S. HRG. 109–293

RESEARCH AND DEVELOPMENT TO PROTECT AMERICA'S COMMUNITIES FROM DISASTER

HEARING

BEFORE THE

SUBCOMMITTEE ON DISASTER PREVENTION AND PREDICTION

OF THE

COMMITTEE ON COMMERCE, SCIENCE, AND TRANSPORTATION UNITED STATES SENATE

ONE HUNDRED NINTH CONGRESS

FIRST SESSION

JUNE 8, 2005

Printed for the use of the Committee on Commerce, Science, and Transportation

U.S. GOVERNMENT PRINTING OFFICE

25–862 PDF WASHINGTON : 2006

For sale by the Superintendent of Documents, U.S. Government Printing Office
Internet: bookstore.gpo.gov Phone: toll free (866) 512–1800; DC area (202) 512–1800
Fax: (202) 512–2250 Mail: Stop SSOP, Washington, DC 20402–0001

SENATE COMMITTEE ON COMMERCE, SCIENCE, AND TRANSPORTATION

ONE HUNDRED NINTH CONGRESS

FIRST SESSION

TED STEVENS, Alaska, *Chairman*

JOHN MCCAIN, Arizona
CONRAD BURNS, Montana
TRENT LOTT, Mississippi
KAY BAILEY HUTCHISON, Texas
OLYMPIA J. SNOWE, Maine
GORDON H. SMITH, Oregon
JOHN ENSIGN, Nevada
GEORGE ALLEN, Virginia
JOHN E. SUNUNU, New Hampshire
JIM DEMINT, South Carolina
DAVID VITTER, Louisiana

DANIEL K. INOUYE, Hawaii, *Co-Chairman*
JOHN D. ROCKEFELLER IV, West Virginia
JOHN F. KERRY, Massachusetts
BYRON L. DORGAN, North Dakota
BARBARA BOXER, California
BILL NELSON, Florida
MARIA CANTWELL, Washington
FRANK R. LAUTENBERG, New Jersey
E. BENJAMIN NELSON, Nebraska
MARK PRYOR, Arkansas

LISA J. SUTHERLAND, *Republican Staff Director*
CHRISTINE DRAGER KURTH, *Republican Deputy Staff Director*
DAVID RUSSELL, *Republican Chief Counsel*
MARGARET L. CUMMISKY, *Democratic Staff Director and Chief Counsel*
SAMUEL E. WHITEHORN, *Democratic Deputy Staff Director and General Counsel*
LILA HARPER HELMS, *Democratic Policy Director*

SUBCOMMITTEE ON DISASTER PREVENTION AND PREDICTION

JIM DEMINT, South Carolina, *Chairman*

TED STEVENS, Alaska
GORDON H. SMITH, Oregon
DAVID VITTER, Louisiana

E. BENJAMIN NELSON, Nebraska, *Ranking*
MARIA CANTWELL, Washington
BILL NELSON, Florida

CONTENTS

RESEARCH AND DEVELOPMENT TO PROTECT AMERICA'S COMMUNITIES FROM DISASTER

WEDNESDAY, JUNE 8, 2005

U.S. SENATE,
SUBCOMMITTEE ON DISASTER PREVENTION AND PREDICTION,
COMMITTEE ON COMMERCE, SCIENCE, AND TRANSPORTATION,
Washington, DC.

The Subcommittee met, pursuant to notice, at 2:30 p.m. in room SR–253, Russell Senate Office Building, Hon. Jim DeMint, Chairman of the Subcommittee, presiding.

OPENING STATEMENT OF HON. JIM DEMINT, U.S. SENATOR FROM SOUTH CAROLINA

Senator DEMINT. Let's call the hearing to order. This is the first hearing of the Subcommittee on Disaster Prevention and Prediction. I think we've got a Ranking Member on the way here, but we'll go ahead and get started, as a courtesy to our witnesses who are here.

This afternoon, we are going to be focusing the Subcommittee's attention on the role that the agencies under the jurisdiction of the Commerce Committee play in supporting the national homeland security mission. As we are all aware, September 11 profoundly changed America. Before the attacks on New York, Washington, and Pennsylvania, counterterrorism was largely the concern of other countries. Foreign nations were preoccupied with defeating the threat from groups like the Red Army Faction, the Shining Path, the Real IRA. And while the United States monitored these groups, the true fighting largely fell to other nations. That has all changed.

