

Resolved, That the Senate Legal Counsel is authorized to represent Secretary Thomson and Mr. Wineman in the case of *Newdow v. Eagen*, et al.

AUTHORIZING REPRESENTATION BY SENATE LEGAL COUNSEL

Mr. REID. Mr. President, I ask unanimous consent the Senate proceed to S. Res. 344.

The PRESIDING OFFICER. The clerk will report the resolution by title.

The legislative clerk read as follows:

A resolution (S. Res. 344) to authorize representation by the Senate Legal Counsel in *Manhardt v. Federal Judicial Qualifications Committee*, et al.

There being no objection, the Senate proceeded to consider the resolution.

Mr. DASCHLE. Mr. President, an unsuccessful applicant for U.S. Attorney in Los Angeles has commenced a civil action in Federal court in California against Senator FEINSTEIN, Senator BOXER, a prominent Republican businessman and political leader in California, and a judicial screening panel set up by these defendants, to challenge the use of this screening panel to identify potential nominees for Federal District Court judgeships in California. Specifically, the plaintiff alleges that the use of informal screening panels to develop lists of potential judicial nominees violates the Federal Advisory Committee Act, the Government in the Sunshine Act, and the separation of powers.

The laws underlying this suite do not apply to the Senate, and the Speech or Debate Clause bars suits against legislators for the performance of their duties under the Constitution. Thus, there is no legal basis for suing Senators for their role in forming, appointing, or relying on judicial screening panels.

Further, the use of informal judicial selection panels to identify potential judicial nominees as a part of the advice and consent function has a long and respected history. Also, the Supreme Court's holding in *Public Citizen versus U.S. Department of Justice* that the Federal Advisory Committee Act does not apply to the longstanding practice of soliciting views on prospective judicial nominees from an American Bar Association committee provides ample support for the challenged practice.

This resolution would authorize the Senate legal counsel to represent the Senators sued in this action to protect their role in the advice and consent process by which the President and the Senate share responsibility for the appointment of Federal judges under the Constitution.

Mr. REID. Mr. President, I ask unanimous consent the resolution and preamble be agreed to, the motion to reconsider be laid on the table, and that any statements in relation thereto be printed in the RECORD.

The PRESIDING OFFICER. Without objection, it is so ordered.

The resolution (S. Res. 344) was agreed to.

The preamble was agreed to.

The resolution, with its preamble, reads as follows:

S. RES. 344

Whereas, Senators Dianne Feinstein and Barbara Boxer have been named as defendants in the case of *Manhardt v. Federal Judicial Qualifications Committee*, et al., Case No. 02-4484 AHM, now pending in the United States District Court for the Central District of California; and

Whereas, pursuant to sections 703(a) and 704(a)(1) of the Ethics in Government Act of 1978, 2 U.S.C. §§288b(a) and 288c(a)(1), the Senate may direct its counsel to represent Members of the Senate in civil actions with respect to their official responsibilities: Now, therefore, be it

Resolved, That the Senate Legal Counsel is authorized to represent Senators Dianne Feinstein and Barbara Boxer in the case of *Manhardt v. Federal Judicial Qualifications Committee*, et al.

CYBER SECURITY RESEARCH AND DEVELOPMENT ACT

Mr. REID. Mr. President, I ask unanimous consent the Senate now proceed to Calendar No. 549, S. 2182.

The PRESIDING OFFICER. The clerk will report the bill by title.

The legislative clerk read as follows:

A bill (S. 2182) to authorize funding for the computer and network security research and development and research fellowship programs, and for other purposes.

There being no objection, the Senate proceeded to consider the bill.

CHECKLIST PROVISION—CYBER SECURITY RESEARCH AND DEVELOPMENT ACT, HR 3394

Mr. HOLLINGS. I would like to engage in a brief colloquy with the ranking member of the Science, Technology, and Space Subcommittee of the Commerce Committee, Senator ALLEN, regarding the provisions of H.R. 3394 that provide for the National Institute of Standards and Technology, NIST, to develop checklists for widely used software products.

Mr. ALLEN. The committee, particularly Senators WYDEN and EDWARDS, working with NIST and industry, have reached agreement on this provision. We recognize that there is no "one-size-fits-all" configuration for any hardware or software systems. We have given NIST flexibility in choosing which checklists to develop and update. We have not required any Federal agency to use the specific settings and options recommended by these checklists.

Mr. HOLLINGS. The ranking member is correct. Our intent with this provision is not to develop separate checklists for every possible Federal configuration. Rather, the checklists would provide agencies with recommendations that will improve the quality and security of the settings and options they select. The use of any checklist should, of course, be consistent with guidance from the Office of Management and Budget.

