AUTHENTICATED
U.S. GOVERNMENT
INFORMATION
GPO

Calendar No. 549

107TH CONGRESS *2d Session*	SENATE	REPORT 107–239

CYBER SECURITY RESEARCH AND DEVELOPMENT ACT

R E P O R T

OF THE

COMMITTEE ON COMMERCE, SCIENCE, AND TRANSPORTATION

ON

S. 2182

AUGUST 1, 2002.—Ordered to be printed

U.S. GOVERNMENT PRINTING OFFICE

99–010 WASHINGTON : 2002

SENATE COMMITTEE ON COMMERCE, SCIENCE, AND TRANSPORTATION

ONE HUNDRED SEVENTH CONGRESS

SECOND SESSION

ERNEST F. HOLLINGS, South Carolina, *Chairman*

DANIEL K. INOUYE, Hawaii
JOHN D. ROCKEFELLER IV, West Virginia
JOHN F. KERRY, Massachusetts
JOHN B. BREAUX, Louisiana
BYRON L. DORGAN, North Dakota
RON WYDEN, Oregon
MAX CLELAND, Georgia
BARBARA BOXER, California
JOHN EDWARDS, North Carolina
JEAN CARNAHAN, Missouri
BILL NELSON, Florida

JOHN MCCAIN, Arizona
TED STEVENS, Alaska
CONRAD BURNS, Montana
TRENT LOTT, Mississippi
KAY BAILEY HUTCHISON, Texas
OLYMPIA J. SNOWE, Maine
SAM BROWNBACK, Kansas
GORDON SMITH, Oregon
PETER G. FITZGERALD, Illinois
JOHN ENSIGN, Nevada
GEORGE ALLEN, Virginia

KEVIN D. KAYES, *Staff Director*
MOSES BOYD, *Chief Counsel*
GREGG ELIAS, *General Counsel*
JEANNE BUMPUS, *Republican Staff Director and General Counsel*
ANN BEGEMAN, *Republican Deputy Staff Director*

Calendar No. 549

107TH CONGRESS 2d Session | SENATE | REPORT 107–239

CYBER SECURITY RESEARCH AND DEVELOPMENT ACT

AUGUST 1, 2002.—Ordered to be printed

Mr. HOLLINGS, from the Committee on Commerce, Science, and Transportation, submitted the following

R E P O R T

[To accompany S. 2182]

The Committee on Commerce, Science, and Transportation, to which was referred the bill (S. 2182) to authorize funding for computer and network security research and development and research fellowship programs, and for other purposes, having considered the same, reports favorably thereon with an amendment in the nature of a substitute and recommends that the bill, as amended, do pass.

PURPOSE OF THE BILL

The purpose of the bill, as reported, is to establish and authorize funding for programs at the National Science Foundation (NSF) and the National Institute of Standards and Technology (NIST) and to better coordinate information technology security research among government, industry and academia.

BACKGROUND AND NEEDS

With the advent of high-speed access to the Internet, computer networks are growing in size and complexity, creating new opportunities for those who would mount malicious computer attacks. At the same time, computer hacking is no longer the sole realm of computer geniuses. Instructions (known as scripts) for exploiting vulnerabilities of computer systems are widely available to anyone with access to the Internet. In some cases, all that is needed to launch an attack is a website address. Moreover, while some vulnerabilities are well known, the companies and individuals who own computers connected to the Internet do not always fix (or

"patch") obvious security holes, even when the "patch" is free and easy to install.

Computer attacks not only threaten the integrity of systems and data connected to the Internet, but also have the effect of undermining public trust in Internet-based electronic commerce, potentially hindering its further development and adoption. If Internet usage is to continue its growth, businesses and consumers must have confidence in the security of their information and the identity of the person or company with whom they are engaging in commerce or conversation. The threat of malicious hacking—and media coverage of high profile computer attacks—has the potential to disturb that trust and the future growth of the Internet and electronic commerce.

It is not just our economic security that is vulnerable to cyber attack. Critical infrastructures, which are increasingly reliant on the Internet for exchange of data and control functions, also are highly susceptible. For example, the systems that control floodgates for dams or distribution of power are accessible via the Internet. Additionally, the potential threat from terrorist hackers (cyber terrorists) to the Federal government's strategic military systems is real. Security experts note that Department of Defense systems face daily attacks, many of which originate on foreign-based computers.

Despite these enormous challenges, however, the United States has failed to conduct an adequate program of world-class, basic research needed to address cyber security needs. While a number of information technology companies support research and development (R&D) on network security, inadequacies in our security arsenal cannot be addressed solely through short-term industry-based applied research. Industry relies heavily on the fundamental research supported by the Federal government and the training of future researchers, including computer scientists, mathematicians, and many others, that Federally funded research programs support.

Unfortunately, with the possible exception of encryption-related research, cyber security research is under-funded, and basic research into the fundamental technological cyber security challenges is not sufficient to support the Nation's needs. Many experts believe that because of these historic funding patterns, there is a severe shortage of researchers in the country with the experience and expertise needed to conduct cutting-edge research in cyber security. For example, experts estimate that there are currently only a total of 45 to 75 cyber security researchers nationwide, compared to 60 or more faculty members per computer science department at typical United States research universities.

This shortage of personnel is not merely a problem for the academic and research community. Federal agencies are finding it increasingly difficult to recruit and hire professional staff with the knowledge and experience needed to analyze risks and manage and secure their own computer networks.