As a part of the Nation's response to September 11, the President and the Congress created the Department of Homeland Security. This agency combined the intelligence, law enforcement, monitoring, first-response, and scientific capabilities of numerous federal agencies under one roof. I am confident that the consolidation of these agencies at the Department of Homeland Security will enhance the Nation's efforts to protect the homeland.

While the Department represents a significant improvement over the multi-agency approach before 9/11, the Department is not the only federal entity contributing to the Nation's response to the threat posed by the international terrorist organizations. Many non-Defense, and non-Homeland-Security agencies play a crucial role in preventing and preparing for the threat posed by terrorists.

This is particularly true in the scientific research community, where significant portions of homeland security research is performed outside the Department of Homeland Security. Specifically, the National Institute for Standards and Technology, the National Oceanic and Atmospheric Administration, and the National Science Foundation are appearing this afternoon to discuss how their work supports the homeland security science-and-technology efforts.

All of these agencies had robust research programs in place long before September 11. They were able to transition and adjust their research regimes quickly so they could respond to the new threat while still supporting their fundamental core mission.

NIST, which grew out of the Bureau of Standards, has long been responsible for helping establish the processes and standards that ensure that devices operate in a manner consistent with their purpose and design. For example, it's critically important that a tool, such as a radiation detector used by a firefighter, behaves as expected when deployed in the field.

NOAA's mission has always been monitoring the ocean and atmosphere, and warning communities when there is a threat. NOAA's expertise in observing the weather in local communities, as well as their work in developing atmospheric models, provides an invaluable tool to the local first-responders in the event of a hazardous chemical release in one of our communities. For example, earlier this year the weather forecast office in Columbia, South Carolina, played a crucial role in providing weather inputs into the atmospheric models used during a chlorine release from a train wreck in Graniteville. While this was not a terrorist attack, the resources and cooperation between NOAA, the Department of Homeland Security, and the first-responders provide an example of how the agencies can work together in response to a disaster.

Finally, NSF support of long-term revolutionary research will lay the foundation for the next generation of technologies to protect the homeland. By pushing the boundaries, scientists will often fail; but, when they make that dramatic and revolutionary breakthrough, they will enable a field of technology that will make the country safer and help us defeat terrorists.

I'm looking forward to the comments of the witnesses this afternoon. When the work of America's scientists and engineers is combined with the courage and commitment of America's first-responders, law enforcement personnel, and intelligence officers, American's homeland can surely be safer.

With that, I'll ask—I guess the Ranking Member is not here. We'll allow his comments later. I'll introduce our panelists.

Appearing before the Subcommittee this afternoon is Dr. Hratch G. Semerjian. Dr. Semerjian is Acting Director of the National Institute of Standards and Technology. Joining him is Vice Admiral Conrad Lautenbacher. Admiral Lautenbacher is Under Secretary of Commerce for Oceans and Atmosphere, and NOAA Administrator. Finally, Dr. Arden Bement—I ought to be able to pronounce that—Director of National Science Foundation, will be addressing the Subcommittee this morning.

With that, we'll—Senator McCain, you said you did not want an opening statement.

Senator MCCAIN. Right.

Senator DEMINT. Thank you.

OK, with that, we'll start with Dr. Semerjian. Please provide a short summary of your testimony. All of your testimonies will be submitted completely for the record.

Thank you, sir.

STATEMENT OF DR. HRATCH G. SEMERJIAN, ACTING DIRECTOR, NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY, TECHNOLOGY ADMINISTRATION, DEPARTMENT OF COMMERCE

Dr. SEMERJIAN. Thank you, Chairman DeMint and Senator McCain.

I'm Hratch Semerjian, Acting Director of NIST. Thank you for this opportunity to testify as part of this distinguished panel about NIST's homeland security efforts.

Our history of supporting homeland- and national-security efforts began shortly after NIST—National Bureau of Standards then, as you pointed out—was founded, in 1901, and continues today with about 100 programs supported by approximately $60 million in direct appropriations, augmented by significant funding support from other agencies, such as the Department of Homeland Security and Department of Justice. Our research is coordinated with the Department of Homeland Security through a Memorandum of Understanding that was signed in May of 2003.

Shortly after September 11, 2001, NIST building and fire experts joined teams of scientists and engineers in assessment of how the Pentagon and the World Trade Center buildings were severely damaged or collapsed in the attacks. NIST experts presented to the U.S. Army Corps of Engineers a report of recommendations for rebuilding and retrofitting the Pentagon that would improve the Pentagon's resistance to similar attacks. NIST also provided assistance through the New York Medical Examiner in identifying victims of the World Trade Center by validating existing methods and devising new DNA analysis techniques to allow identifications that would not otherwise have been possible due to small and degraded samples.