Mr. ALLEN. I agree with the chairman.

Mr. WYDEN. Mr. President, I would like to say a few words about the Senate's passage of the Cybersecurity Research and Development Act.

Americans today live in an increasingly networked world. The spread of the Internet creates lots of great new opportunities. But there is also a downside: security risks. The Internet connects people not just to friends, potential customers, and useful sources of information, but also to would-be hackers, viruses, and cybercriminals.

In July 2001, after I became chairman of the Science and Technology Subcommittee of the Senate Commerce Committee, I chose cybersecurity as the topic for my first hearing. The message from that hearing was that cybersecurity risks are mounting. And that was before the horrific attacks of September 11 hammered home the point that there are determined, organized enemies of this country who wish to wreak as much havoc as they can. The terrorists are looking for vulnerabilities, and they are not technological simpletons.

This legislation is essential to the Nation's effort to address cybersecurity threats. It is a necessary complement to both the homeland security legislation pending in Congress and to the draft cybersecurity strategy released on September 18 by the administration. Because reorganizing the Federal Government to deal more effectively with security threats is only part of the battle. The same goes for many of the steps called for in the Administration's cybersecurity strategy.

In the long run, all Government and private sector cybersecurity efforts depend on people—trained experts with the knowledge and skills to develop innovative solutions and respond creatively and proactively to evolving threats. Without a strong core of cybersecurity experts, no amount of good intentions and no amount of Government reorganizing will be sufficient to keep this country one step ahead of hackers and cyberterrorists.

Therefore, this legislation makes a strong commitment to support basic cybersecurity research, so that the country's pool of top-flight cybersecurity experts can keep pace with the evolving risks. Specifically, the bill authorizes \$978 million over five years to create new cybersecurity research and development programs at the National Science Foundation, NSF, and the National Institute of Standards and Technology, NIST. The NSF program will provide funding for innovative research, multidisciplinary academic centers devoted to cybersecurity, and new courses and fellowships to educate the cybersecurity experts of the future. The NIST program likewise will support cutting-edge cybersecurity research, with a special emphasis on promoting cooperative efforts between government, industry, and academia.

All of these programs will support advanced cybersecurity research at a

basic, non-applied level, some of which may not pay off for a number of years. Nonetheless, it is my strong expectation that as this fundamental research yields results, those results will be made available promptly to the private sector, where they will serve as the foundation for a wide range of practical, tangible cybersecurity improvements, products, and solutions. This kind of commercialization of the results of Federal investment in computer and network security research is consistent with long-standing U.S. technology transfer policy, and will serve the national interest in enhancing the security and reliability of cyberspace for commercial, academic, and individual users, as well as Federal and state governments.

I should also note that, in addition to the extramural research grants at NSF and NIST, the bill will support NIST's ongoing cybersecurity research. Americans for Computer Privacy, the Business Software Alliance, the Information Technology Association of America, the Information Technology Industry Council, the Software & Information Industry Association, and the U.S. Chamber of Commerce noted in a recent letter to Senators LIEBERMAN and THOMPSON that NIST's Computer Security Division's "job is to improve the security of civilian computer systems through technical standards and cooperation with industry." This legislation will provide funding to support NIST in continuing that work.

There is broad consensus on the need for this legislation. It has already passed the House by an overwhelming bipartisan vote, thanks to the leadership of Congressman SHERRY BOEHLERT. I introduced the Senate version, S. 2182, and the ranking member of the Science and Technology Subcommittee, Senator ALLEN, joined me in shepherding it through the Commerce Committee. We worked closely with Senator EDWARDS on provisions to help Federal Government agencies safeguard the security of their computer systems. And we worked closely with businesses and experts in the cybersecurity field, to ensure widespread support within the high tech industry.

Specifically, I would like to mention a few changes that have been made to the bill since we reported the bill from the Commerce Committee. The most significant changes to the bill came in working with Senator EDWARDS and cybersecurity businesses and experts to give federal agencies additional tools to strengthen the security of their computer systems, while at the same time encouraging innovation and allowing agencies the flexibility to adopt a variety of cybersecurity products.

In addition, working with our colleagues on the House Science Committee, we adjusted the list of research areas of basic NSF research grants. No list could ever encompass every computer security technology, and for that reason the list is not exclusive. The intention was simply to give some gen-

eral examples of broad research areas, without naming specific technologies. But obviously, when individual grants are awarded, they may well focus on particular technologies that are not listed by name in the final version of the bill, such as digital watermarking.