S. 2182 would substantially increase the government's commitment to cyber security research and development by creating a broad program of cyber security R&D at NSF and NIST. The program would support R&D, student scholarships, improved faculty development, and upgrades of networks and facilities. A broad range of institutions would be able to participate, including institu-

tions of higher education (as well as, consortia thereof and community colleges), non-profits, governmental laboratories, and private industry.

LEGISLATIVE HISTORY

On July 16, 2001, and April 24, 2002, the Subcommittee on Science, Technology, and Space conducted hearings on cyber security. At the July 16, 2001, hearing entitled "Holes in the Net: Security Risk and the E-Consumer," witnesses included: Dr. Vinton G. Cerf, Senior Vice President, Internet Architecture and Technology, WorldCom; Mr. Harris N. Miller, President, Information Technology Association of America; and Mr. Bruce Schneier, Chief Technical Officer, Counterpane Internet Security, Inc. At the April 24, 2002, hearing, entitled "Homeland Security and the Technology Sector,"which focused on both S. 2182 and S. 2037, witnesses included: The Honorable Sherwood Boehlert, Chairman of the House Science Committee; Dr. George Strawn, Acting Assistant Director for Computer Information Science and Engineering at the National Science Foundation; Dr. Lance Hoffman, Department of Computer Science, George Washington University; Mr. W. Wyatt Starnes, President and Chief Executive Officer, Tripwire, Inc.; and Mr. Ronil Hira, Chairman of the Research and Development Policy Committee of the Institute of Electrical and Electronics Engineers.

On April 17, 2002, Senator Wyden, Chairman of the Subcommittee on Science, Technology, and Space, introduced S. 2182, the Cyber Security Research and Development Act.

On May 17, 2002, the Committee met in open executive session and, by a voice vote, ordered S. 2182 to be reported with a substitute amendment offered by Senator Wyden and Senator Edwards. The substitute included provisions from Senator Edwards's cyber security bills, S. 1900 and S. 1901, dealing with: (1) the establishment of an NSF program of forgivable loans to doctoral students in cyber security who agree to teach for 5 years; and (2) the development of information security benchmarks by NIST which will be implemented by Federal agencies. In addition, the substitute included provisions to enhance ethnic and racial diversity as a goal in NSF's new cyber security programs. The substitute also contained provisions to raise the profile of NIST's Computer Security Division to allow for cost sharing of new NIST grants, and to allow for a discretionary Director's Fund to permit NIST to fund promising projects in a more expeditious manner.

On February 7, 2002, the House of Representatives passed the companion measure to S. 2182, H.R. 3394, which was subsequently received in the Senate and referred to the Committee.

SUMMARY OF MAJOR PROVISIONS

AUTHORIZATION OF APPROPRIATIONS

S. 2182, as reported, would authorize appropriations to NSF and NIST for cyber security R&D. A total of $126.56 million would be authorized to be appropriated in fiscal year (FY) 2003, increasing to $249.05 million by FY 2007, for a 5-year total of $978.65 million.

NSF PROGRAMS

At the NSF, S. 2182, as reported, would establish and authorize: (1) merit-based grants in cyber security that would support innovative approaches from individual researchers to enhance cyber security; (2) Centers for Computer and Network Security Research, which would generate innovative approaches to computer security by conducting cutting-edge, multi-disciplinary research; (3) capacity building grants to institutions to improve their undergraduate or master's cyber security programs; (4) grants to improve cyber security education at community colleges as part of NSF's existing program pursuant to the Scientific and Advanced Technology Act of 1992, (46 U.S.C. 1862i); (5) graduate traineeships in computer and network security, which are merit-based grants to institutions to award fellowships to students pursuing cyber security doctoral degrees; (6) the inclusion of cyber security as an approved field of specialization supported by the Graduate Research Fellowships Program established under section 10 of NSF's Organic Act (42 U.S.C. 1869); and (7) a cyber security faculty development program to award merit-based grants to institutions that would award fellowships, in the form of loans, to students pursuing cyber security doctoral degrees, where 20 percent of the loan would be forgiven for each year the fellow remains a full time faculty professor in the cyber security field upon graduation.

NIST PROGRAMS

At NIST, S. 2182, as reported, would establish and authorize: (1) grants to colleges and universities that partner with for-profit entities to support long-term cyber security research; (2) research fellowships for post-doctoral students in cyber security, information technology, or related fields wishing to transfer into the cyber security field; (3) development of benchmark cyber security standards for Federal agencies; and (4) establishment of an Office for Information Security Programs, headed by a Director who reports directly to the NIST Director.

ESTIMATED COSTS

In accordance with paragraph 11(a) of rule XXVI of the Standing Rules of the Senate and section 403 of the Congressional Budget Act of 1974, the Committee provides the following cost estimate, prepared by the Congressional Budget Office:

U.S. CONGRESS,
CONGRESSIONAL BUDGET OFFICE,
Washington, DC, May 28, 2002.

Hon. ERNEST F. HOLLINGS,
Chairman, Committee on Commerce, Science, and Transportation, U.S. Senate, Washington, DC.

DEAR MR. CHAIRMAN: The Congressional Budget Office has prepared the enclosed cost estimate for S.2182, 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 contracts are Kathleen Gramp and Ken Johnson.

Sincerely,

BARRY B. ANDERSON
(For Dan L. Crippen, Director).

Enclosure.

CONGRESSIONAL BUDGET OFFICE COST ESTIMATE

S. 2182—Cyber Security Research and Development Act

Summary: S. 2182 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, and loans for certain doctoral fellowship related to computer security, and would authorize NIST to conduct similar research at its laboratories. It would authorize the appropriation of $978 million over the 2002–2007 period for these activities. 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 nation's computer network infrastructure.