Later this month, we'll conclude our comprehensive technical investigation into how the World Trade Center Towers collapsed by issuing our findings and recommendations for improvements to building and fire codes, standards, and practices.

After the October 2001 bioterrorist attacks, NIST worked with the federal agencies and the private sector to solve the challenging problem of ensuring that commercial radiation facilities could effectively sterilize U.S. mail contaminated with anthrax. When the Hart Senate Office building was contaminated with anthrax, NIST experts in ventilation systems and indoor air quality modeled the flow patterns in the building and helped the EPA with planning of the decontamination efforts.

Subsequent to the attacks of 9/11, NIST has supported the Nation's homeland security effort in a number of different research areas. Today, I'd like to highlight just a few of these for the Subcommittee. I have provided more details, of course, in my written testimony. I should note that in all of these efforts we work very closely with our colleagues in other federal agencies.

As part of its fulfillment of the Patriot Act, NIST conducted the fingerpoint vendor technology evaluation in 2003. This program was the first large-scale evaluation of 34 different fingerprint matching systems. The evaluation, which was based on fingerprint data from a variety of Federal and State government sources, tested performance accuracy for various numbers and types of fingerprints, and provided valuable recommendations and input to the DHS's US–VISIT program.

NIST has provided the common technical thread for the development of several standards important to DHS and the first-responder community. Our Office of Law Enforcement Standards is facilitating communication's interoperability efforts through the consensus standards process by employing a structured approach for confronting interoperability standardization issues. In response to Congress' call for immediate standards for communications interoperability, NIST, along with DHS and DOJ, has developed a partnership with Project 25 Steering Committee made up of public-safety leaders to either significantly accelerate the current P25 standards development or to develop interim communications standards in the absence of P25 standards.

NIST, working with DHS, IEEE—that's the Institute for Electronics and Electronic Engineering—and the private sector organized the necessary expertise and drafting of four new national standards establishing baseline performance criteria and testing requirements for radiation detection devices. The specifications will ensure that ever-more-widely used detectors will reliably discern above background levels of radiation at ports of entry or other key locations.

Additionally, NIST served as the executive agent for the Interagency Board for Equipment Standardization and Interoperability, which was created by the Justice and Defense Departments to advise federal, state, and local agencies on the selection and use of the best available equipment and procedures for first-responders.

The IAB designated NIST to coordinate the development of a suite of eight standards for respiratory equipment, suits, gloves, and other gear that protect first-responders against chemical and biological hazards. These standards were announced in February 2004.

NIST is also conducting research on a class of microsensors that has the potential to serve as a cost-effective early-warning system for toxic gases, and may also be applicable to detection of vapors from explosive materials. NIST also contributed and participated in the process to develop a standard test method for handheld bioassays for detection of anthrax, and is currently managing a supporting project to develop sampling protocols for suspicious powders.

Finally, NIST is managing, for the Department of Homeland Security, an effort to develop a standard for handheld devices for detection of chemical warfare agents that could be used by first-responders. This standard is currently being validated through ASTM.

As the Committee can see by these examples, NIST has a very diverse portfolio of research activity supporting our Nation's homeland security efforts. NIST is working very closely with DHS

Science and Technology Directorate to coordinate our research efforts and to ensure effective implementation. Our long history of research supporting homeland and national security has been critical for the development of an effective deployment of new technologies to protect the homeland.

Once again, thank you for inviting me to testify, and I will be happy to answer any questions you may have.

Thank you, Senator.

[The prepared statement of Dr. Semerjian follows:]

PREPARED STATEMENT OF DR. HRATCH G. SEMERJIAN, ACTING DIRECTOR, NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY, TECHNOLOGY ADMINISTRATION, DEPARTMENT OF COMMERCE

Introduction

Chairman DeMint and Members of the Committee, I am Hratch Semerjian, Acting Director of the National Institute of Standards and Technology (NIST), part of the Technology Administration of the Department of Commerce. Thank you for this opportunity to testify about the contributions of NIST to homeland security. In accomplishing this and all parts of its mission, NIST works in many ways with companies, universities, and other government agencies to help protect our Nation against terrorism.

Since World War II, our Nation's greatest resources for homeland and national security have been a strong economy and a technological edge based on innovation. NIST has the unique mission of providing the measurements and standards infrastructure that the private sector, universities, and government agencies need to develop new technologies, products and services, conduct research, and effectively carry out their responsibilities. NIST measurements and standards and our support of new technologies have strengthened our economy and enabled the development and effective deployment of new homeland security technologies.