Another change is the deletion of a cost-sharing provision added in committee. Instead, the bill language makes it clear that research grants under the NIST cybersecurity research program will be awarded to institutions of higher education rather than directly funding industry research.

I thank my Senate colleague for taking up and approving this timely legislation. The stakes are high, and you can bet that hackers and cyberterrorists won't stand still. So it is important to launch these new cybersecurity research programs as soon as possible. I believe this legislation needs to be enacted into law this fall, and I urge the House and the President to move swiftly to ensure that happens.

Mr. ALLEN. Mr. President, I rise to thank my colleagues for their unanimous support of S. 2182, the Cyber Security Research & Development Act. I would also like to thank Senator WYDEN for his leadership and continued work on pushing this important measure through the legislative process.

S. 2182 addresses the important issue of cyber security. As our reliance on technology and the Internet have grown over the past decade, our vulnerability to attacks on the Nation's critical infrastructure and networked systems has also grown exponentially. The high degree of interdependence between information systems exposes America's network infrastructure to both benign and destructive disruptions. Such cyber attacks can take several forms, including: defacement of web sites; denial of service; virus infection throughout the computer network; and unauthorized intrusions and sabotage of systems and networks resulting in critical infrastructure outages and corruption of vital data.

Past attacks, such as the Code Red virus, show the types of danger and potential disruption cyber attacks can have on our Nation's infrastructure. The cyber threats before this country are significant and are unfortunately only getting more complicated and sophisticated as time goes on.

A survey last year by the Computer Security Institute and FBI found that 85 percent of 538 respondents experienced computer intrusions. 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 exploded from 9,589 in 1999 to 52,658 in 2001. What is alarming is that CERT estimates these statistics may only represent 20% of the incidents that actually have occurred.

A recent public opinion survey indicates that over 70 percent of Americans are concerned about computer security and 74 percent are concerned about terrorist using the Internet to launch a cyber-attack against our country's infrastructure. One survey shows that half of all information technology professionals believe that a major attack will be launched against the Federal Government in the next 12 months.

Indeed, cyber security is essential to both homeland security and national security. The Internet's security and reliability support the economy, critical infrastructures and national defense. At a time when uncertainty threatens confidence in our nation's preparedness, the Federal Government needs to make information and cyber security a priority.

Currently, federally funded research on cyber security is less than \$60 million per year. Experts believe that fewer than 100 United States researchers have the experience and expertise to conduct cutting edge research in cyber security.

The Cyber Security Research and Development Act will play a major role in fostering greater research in methods to prevent future cyber attacks and design more secure networks. Our legislation will harness and link the intellectual power of the National Science Foundation, the National Institute of Science and Technology, our Nation's universities, and private industry to develop new and improved computer cryptography and authentication, firewalls, computer forensics, intrusion detection, wireless security and systems management.

In addition, our bill is designed to draw more college undergraduate and graduate students into the field of cyber security research. It establishes programs to use internships, research opportunities, and better equipment to engage students in this field. America is a leader in the computer hardware and software development. In order to preserve America's technological edge, we must have a continuous pipeline of new students involved in computer science study and research.

S. 2182 highlights the role the Federal Government will play in helping prepare and prevent cyber attacks, but only if we can ensure the cutting edge research and technology funded in this legislation is made commercially available.

Clearly, there is an urgent need for private sector, academic, and individual users as well as the Federal and State governments to deploy security innovations. I am confident that the federal investment for long-term projects outlined in this legislation will yield significant results to enhance the security and reliability of cyberspace.

I am glad to see the Senate come together and pass this important legislation and again thank my colleague from Oregon for his leadership. I have truly enjoyed working with him for the

successful passage of this positive and constructive legislation that will improve the security of Americans.

Mr. REID. Mr. President, I ask unanimous consent that the committee-reported substitute amendment be withdrawn; and on behalf of Senators WYDEN and ALLEN, I ask unanimous consent that the amendment at the desk be considered and agreed to, the bill, as amended, be read three times, and the Commerce Committee then be discharged from further consideration of H.R. 3394, the House companion; that all after the enacting clause be stricken, and the text of S. 2182, as amended, be inserted in lieu thereof; that H.R. 3394 be read three times, passed, the motion to reconsider be laid on the table; and that any statements relating to this matter be printed in the RECORD, with no intervening action or debate; and that S. 2182 be returned to the calendar.

The PRESIDING OFFICER. Without objection, it is so ordered.

The committee amendment in the nature of a substitute was withdrawn.

The amendment (No. 4890) was agreed to.