Assuming appropriation of the specified amounts, CBO estimates that implementing this bill would cost $671 million over the 2002–2007 period. the bill would not affect direct spending or receipts; therefore, pay-as-you-go procedures would not apply.

S. 2182 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 S. 2182 is shown in the following table. The costs of this legislation fall within budget functions 250 (general science, space, and technology) and 370 (commerce and housing credit).

	By fiscal year, in million of dollars—					
	2002	2003	2004	2005	2006	2007
CHANGES IN SPENDING SUBJECT TO APPROPRIATION						
National Science Foundation: [1]						
Authorization Level	0	78	110	128	134	142
Estimated Outlays	0	15	58	93	114	125
National Institute of Standards and Technology: [2]						
Authorization Level	2	47	62	76	92	107
Estimated Outlays	0	23	37	53	69	84
Total Changes:						
Authorization Level	2	125	172	204	226	249
Estimated Outlays	0	38	95	146	183	209

[1] NSF has a total appropriation of $4.9 billion in 2002.
[2] Thus far, NIST has a total appropriation of $680 million in 2002.

Basis of estimate: S. 2182 would authorize the appropriation of $592 million for NSF and $386 million for NIST over the 2002–2007 period for these agencies to carry out a variety of grant, fellowship, loan, and other programs related to research on computer security. Based on the spending patterns of similar NSF and NIST programs, CBO estimates that implementing the bill would cost

NSF and about $405 million and NIST about $266 million over the 2002–2007 period, assuming the appropriation of the authorized amounts. For this estimate, CBO assumes that funds will be appropriated near the beginning of each fiscal year, with the exception of the $2 million authorization for NIST in 2002 (which we assume will be provided this summer).

CBO expects that the doctoral fellowships authorized by this bill would be treated as direct loans and would be subject to credit reform procedures. S. 2182 would require that such fellowships be repaid but would forgive specified amounts if the recipient is employed as a full-time faculty member. For this estimate, CBO assumes that NSF would use the $5 million authorized annually for these fellowships to cover the subsidy cost of such loans.

Pay-as-you-go considerations: None.

Estimated impact on state, local, and tribal governments: S. 2182 contains no intergovernmental mandates as defined in UMRA and would impose no costs on state, local, or tribal governments. The bill would benefit public universities by authorizing the appropriation of $978 million, much of which would be for grant programs to institutions of higher education, including public universities, for a number of projects aimed at improving computer and network security. Any costs incurred by public universities would be voluntary.

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

Previous CBO estimate: On December 17, 2001, CBO transmitted a cost estimate for H.R. 3394, the Cyber Security Research and Development Act, as ordered reported by the House Committee on Science on December 6, 2001. H.R. 3394 is very similar to S. 2182, although H.R. 3394 would authorize the appropriation of $878 million over the 2002–2007 period. CBO estimated that implementing H.R. 3394 would cost $420 million during the 2002–2006 period, assuming the appropriation of the necessary amounts.

Estimate prepared by: Federal costs: Kathleen Gramp (NSF) and Ken Johnson (NIST); impact on state, local, and tribal governments: Elyse Goldman; impact on the private sector: Cecil McPherson.

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

REGULATORY IMPACT STATEMENT

In accordance with paragraph 11(b) of rule XXVI of the Standing Rules of the Senate, the Committee provides the following evaluation of the regulatory impact of the legislation, as reported:

NUMBER OF PERSONS COVERED

The Committee believes that the bill would not subject any individuals or businesses affected by the legislation to any additional regulation. Neither NSF nor NIST are regulatory agencies; therefore they have no regulatory authority. Section 8(c) of the bill would require NIST to adopt Federal agency benchmark security standards to be implemented by Federal civilian agencies. The standards would not directly impose any requirements on individuals or businesses to further regulation.

ECONOMIC IMPACT

This legislation would not have an adverse economic impact on the Nation. It would authorize significant funding for research and development in computer and information security, promoting sustained economic growth through better protection of our critical infrastructures that have become increasingly dependent on electronic networks. In addition, this legislation would significantly enhance the growth and development of the computer and information security field in this country.

PRIVACY

S. 2182 would not have a negative impact on the personal privacy of individuals. The purpose of this legislation is to support research and development in information security, which should lead to increased protection for personal data stored on computer networks.

PAPERWORK

This legislation would not increase paperwork requirements for private individuals or businesses. It would require four Federal reports: (1) within 180 days of enactment, the Director of NIST must submit a report to the Senate Committee on Commerce, Science, and Transportation, the House Committee on Science, and the House and Senate Appropriations Committees identifying specific Federal agency benchmark security standards that should be developed over the following 12 month period, and recommending, in consultation with the Office of Management and Budget any additional funding that may be necessary; (2) not later than 1 year after the date of the report referred to above, the Director of NIST, in consultation with appropriate public and private entities, must submit a follow-up report containing recommendations for specific, reasonable Federal agency benchmark security standards to the Secretary of Commerce and the Chairman of the Federal Chief Information Officers (CIOs) Council. The Director of NIST shall review the recommended standards not less than once every 6 months and update such standards or issue new standards as necessary. The Director is not prohibited from updating any portion of such recommended standards more frequently if circumstances so require. The Secretary of Commerce shall widely disseminate the report, along with any updates; (3) not later than 36 months after the date of enactment, the Chairman of the Federal CIOs Council must submit a report to Congress describing the status of, costs associated with, and barriers to implementation of the Federal agency benchmark security standards at each agency/department of the government; and (4) within 3 months after the date of enactment, NIST must arrange for the National Academy of Sciences to conduct a study to examine the impact of requiring Federal agencies to implement benchmark security standards on national cyber security preparedness. NIST would be directed to transmit the report containing the results of the study to Congress not later than 21 months after the date of enactment of this Act.