NIST's long and productive history of supporting homeland and national security efforts began shortly after its founding as the National Bureau of Standards. Partly in response to the Baltimore fire of 1904, Bureau researchers worked on the development of a national standard for hose couplings as well as a standard for an interchangeable device for nonstandard couplings. Other examples include crucial support for the development of nuclear weapons, aircraft instruments, and other technologies that helped the U.S. succeed in past conflicts. With its long experience as well as a diverse array of expertise, NIST was able to quickly respond to the terrorist attacks of 2001.

NIST currently has about 100 programs, supported by approximately $60 million in direct appropriations augmented by significant funding support from other agencies. This research is coordinated with the Department of Homeland Security (DHS) through a Memorandum of Understanding signed in 2003 between former Under Secretary for Technology, Phillip Bond, and Under Secretary for Science and Technology at DHS, Charles McQueary. In addition, other long standing relationships with the Department of Justice, the State Department, the National Security Agency, and the Office of Management and Budget also ensure that NIST's research is sufficiently coordinated. NIST's homeland security research spans the following areas:

- Chemical, biological, radiological, nuclear, explosive threat detection and remediation
- Safety of buildings and structures
- Safety and effectiveness of emergency responders
- Transportation system safety
- Information security
- Critical infrastructure protection
- Biometric identification
- DNA identification and diagnostics

This afternoon I would like to describe NIST's response to 9/11, and then share just a few examples of other NIST research supporting homeland security.

NIST Response to 9/11 and the World Trade Center Report

As I previously stated NIST responses to the terrorist attacks of 2001 were swift. Shortly after September 11, 2001, NIST building and fire experts joined teams of

scientists and engineers in assessment of how the Pentagon as well as the World Trade Center buildings were severely damaged or collapsed in the attacks. Two months later, NIST experts presented to the U.S. Army Corps of Engineers a report of recommendations for rebuilding and retrofitting the Pentagon that would improve the Pentagon's resistance to similar attacks. NIST also provided assistance to the New York City medical examiner in identifying victims of the World Trade Center by validating existing methods and devising new DNA analysis techniques to allow identifications that would not otherwise have been possible due to small and degraded samples. In addition, NIST contributed expertise on life-cycle cost analysis and priority setting that are key components of the risk assessment guide issued by the Federal Emergency Management Agency (FEMA) to mitigate potential terrorist attacks against buildings.

After the October 2001 bioterrorist attacks, NIST worked with federal agencies and the private sector to ensure that commercial radiation facilities could effectively sterilize U.S. mail contaminated with anthrax. NIST worked with the Armed Forces Radiobiology Research Institute in Bethesda, the U.S. Postal Service, and other agencies to solve this challenging problem.

When the Hart Senate Office Building in Washington, DC was contaminated with anthrax, NIST experts in ventilation systems and indoor air quality modeled the different ways air flow in the building may have disseminated the anthrax spores. These models helped the Environmental Protection Agency plan the decontamination of the building. Since then, similar models have been used to evaluate protection technologies such as air filters, air cleaners, and sensor-driven ventilation systems, and one was incorporated into the Immune Building Toolkit developed by the Defense Advanced Research Projects Agency (DARPA).

The collapse of New York City's World Trade Center structures was among the worst building disasters in recorded history. As part of its larger effort to save lives in future terrorist attacks or natural disasters, NIST has been carrying out a response plan with three parts:

- A building and fire safety investigation of the probable causes of the WTC tower collapse after terrorists flew jet-fuel laden airliners into the buildings, and the associated evacuation and emergency response procedures.
- A research and development program to provide the technical basis for improved building and fire codes, standards, and practices.
- A dissemination and technical assistance program to engage leaders of the construction and building community in implementing proposed changes to practices, standards and codes.

The investigation was conducted with $16 million in funding by the U.S. Congress from an emergency supplemental appropriation and transferred to NIST from FEMA. It builds on the findings and recommendations of an earlier WTC building performance study conducted jointly by FEMA and the American Society of Civil Engineers.

The investigation's analysis, which is the most detailed examination of a building failure ever conducted, established the probable sequences for the collapse of each tower:

1. The aircraft impact severed perimeter columns, damaged interior core columns, and dislodged fireproofing off structural beams.
2. The fires, which were initiated by jet fuel but fed by building contents such as furniture and paper, weakened the building core.
3. The fires also weakened floors, which sagged and pulled inward on the perimeter columns.
4. The fire weakened perimeter columns bowed inward and buckled due to the floor pull-in forces, leading to collapse.