(The amendment is printed in today's RECORD under "Text of Amendments.")

The bill (S. 2182), as amended, was read the third time.

The bill (H.R. 3394), as amended, was read the third time and passed, as follows:

(The bill will be printed in a future edition of the RECORD.)

INLAND FLOOD FORECASTING AND WARNING SYSTEM ACT OF 2002

Mr. REID. Mr. President, I ask unanimous consent that the Senate proceed to calendar No. 698, H.R. 2486.

The PRESIDING OFFICER. The clerk will state the bill by title.

The legislative clerk read as follows:

A bill (H.R. 2486) to authorize the National Oceanic and Atmospheric Administration, through the United States Weather Research Program, to conduct research and development, training, and outreach activities relating to inland flood forecasting improvement, and for other purposes.

There being no objection, the Senate proceeded to consider the bill.

Mr. REID. Mr. President, I ask unanimous consent that the bill be read the third time and passed; that the motion to reconsider be laid upon the table; and that any statements relating to this matter be printed in the RECORD.

The PRESIDING OFFICER. Without objection, it is so ordered.

The bill (H.R. 2486) was read the third time and passed.

(The bill will be printed in a future edition of the RECORD.)

BLACK LUNG BENEFIT CONSOLIDATION

Mr. REID. Mr. President, I ask unanimous consent that the Senate proceed

to the consideration of H.R. 5542 now at the desk.

The PRESIDING OFFICER. The clerk will state the bill by title.

The legislative clerk read as follows:

A bill (H.R. 5542) to consolidate all black lung benefit responsibility under a single official, and for other purposes.

There being no objection, the Senate proceeded to consider the bill.

Mr. REID. Mr. President, I ask unanimous consent that the bill be read the third time, and passed; that the motion to reconsider be laid upon the table, and that any statements relating to the bill be printed in the RECORD.

The PRESIDING OFFICER. Without objection, it is so ordered.

The bill (H.R. 5542) was read the third time and passed.

(This bill will be printed in a future edition of the RECORD.)

ORDERS FOR THURSDAY, OCTOBER 17, 2002

Mr. REID. Mr. President, I ask unanimous consent that when the Senate completes its business today, it stand in adjournment until 11 a.m., Thursday, October 17; that following the prayer and the pledge, the morning hour be deemed to have expired, the Journal of the proceedings be approved to date, the time for the two leaders be reserved for their use later in the day, and that there be a period of morning business, with Senators permitted to speak therein for up to 10 minutes each, with the time until 12 noon under the control of the Republican leader or his designee, and the time from 12 noon to 1 p.m. under the control of Senator DASCHLE or his designee.

The PRESIDING OFFICER. Without objection, it is so ordered.

ADJOURNMENT UNTIL 11 A.M. TOMORROW

Mr. REID. Mr. President, there is no further business to come before the Senate. Therefore, I ask unanimous consent that we stand in adjournment under the previous order.

There being no objection, the Senate, at 9:04 p.m., adjourned until Thursday, October 17, 2002, at 11 a.m.

NOMINATIONS

Executive nominations received by the Senate October 16, 2002:

BROADCASTING BOARD OF GOVERNORS

BLANQUITA WALSH CULLUM, OF VIRGINIA, TO BE A MEMBER OF THE BROADCASTING BOARD OF GOVERNORS FOR A TERM EXPIRING AUGUST 13, 2005, VICE CHERYL F. HALPERN, TERM EXPIRED.

EXECUTIVE OFFICE OF THE PRESIDENT

FELICIANO FOYO, OF FLORIDA, TO BE A MEMBER OF THE ADVISORY BOARD FOR CUBA BROADCASTING FOR A TERM EXPIRING AUGUST 12, 2004, VICE JORGE L. MAS.

DEPARTMENT OF STATE

MARY CARLIN YATES, OF OREGON, A CAREER MEMBER OF THE SENIOR FOREIGN SERVICE, CLASS OF MINISTER-COUNSELOR, TO BE AMBASSADOR EXTRAORDINARY AND

PLENIPOTENTIARY OF THE UNITED STATES OF AMERICA TO THE REPUBLIC OF GHANA.