S. 2182, as reported, would also require the Chairman of the Federal CIOs Council to provide to the NIST Director a classified

list of current Federal government security standards not later than 90 days after the date of enactment.

SECTION-BY-SECTION ANALYSIS

Section 1. Short title

Section 1 would give the short title of the bill, the "Cyber Security Research and Development Act."

Section 2. Findings

Section 2 presents the findings concerning: the interdependent nature of critical infrastructures brought about by advancements in computing and communications technology; the increased consequences of failure of communications and computer systems stemming from exponential increases in interconnectivity; the Nation's lack of preparedness for a coordinated cyber and physical attack; the shortage of outstanding researchers in the field of cyber security; the lack of coordination among government, academia, and industry for computer security; the need to significantly increase the Federal investment in computer and network security research and development; and the level of minority participation in the United States computer and information science workforce.

Section 3. Definitions

Section 3 includes the following definitions: (1) the term "Director" means the Director of the National Science Foundation (NSF), except in section 8 where it refers to the Director of the National Institute for Standards and Technology (NIST); (2) the term "institution of higher education" is given the meaning found in the Higher Education Act of 1965; and (3) "Federal agency benchmark security standards" means a baseline minimum security configuration for specific computer hardware or software components, an operational procedure or practice, or organizational structure that increases the security of the information technology assets of an agency or department of the Federal government.

Section 4. National Science Foundation research

Section 4(a) would establish an NSF program to award merit-reviewed, competitively based grants for basic research on innovative approaches to enhance computer security. Research areas include authentication and cryptography; computer forensics and intrusion detection; reliability of computer and network applications, middleware, operating systems, and communications infrastructure; privacy and confidentiality; network security architecture, including tools for security administration and analysis such as firewall technology; emerging threats, including malicious such as viruses and worms; vulnerability assessments; operations and control systems management; management of interoperable digital certificates or digital watermarking; and remote access and wireless security. This subsection would also authorize appropriations of $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.

Section 4(b) would establish an NSF program to award multiyear grants to institutions of higher education (or consortia thereof) to establish multidisciplinary Centers for Computer and Network

Security Research. Institutions (or consortia) receiving grants may partner with one or more government laboratories or for-profit institutions. Applications for these grants would be reviewed on the basis of the ability of the institution (or consortium) to generate innovative approaches to computer and network security research; the applicant's experience in conducting research on computer and network security and capacity to foster new multi-discipline collaborations; 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. This subsection would require the Director to convene an annual meeting of Centers to foster greater collaboration and communication. Appropriations of $12 million for FY 2003, $24 million for FY 2004, $36 million for FY 2005, $36 million for FY 2006, and $36 million for FY 2007 would be authorized.

Section 5. National Science Foundation Computer and Network Security programs

Section 5(a) (capacity building) would establish 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 would be used for purposes including curriculum development, equipment acquisition, faculty enhancement, and the establishment of a student internship program in government or industry. Applicants must describe the plan for building increased capacity in computer and network security, must articulate the roles and responsibilities of each partnering institution or collaborative group, and must provide evidence of high potential for success in educating and placing students in relevant jobs or graduate programs. The Director would be required to evaluate the impact of the program on increasing the quality and quantity of computer and network security professionals not later than 5 years after establishment. The program would authorize $15 million for FY 2003 and $20 million for each of fiscal years 2004–2007.

Section 5(b) would expand NSF's existing program for community colleges (established by the Scientific and Advanced Technology Act of 1992, P.L. 102–476) to include grants to improve education in fields related to computer and network security. It would authorize $1 million for FY 2003 and $1.25 million for each of fiscal years 2004–2007.

Section 5(c) (Graduate Traineeships in Computer and Network Security Research) would establish a competitive, merit-based NSF program to award grants to institutions of higher education to establish traineeship programs for graduate students pursuing studies in computer and network security research leading to a doctorate degree. Grant funds would 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. Appropriations of $10 million for FY 2003, and $20 million for each of fiscal years 2004–2007 would be authorized.

Section 5(d) would direct NSF to include computer and network security as an approved field of specialization under its current Graduate Research Fellowships program.

Section 5(e) (Cyber Security Faculty Development Fellowship Program) would establish an NSF program to award grants to institutions of higher learning to establish traineeship programs to enable graduate students to pursue academic careers in cyber security upon completion of doctoral degrees. Funds received by an institution would be made available to fellows, in the form of loans, for up to 5 years on a merit-reviewed, competitive basis to cover tuition and fees for doctoral study and a $25,000 per year stipend. Loans would be forgiven at 20% for each year the fellow is employed as a full-time faculty member at an institution, thereby forgiving the loan in total if the fellow teaches for 5 years. Appropriations of $5 million per year for fiscal years 2003–2007 would be authorized.

Section 6. Consultation

Section 6 would require the NSF Director to consult with other Federal agencies in carrying out the programs described in Sections 4 and 5.

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

Section 7 of the bill would amend 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.

Section 8. National Institute of Standards and Technology research program

Section 8(a) would amend the National Institute of Standards and Technology Act by creating a new section 22 to establish a program that provides assistance to institutions of higher education that partner with for-profit entities to support multidisciplinary, long-term research to improve the security of computer systems. Partnerships may also include government laboratories.