Along with this analysis, NIST released in April drafts of 15 reports from three projects of the investigation:

- Analysis of building and fire codes and practices
- Occupant behavior, egress and emergency communications
- Fire service technologies and guidelines

Recommendations for improvements to building and fire codes, standards and practices derived from these and the other five projects in the investigation will be released for public comment later this month, along with the draft of the final investigation report and drafts of 27 reports from the remaining five projects.

Additional Homeland Security Research

NIST, with its diverse research portfolio is also supporting the Nation's homeland security efforts in a number of ways that are not directly related to the attacks of 9/11.

Cybersecurity

Cybersecurity work at NIST plays a key role in addressing the urgent need to improve the cybersecurity posture of the Nation, and in particular that of the Federal Government. Some examples of recent and continuing NIST work in this field are:

- NIST is developing minimum security controls for *all* federal computer systems. This effort will have a huge impact on the Nation. These minimum security controls will be mandatory for federal agencies, although we expect they may become a *de facto* standard in the private sector as well.
- NIST continues to publish a wide range of cybersecurity standards and guidelines, which are available free on NIST's Web site. These are frequently used by the private sector, state and local governments, and even some foreign governments. Our contingency planning guideline alone was downloaded more than 400,000 times during the first year it was available.
- Homeland Security Presidential Directive #12, which mandates a common identification standard for all federal employees and contractors, requires NIST to develop a series of standards leading to reliable and secure "smart cards." NIST computer security specialists worked closely with other federal agencies—including the Office of Management and Budget, the Office of Science and Technology Policy, and the Departments of Defense, State, Justice, and Homeland Security—as well as private industry, to develop Federal Information Processing Standard 201, Personal Identity Verification of Federal Employees and Contractors.
- NIST is supporting the Small Business Administration in security outreach activities to small businesses.
- NIST is developing cryptographic standards for "constrained environments." An example is a "smart card" with limited memory and little or no computing power.
- NIST is beginning work to develop security checklists for computer systems that control buildings and manufacturing processes.
- NIST is developing the National Vulnerability Database, a comprehensive information technology database and search engine that integrates all publicly available U.S. Government vulnerability resources and provides links to industry resources.
- NIST is working to develop metrics for the effectiveness of software assurance tools, and assessing current methods and tools in order to identify deficiencies which can lead to software product failures and vulnerabilities.
- NIST continues to develop security guidelines/best practices on risk assessment, media destruction and sanitization, desktop IT security scenarios, and malware mitigation measures.

Additionally, NIST's Hollings Manufacturing Extension Partnership is beginning its outreach activities to small and medium sized manufacturers by providing them guidance with vulnerability assessments, business continuity, and supply chain implications.

Biometrics

As part of its fulfillment of the Patriot Act, NIST conducted the Fingerprint Vendor Technology Evaluation in 2003. The 18 competing companies used 34 different fingerprint matching systems. The evaluation, which was based on fingerprint data from a variety of U.S. and State Government sources, tested performance accuracy for various numbers and types of fingerprints.

The evaluation demonstrated the significance of fingerprint quality as well as the number of fingers used. (The matching accuracy using four fingers was better than the accuracy using only two fingers, which in turn was better than single-finger matching.) The test also showed that the most accurate fingerprint systems perform better than the most accurate facial recognition systems, even when using only a single fingerprint.

NIST's key Patriot Act recommendations included in the report to Congress titled "Use of Technology Standards and Interoperable Databases with Machine-Readable, Tamper-Resistant Travel Documents" dated February 2003:

1. For verification ("one-to-one matching" to establish that the person is who he/she claims to be), NIST recommends one face image and two index fingerprints.

2. For identification ("one-to-many matching" to find the identity of a person in a large database), NIST recommends ten slap fingerprint images for enrollment and checking of large databases. Face images are not recommended.

The Consolidated Appropriations Act, 2005, provided an increase of $2.0 million to NIST's biometric program. This new funding will allow NIST to begin testing the accuracy of multimodal systems, develop guidelines for testing fingerprint segmentation methods, and determining the influence of multiple images on the accuracy of facial biometrics.

Radiation detectors

NIST, in cooperation with the American National Standards Institute (ANSI), has an extensive program to develop and support standards for the radiation detectors used by first responders and for other homeland security applications. The standards will help first responders and government agencies make better use of existing equipment and acquire the right equipment for emergency response, and they will encourage manufacturers to better design instruments and represent their specifications to agency and responder buyers.

