIE BERNICE JOHNSON (TX)

The Committee on Science held two full committee hearings devoted to research and development needs related to cyber security. These hearings offered a sobering view of the security of our nation's critical infrastructures and highlighted the lack of world-class research being conducted to address these cyber security needs. Four challenges emerged from these hearings that demand an immediate and sustained response:

- Too little cyber security research is being conducted and the research that is funded is incremental and unlikely to lead to the development of breakthrough approaches to cyber security.
- There is inadequate coordination between government, academia, and industry and no Federal agency has stepped forward to take the lead in supporting cyber security research.
- Too few researchers are prepared to meet our current and projected cyber security research needs.
- Too few undergraduate and graduate students are pursuing studies in cyber security related fields.

The Cyber Security Research and Development Act responds to these challenges. It creates important new research programs at the National Science Foundation (NSF) and the National Institute of Standards and Technology (NIST). Building upon NSF's proven capacity to mobilize the academic research community, the Act authorizes NSF to create new academic centers and fellowships to stimulate innovative thinking about cyber security. Building upon NIST's proven ability to work with industry, the Act authorizes NIST to initiate a new research grant program that strengthens the interaction between government, academia, and industry.

Funding for NSF is provided for competitive, peer-reviewed grant programs, including:

- $233 million over five years for a program providing grants to researchers for the pursuit of particularly innovative computer and network security basic research.
- $144 million over five years to fund multi-year grants to colleges and universities to establish multidisciplinary Centers for Computer and Network Security Research, alone or in partnership with other universities or with businesses and government laboratories.
- $95 million over five years for the award of grants to colleges and universities to improve undergraduate and master's degree programs including through the creation of internship programs and new courses.
- $6 million over five years to make grants to community colleges in order to enhance their ability to contribute to the supply of computer and network security technicians.
- $90 million over five years to establish a competitive grant program that will enable colleges and universities to offer fellowships, research opportunities in industry, and other educational opportunities to students pursuing doctoral degrees in computer and network security.

The Act authorizes NIST to use an administrative model that has been successfully implemented at the Defense Advanced Research Projects Agency. The Act authorizes NIST to invest talented project managers with broad latitude to establish cyber security research objectives and to solicit and award proposals. This structure shortens the approval time for research proposals and allows the project manager to move quickly to in vest in promising new ideas.

The funding for NIST includes:

- $275 million over five years for a grant program to support high-risk, cutting-edge research by academic researchers who are working with industry.
- Establishes research fellowships to increase the number of researchers engaged in computer and network security research.
- $32 million over five years for an in-house research program in computer and network security.

Finally, the bill requires a National Academy of Sciences study and report to Congress on the nation's critical infrastructure vulnerabilities.

CYBER SECURITY RESEARCH AND DEVELOPMENT ACT YEARLY AUTHORIZATION OF APPROPRIATIONS

[In millions of dollars]

Program	FY2003	FY2004	FY2005	FY2006	FY2007	Total
Section 4 National Science Foundation Research:						
Computer and Network Security Research Grants ..	35	40	46	52	60	233
Computer and Network Security Research Centers	12	24	36	36	36	144
Section 5 National Science Foundation Computer and Network Security Programs:						
Computer and Network Security Capacity Building Grants	15	20	20	20	20	95
Scientific and Advanced Technology Act of 1992 ..	1	1.25	1.25	1.25	1.25	6
Graduate Traineeships in Computer and Network Security Research	10	20	20	20	20	90
Section 6. Fostering Research and Education in Computer and Network Security.						
Section 7. National Institute of Standards and Technology Research Program	25	40	55	70	85	275
Section 8. Computer Security Review, Public Meetings, and Information	1.03	1.06	.....	.....	.....	2.09
Section 9. Intramural Security Research	6	6.2	6.4	6.6	6.8	32
Section 11. National Academy of Sciences Study on Computer and Network Security in Critical Infrastructures	0.7	.....	.....	.....	.....	0.7
Total	105.73	152.51	184.65	205.85	229.05	877.79

Five Year Total: $877.79 million.

○