IN THE AIR FORCE

THE FOLLOWING NAMED OFFICERS FOR APPOINTMENT IN THE RESERVE OF THE AIR FORCE TO THE GRADE INDICATED UNDER TITLE 10, U.S.C., SECTION 12203:

To be major general

BRIGADIER GENERAL RICHARD C. COLLINS, 0000
BRIGADIER GENERAL SCOTT R. NICHOLS, 0000
BRIGADIER GENERAL DAVID A. ROBINSON, 0000
BRIGADIER GENERAL MARK V. ROSENKER, 0000
BRIGADIER GENERAL CHARLES E. STENNER JR., 0000
BRIGADIER GENERAL THOMAS D. TAVERNEY, 0000
BRIGADIER GENERAL KATHY E. THOMAS, 0000

To be brigadier general

COLONEL RICARDO APONTE, 0000
COLONEL FRANK J. CASSERINO, 0000
COLONEL CHARLES D. ETHREDGE, 0000
COLONEL THOMAS M. GISLER JR., 0000
COLONEL JAMES W. GRAVES, 0000
COLONEL JOHN M. HOWLETT, 0000
COLONEL MARTIN M. MAZICK, 0000
COLONEL HANFRED J. MOEN JR., 0000
COLONEL JAMES M. MUNGENAST, 0000
COLONEL JACK W. RAMSAUR II, 0000
COLONEL DAVID N. SENTRY, 0000
COLONEL BRADLEY C. YOUNG, 0000

IN THE ARMY

THE FOLLOWING ARMY NATIONAL GUARD OF THE UNITED STATES OFFICERS FOR APPOINTMENT IN THE RESERVE OF THE ARMY TO THE GRADE INDICATED UNDER TITLE 10, U.S.C., SECTION 12203:

To be major general

BRIGADIER GENERAL EMILE P. BATAILLE, 0000
BRIGADIER GENERAL DANIEL D. DENSFORD, 0000
BRIGADIER GENERAL DANIEL E. LONG JR., 0000
BRIGADIER GENERAL MICHAEL J. SQUIER, 0000
BRIGADIER GENERAL ROY M. UMBARGER, 0000
BRIGADIER GENERAL ANTONIO J. VICENS-GONZALEZ, 0000
BRIGADIER GENERAL WALTER E. ZINK II, 0000

To be brigadier general

COLONEL NORMAN E. ARFLACK, 0000
COLONEL JERRY G. BECK JR., 0000
COLONEL RAYMOND W. CARPENTER, 0000
COLONEL HERMAN M. DEENER, 0000
COLONEL ROBERT P. FRENCH, 0000
COLONEL JOHN T. FURLOW, 0000
COLONEL CHARLES L. GABLE, 0000
COLONEL FRANCIS P. GONZALES, 0000
COLONEL DEAN E. JOHNSON, 0000
COLONEL DAVID A. LEWIS, 0000
COLONEL THOMAS D. MILLS, 0000
COLONEL VERN T. MIYAGI, 0000
COLONEL ROGUE C. NIDO LANASUSSE, 0000
COLONEL J. W. NOLES, 0000
COLONEL THOMAS R. RAGLAND, 0000
COLONEL TERRY L. ROBINSON, 0000
COLONEL CHARLES G. RODRIGUEZ, 0000
COLONEL CHARLES D. SAFLEY, 0000
COLONEL RANDALL E. SAYRE, 0000
COLONEL DONALD C. STORM, 0000
COLONEL WILLIAM H. WADE, 0000
COLONEL GREGORY L. WAYT, 0000
COLONEL MERREL W. YOCUM, 0000

IN THE AIR FORCE

THE FOLLOWING NAMED OFFICERS FOR APPOINTMENT TO THE GRADE INDICATED IN THE RESERVE OF THE AIR FORCE UNDER TITLE 10, U.S.C., SECTION 12203:

To be colonel

BRANFORD J. MCALLISTER, 0000
ALICE SMART, 0000

IN THE NAVY

THE FOLLOWING NAMED OFFICERS FOR REGULAR APPOINTMENT TO THE GRADES INDICATED IN THE UNITED STATES NAVY UNDER TITLE 10, U.S.C., SECTION 531:

To be commander

ROWLAND E. MCCOY, 0000

To be lieutenant commander

ROGER L. BOUMA, 0000
JAMES T. DENLEY, 0000
JOHN V. DICKENS III, 0000
KIMBERLY S. FRY, 0000
JEROME A. HINSON, 0000
TAMMY C. JONES, 0000
JOHN T. LEE, 0000
STEVEN M. RESWEBER, 0000
ROBERT D. REUER, 0000
LOUIS ROSA, 0000
DUANE A. SAND, 0000
FRANK W. SHEARIN III, 0000
JOHN M. SHIMOTSU, 0000
RALPH R. SMITH III, 0000
WALTER R. STEELE, 0000
DAVID A. TOELLNER, 0000
ROBERT A. WACHTEL, 0000
ALAN K. WILMOT, 0000