The new section 22(b) would authorize the NIST Director to award research fellowships to post-doctoral researchers engaged in computer security research and to senior researchers who wish to transition from other research fields to computer security research. The new section 22(c) would authorize the Director to award grants or cooperative agreements and would set forth applicant eligibility requirements.

The new section 22(d) would require cost-sharing (up to 50%) by the for-profit entities pursuant to a sliding scale, with the least amount required for projects that will be broadly applicable and widely shared. The new section 22(e) would instruct 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. The new section 22(f) would give the NIST Director the responsibility of reviewing, periodically, the portfolio of research awards in consultation with NIST's existing Computer System Security and Privacy Advisory Board. The Director would also be instructed to contract with the National Research Council to conduct a formal review of the program during its fifth

year and to submit a report of this review to Congress no later than 6 years after the initiation of the program.

Section 8(b) would amend the definition of Computer System by amending Section 20(d)(1)(B)(i) of the NIST Act to read "computers and computer networks."

Section 8(c)(1) would require the Director of NIST to submit a report to the Senate Committee on Commerce, Science, and Transportation; the House Committee on Science; and the House and Senate Appropriations Committees, not later than 180 days after enactment of this Act, identifying specific Federal agency benchmark security standards that should be developed by NIST over the following 12 month period, and recommending (in consultation with the Office of Management and Budget (OMB)) any additional funding authorization that may be necessary.

Section 8(c)(2) would require NIST to submit a follow-up report selecting and adopting Federal agency benchmark security standards. The Director of NIST, in consultation with appropriate public and private entities, must submit the report to the Secretary of Commerce and the Chairman of the Federal CIOs Council not later than 1 year after the date of the report issued in section 8(c)(1). The Director shall review these standards not less than once every 6 months, and update such standards or issue new standards as necessary. Nothing in this title shall prohibit the Director from updating any portion of such recommended standards more frequently if it is determined that circumstances so require. The Secretary of Commerce would widely disseminate the report and any updates. Section 8(c)(3) would require civilian departments and agencies to implement the standards recommended by the report not later than 90 days after the date of the report. The Committee understands civilian agencies to be those agencies not excluded under section 20 of the NIST Organic Act. Updates must be similarly implemented not later than 30 days. To facilitate NIST's duties under this section, not later than 90 days after the enactment of this Act, the Chairman of the Federal CIOs Council shall provide to the NIST Director a classified list of the current Federal government security standards. Appropriations are authorized for activities under this subsection of $15 million per year for fiscal years 2003–2007.

Section 8(d) would require two reports to Congress. Within 36 months after the date of enactment, the Chairman of the Federal CIOs Council is directed to submit a report to Congress describing the status of, costs associated with, and barriers to implementation and recommendations for over-coming such barriers of the Federal agency benchmark security standards at each department and agency of the Federal government. Not later than 3 months after the date of enactment, NIST would arrange for the National Academy of Sciences to conduct a study analyzing the effect of implementation of Federal agency benchmark security standards on the state of national cyber security preparedness. Appropriations of $800,000 would be authorized for this report.

Section 8(e) would amend the National Institute of Standards and Technology Act to establish an Office for Information Security Programs. The Computer Security Division already exists at NIST; this subsection renames that office and elevates Information Secu-

rity Programs to be on par with NIST's other laboratories with a Director reporting to the Director of NIST.

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

This section would authorize 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.

Section 10. Intramural security research

Section 10 would amend 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 multidisciplinary, high-risk, long-term research on ways to improve security of computer systems.

Section 11. Authorization of appropriations

This section would authorize appropriations for sections 8 and 10 of the bill. For the research programs in section 8, it would authorize $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. For section 10, it would authorize $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.

Section 12. National Academy of Sciences Study on Computer and Network Security in Critical Infrastructures

Section 12 would authorize 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 not later than 3 months after the date of enactment of the Act. The study would require 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. For the purpose of carrying out the study, $700,000 is authorized.

Section 13

This section would give the Office of Science and Technology Policy (OSTP) the responsibility to coordinate Federal cyber security R&D, and ensure consultation with the Office of Homeland Security, the President's Critical Infrastructure Protection Board, and other relevant agencies. This section also would encourage OSTP to

promote cooperation between the Federal government, academia, and private industry.

CHANGES IN EXISTING LAW

In compliance with paragraph 12 of rule XXVI of the Standing Rules of the Senate, 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 material is printed in italic, existing law in which no change is proposed is shown in roman):

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY ACT

COMPUTERS STANDARDS PROGRAM.

[15 U.S.C. 278g–3]

SEC. 20. (a) DEVELOPMENT OF STANDARDS, GUIDELINES, METHODS, AND TECHNIQUES FOR COMPUTER SYSTEMS.—The Institute shall—

(1) have the mission of developing standards, guidelines, and associated methods and techniques for computer systems;

(2) except as described in paragraph (3) of this subsection (relating to security standards), develop uniform standards and guidelines for Federal computer systems, except those systems excluded by section 2315 of title 10, United States Code, or section 3502(9) of title 44, United States Code;

(3) have responsibility within the Federal Government for developing technical, management, physical, and administrative standards and guidelines for the cost-effective security and privacy of sensitive information in Federal computer systems except—

(A) those systems excluded by section 2315 of title 10, United States Code, or section 3502(9) of title 44, United States Code; and

(B) those systems which are protected at all times by procedures established for information which has been specifically authorized under criteria established by an Executive order or an Act of Congress to be kept secret in the interest of national defense or foreign policy, the primary purpose of which standards and guidelines shall be to control loss and unauthorized modification or disclosure of sensitive information in such systems and to prevent computer-related fraud and misuse;

(4) submit standards and guidelines developed pursuant to paragraphs (2) and (3) of this subsection, along with recommendations as to the extent to which these should be made compulsory and binding, to the Secretary of Commerce for promulgation under section 5131 of the Clinger-Cohen Act of 1996;

(5) develop guidelines for use by operators of Federal computer systems that contain sensitive information in training their employees in security awareness and accepted security practice, as required by section 5 of the Computer Security Act of 1987; and

(6) develop validation procedures for, and evaluate the effectiveness of, standards and guidelines developed pursuant to

paragraphs (1), (2), and (3) of this subsection through research and liaison with other government and private agencies.

(b) TECHNICAL ASSISTANCE AND IMPLEMENTATION OF STANDARDS DEVELOPED.—In fulfilling subsection (a) of this section, the Institute is authorized—

(1) to assist the private sector, upon request, in using and applying the results of the programs and activities under this section;

(2) as requested, to provide to operators of Federal computer systems technical assistance in implementing the standards and guidelines promulgated pursuant to section 5131 of the Clinger-Cohen Act of 1996;

(3) to assist, as appropriate, the Office of Personnel Management in developing regulations pertaining to training, as required by section 5 of the Computer Security Act of 1987;

(4) to perform research and to conduct studies, as needed, to determine the nature and extent of the vulnerabilities of, and to devise techniques for the cost-effective security and privacy of sensitive information in Federal computer systems; and

(5) to coordinate closely with other agencies and offices (including, but not limited to, the Departments of Defense and Energy, the National Security Agency, the General Accounting Office, the Office of Technology Assessment, and the Office of Management and Budget)—

(A) to assure maximum use of all existing and planned programs, materials, studies, and reports relating to computer systems security and privacy, in order to avoid unnecessary and costly duplication of effort; and

(B) to assure, to the maximum extent feasible, that standards developed pursuant to subsection (a)(3) and (5) are consistent and compatible with standards and procedures developed for the protection of information in Federal computer systems which is authorized under criteria established by Executive order or an Act of Congress to be kept secret in the interest of national defense or foreign policy.

(c) PROTECTION OF SENSITIVE INFORMATION.—For the purposes of—

(1) developing standards and guidelines for the protection of sensitive information in Federal computer systems under subsections (a)(1) and (a)(3), and

(2) performing research and conducting studies under subsection (b)(5), the Institute shall draw upon computer system technical security guidelines developed by the National Security Agency to the extent that the National Bureau of Standards determines that such guidelines are consistent with the requirements for protecting sensitive information in Federal computer systems.

(d) ESTABLISHMENT OF AN OFFICE FOR INFORMATION SECURITY PROGRAMS.—

(1) IN GENERAL.—There is established in the Institute an Office for Information Security Programs.

(2) HEAD.—The Office for Information Security Programs shall be headed by a Director, who shall be a senior executive and shall be compensated at a level in the Senior Exec-

utive Service under section 5382 of title 5, United States Code, as determined by the Secretary of Commerce.

(3) FUNCTION.—The Director of the Institute shall delegate to the Director of the Office of Information Security Programs the authority to administer all functions under this section, except that any such delegation shall not relieve the Director of the Institute of responsibility for the administration of such functions. The Director of the Office of Information Security Programs shall serve as principal adviser to the Director of the Institute on all functions under this section.

[(d)] *(e)* DEFINITIONS.—As used in this section—

(1) the term "computer system"—

(A) means any equipment or interconnected system or subsystems of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception, of data or information; and

(B) includes—

[(i) computers;] *(i) computers and computer networks;*

(ii) ancillary equipment;

(iii) software, firmware, and similar procedures;

(iv) services, including support services; and

(v) related resources;

(2) the term "Federal computer system" means a computer system operated by a Federal agency or by a contractor of a Federal agency or other organization that processes information (using a computer system) on behalf of the Federal Government to accomplish a Federal function;

(3) the term "operator of a Federal computer system" means a Federal agency, contractor of a Federal agency, or other organization that processes information using a computer system on behalf of the Federal Government to accomplish a Federal function;

(4) the term "sensitive information" means any information, the loss, misuse, or unauthorized access to or modification of which could adversely affect the national interest or the conduct of Federal programs, or the privacy to which individuals are entitled under section 552a of title 5, United States Code (the Privacy Act), but which has not been specifically authorized under criteria established by an Executive order or an Act of Congress to be kept secret in the interest of national defense or foreign policy; and

(5) the term "Federal agency" has the meaning given such term by section 3(b) of the Federal Property and Administrative Services Act of 1949 .

(f) INTRAMURAL SECURITY RESEARCH.—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 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.

(g) AUTHORIZATION OF APPROPRIATIONS.—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, through the Director of the Office for Information Security Programs, 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 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) IN GENERAL.—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) SENIOR RESEARCH FELLOWSHIPS.—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) ELIGIBILITY.—

(A) IN GENERAL.—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) STIPENDS.—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.—

(1) IN GENERAL.—The Director is authorized to award grants or cooperative agreements to institutions of higher education to carry out the program established under subsection (a).

(2) ELIGIBILITY.—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—

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

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

(C) 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

(D) 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) SLIDING SCALE COST-SHARING.—In awarding a grant under this section, the Director shall require up to 50 percent of the costs of the project funded by the grant to be met by the for-profit entity or entities in the partnership. The Director shall base the percentage of cost-sharing required under this paragraph on a sliding scale reflecting the degree to which the results of the research undertaken by a partnership may reasonably be expected to be applied and shared, with—

(1) the smallest percentage of cost-sharing required for projects the anticipated results of which are reasonably expected to be of broadest potential application and broadly shared; and

(2) the greatest percentage of cost-sharing required for projects the anticipated results of which are reasonably expected—

(A) to be of narrow or proprietary application; or

(B) not to be broadly shared.

(e) PROGRAM OPERATION.—

(1) MANAGEMENT.—The program established under subsection (a) shall be headed by the Director of the Office for Information Security Programs and 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, on a competitive basis, as program managers.

(2) MANAGERS MAY BE EMPLOYEES.—Program managers designated under paragraph (1) may be new or existing employees of the Institute.

(3) MANAGER RESPONSIBILITY.—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.

(4) From amounts available for awards under subsection (c), the Director, in consultation with the Director of the Office for Information Security Programs established in section 20 of this Act, may assign up to 5 percent to a Directors Fund which may be awarded throughout the fiscal year at the discretion of the Director to promising projects designed to fulfill the goals Stated in subsection (a). Such projects should be innovative in nature and should meet emerging needs in computer security.

(f) REVIEW OF PROGRAM.—

(1) PERIODIC REVIEW.—The Director shall periodically review the portfolio of research awards monitored by each program manager designated in accordance with subsection (e). 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 (e).

(2) COMPREHENSIVE 5-YEAR REVIEW.—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 (e)(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 6 years after the initiation of the program.

(g) DEFINITIONS.—In this section:

(1) COMPUTER SYSTEM.—The term "computer system" has the meaning given that term in section 20(d)(1).

(2) INSTITUTION OF HIGHER EDUCATION.—The term "institution of higher education" has the meaning given that term in section 101 of the Higher Education Act of 1965 (20 United States Code 1001).

APPROPRIATIONS; AVAILABILITY

[15 U.S.C. 278h]

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.

* * * * * * *

NATIONAL SCIENCE FOUNDATION ACT OF 1950

SEC. 3. FUNCTIONS.

[42 U.S.C. 1862]

(a) INITIATION AND SUPPORT OF STUDIES AND PROGRAMS; SCHOLARSHIPS; CURRENT REGISTER OF SCIENTIFIC AND TECHNICAL PERSONNEL.—The Foundation is authorized and directed—

(1) to initiate and support basic scientific research and programs to strengthen scientific research potential and science education programs at all levels in the mathematical, physical, medical, biological, social, and other sciences, and to initiate and support research fundamental to the engineering process and programs to strengthen engineering research potential and engineering education programs at all levels in the various fields of engineering, by making contracts or other arrangements (including grants, loans, and other forms of assistance) to support such scientific, engineering, and educational activities and to appraise the impact of research upon industrial development and upon the general welfare;

(2) to award, as provided in section 10, scholarships and graduate fellowships for study and research in the sciences or in engineering;

(3) to foster the interchange of scientific and engineering information among scientists and engineers in the United States and foreign countries;

(4) to foster and support the development and use of computer and other scientific and engineering methods and technologies, primarily for research and education in the sciences and engineering;

(5) to evaluate the status and needs of the various sciences and fields of engineering as evidenced by programs, projects, and studies undertaken by agencies of the Federal Government, by individuals, and by public and private research groups, employing by grant or contract such consulting services as it may deem necessary for the purpose of such evaluations;

and to take into consideration the results of such evaluations in correlating the research and educational programs undertaken or supported by the Foundation with programs, projects, and studies undertaken by agencies of the Federal Government, by individuals, and by public and private research groups;

(6) to provide a central clearinghouse for the collection, interpretation, and analysis of data on scientific and engineering resources 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.] *Congress; and*

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

(b) CONTRACTS, GRANTS, LOANS, ETC. FOR SCIENTIFIC AND ENGINEERING ACTIVITIES; FINANCING OF PROGRAMS.—The Foundation is authorized to initiate and support specific scientific and engineering activities in connection with matters relating to international cooperation, national security, and the effects of scientific and engineering applications upon society by making contracts or other arrangements (including grants, loans, and other forms of assistance) for the conduct of such activities. When initiated or supported pursuant to requests made by any other Federal department or agency, including the Office of Technology Assessment, such activities shall be financed whenever feasible from funds transferred to the Foundation by the requesting official as provided in section 14(f), and any such activities shall be unclassified and shall be identified by the Foundation as being undertaken at the request of the appropriate official.

(c) SCIENTIFIC AND ENGINEERING RESEARCH PROGRAMS AT ACADEMIC AND OTHER NONPROFIT INSTITUTIONS; APPLIED SCIENTIFIC RESEARCH AND ENGINEERING RESEARCH PROGRAMS BY PRESIDENTIAL DIRECTIVE; EMPLOYMENT OF CONSULTING SERVICES; COORDINATION OF ACTIVITIES.—In addition to the authority contained in subsections (a) and (b), the Foundation is authorized to initiate and support scientific and engineering research, including applied research, at academic and other nonprofit institutions. When so directed by the President, the Foundation is further authorized to support, through other appropriate organizations, applied scientific research and engineering research relevant to national problems involving the public interest. In exercising the authority contained in this subsection, the Foundation may employ by grant or contract such consulting services as it deems necessary, and shall coordinate and correlate its activities with respect to any such problem with other agencies of the Federal Government undertaking similar programs in that field.

(d) PROMOTION OF BASIC RESEARCH AND EDUCATION IN SCIENCE AND ENGINEERING.—The Board and the Director shall recommend and encourage the pursuit of national policies for the promotion of research and education in science and engineering.

(e) BALANCING OF RESEARCH AND EDUCATIONAL ACTIVITIES IN THE SCIENCES AND ENGINEERING.—In exercising the authority and discharging the functions referred to in the foregoing subsections, it shall be an objective of the Foundation to strengthen research and education in the sciences and engineering, including independent research by individuals, throughout the United States, and to avoid undue concentration of such research and education.

(f) ANNUAL REPORT TO THE PRESIDENT AND CONGRESS.—The Foundation shall render an annual report to the President for submission on or before the 15th day of April of each year to the Congress, summarizing the activities of the Foundation and making such recommendations as it may deem appropriate. Such report shall include information as to the acquisition and disposition by the Foundation of any patents and patent rights.

(g) SUPPORT OF ACCESS TO COMPUTER NETWORKS.—In carrying out subsection (a)(4), the Foundation is authorized to foster and support access by the research and education communities to computer networks which may be used substantially for purposes in addition to research and education in the sciences and engineering, if the additional uses will tend to increase the overall capabilities of the networks to support such research and education activities.

NATIONAL SCIENCE AND TECHNOLOGY POLICY ACT

SEC. 205. POLICY PLANNING; ANALYSIS; ADVICE; ESTABLISHMENT OF ADVISORY PANEL.

[42 U.S.C. 6614]

(a) The Office shall serve as a source of scientific and technological analysis and judgment for the President with respect to major policies, plans, and programs of the Federal Government. In carrying out the provisions of this section, the Director shall—

(1) seek to define coherent approaches for applying science and technology to critical and emerging national and international problems and for promoting coordination of the scientific and technological responsibilities and programs of the Federal departments and agencies in the resolution of such problems;

(2) assist and advise the President in the preparation of the Science and Technology Report, in accordance with section 209 of this Act;

(3) gather timely and authoritative information concerning significant developments and trends in science, technology, and in national priorities, both current and prospective, to analyze and interpret such information for the purpose of determining whether such developments and trends are likely to affect achievement of the priority goals of the Nation as set forth in section 101(b) of this Act;

(4) encourage the development and maintenance of an adequate data base for human resources in science, engineering, and technology, including the development of appropriate models to forecast future manpower requirements, and assess the

impact of major governmental and public programs on human resources and their utilization;

(5) initiate studies and analyses, including systems analyses and technology assessments, of alternatives available for the resolution of critical and emerging national and international problems amendable to the contributions of science and technology and, insofar as possible, determine and compare probable costs, benefits, and impacts of such alternatives;

(6) advise the President on the extent to which the various scientific and technological programs, policies, and activities of the Federal Government are likely to affect the achievement of the priority goals of the Nation as set forth in section 101(b) of this Act;

(7) provide the President with periodic reviews of Federal statutes and administrative regulations of the various departments and agencies which affect research and development activities, both internally and in relation to the private sector, or which may interfere with desirable technological innovation, together with recommendations for their elimination, reform, or updating as appropriate;

(8) develop, review, revise, and recommend criteria for determining scientific and technological activities warranting Federal support, and recommend Federal policies designed to advance (A) the development and maintenance of broadly based scientific and technological capabilities, including human resources, at all levels of government, academia, and industry, and (B) the effective application of such capabilities to national needs;

(9) assess and advise on policies for international cooperation in science and technology which will advance the national and international objectives of the United States;

(10) identify and assess emerging and future areas in which science and technology can be used effectively in addressing national and international problems;

(11) report at least once each year to the President and the Congress on the overall activities and accomplishments of the Office, pursuant to section 206 of this Act;

(12) periodically survey the nature and needs of national science and technology policy and make recommendations to the President, for review and transmission to the Congress, for the timely and appropriate revision of such policy in accordance with section 102(a)(6) of this Act; **[**and**]**

(13) develop strategies, in consultation with the Office of Homeland Security, the President's Critical Infrastructure Protection Board, and the relevant Federal departments and agencies, to foster greater coordination of Federal research and development activities and promote cooperation between the Federal Government, institutions of higher education, and private industry in the field of cyber security; and

[(13)**]** *(14)* perform such other duties and functions and make and furnish such studies and reports thereon, and recommendations with respect to matters of policy and legislation as the President may request.

(b)(1) The Director shall establish an Intergovernmental Science, Engineering, and Technology Advisory Panel (hereinafter referred

to as the "Panel"), whose purpose shall be to (A) identify and define civilian problems at State, regional, and local levels which science, engineering, and technology may assist in resolving or ameliorating; (B) recommend priorities for addressing such problems; and (C) advise and assist the Director in identifying and fostering policies to facilitate the transfer and utilization of research and development results so as to maximize their application to civilian needs.

(2) The Panel shall be composed of (A) the Director of the Office, or his representative; (B) at least ten members representing the interests of the States, appointed by the Director of the Office after consultation with State officials; and (C) the Director of the National Science Foundation, or his representative.

(3)(A) The Director of the Office, or his representative, shall serve as Chairman of the Panel.

(B) The Panel shall perform such functions as the Chairman may prescribe, and shall meet at the call of the Chairman.

(4) Each member of the Panel shall, while serving on business of the Panel, be entitled to receive compensation at a rate not to exceed the daily rate prescribed for GS–18 of the General Schedule under section 5332 of title 5, United States Code, including travel-time, and, while so serving away from his home or regular place of business, he may be allowed travel expenses, including per diem in lieu of subsistence in the same manner as the expenses authorized by section 5703(b) of title 5, United States Code, for persons in government service employed intermittently.

○