This program includes:

- Leadership in the development of the four ANSI standards that are currently released. These standards cover electronic personal alarming detectors (called "pagers"), personal radiation dosimeters, portable instruments, radionuclide identifiers (specialized devices that can identify specific radioactive materials), and portal monitors.
- Ongoing development of newer standards, such as for portal monitors with radionuclide identification.
- Leadership in the development of test and evaluation protocols for determining whether such radiation detectors meet the technical requirements of the new ANSI standards.

As an example of the application of the new standards, NIST recently tested 31 commercial detectors, including hand-held survey meters, pagers, and radionuclide identifiers. Federal, state, and local agencies are using such instruments as part of homeland security-related efforts to detect and identify radioactive materials. The tests determined that portable radiation detectors generally perform well against the new consensus standards but provided inaccurate readings for certain types of radiation. Researchers compared the device readings to NIST measurements for different radiations levels. The majority of the detectors agreed with NIST-measured values but some detectors tested had a large discrepancy in readings for the lowest-energy X-rays, and were much larger than those stated in manufacturers' specifications.

Other examples of NIST work related on radiation detectors include the following:

- Technical guidance for emergency responders.
- Development of a test bed for evaluating hand-held radiological detectors and truck portal monitors.
- Development of NIST-traceable test sources for gamma rays and neutrons used in calibrations of detectors.
- Development of methods, testing materials, standard reference materials, and measurement validations for radiological clean-up and mitigation.

Public Safety Communications Interoperability

NIST's Office of Law Enforcement Standards (OLES) is the common technical thread that is working to facilitate local, state, and federal communications interoperability efforts through the consensus standards process. Funded through SAFECOM, a program of DHS's Science and Technology Directorate's Office for Interoperability and Compatability, the Department of Justice's Community Oriented Policing Service, and the Advanced Generation of Interoperability for Law Enforcement (AGILE) program, OLES has been employing a structured approach for confronting interoperability standardization issues. This standardization strategy is centered on the development of an architectural framework that satisfies the real-world requirements of public safety responders. The framework defines the overall structured approach for facilitating interoperability. Functional Standards (in the form of Interface Specifications) then define the details of the structure, and indicate how the architecture (and its components) will operate. Although progress has been slow in the development of these standards, significant progress has been

achieved within the last year. OLES helped to complete the Public Safety Statement of Requirements for Wireless Communications and Interoperability on behalf of SAFECOM in March 2004. This is the first comprehensive, practitioner-accepted, record of the telecommunication needs of the public safety community within and across local, state, federal, and tribal boundaries.

Additionally, OLES on behalf of DHS SAFECOM, produced a draft of an architectural framework which is in essence a map that shows a network of networks and a system of systems approach which will be employed by public safety in the future. In response to Congress' call for immediate standards for communications interoperability, NIST, along with DHS and DOJ, have developed a partnership with public safety leadership to either significantly accelerate the current P25 standards development or develop interim communications standards in the absence of P25 standards. Additionally, Congress requested that SAFECOM produce a report on the plan for accelerating the development of national voluntary consensus standards for public safety interoperable communications. It is expected that because of the recent efforts by NIST and its partners, key interoperability standards will be published by the end of 2005, and products employing these standards would be available by the end of 2006.

Operations in Collapsed Buildings

In 2001, search-and-rescue robots that had been tested on a special NIST course penetrated areas too small and too hazardous for emergency responders to locate remains of several victims at the World Trade Center site. At that time, NIST already had expertise with collapsed buildings, including setting up competitions designed to accelerate the development and testing of urban search-and-rescue robots. Last year, NIST organized competitions in New Orleans, San Jose, and Lisbon, Portugal. More broadly, NIST has launched a DHS-funded multi-year program to develop comprehensive standards and performance metrics for urban search-and-rescue robots.

Collapsed buildings also present a significant problem in terms of radio communications. First responders who rely on radio communications often lose signals in shielded or complex environments such as in steel and reinforced concrete high-rise structures, and in the basements or elevator shafts of buildings. It also is very difficult to detect radio signals through the dense rubble of a building that has collapsed as a result of natural disasters or terrorist attacks. To simulate disaster environments, NIST is using real-world "laboratories"—buildings that are scheduled to be imploded as part of construction and recycling projects—such as the old Washington Convention Center and Veterans Stadium in Philadelphia. After the implosion, NIST researchers studied various schemes for detecting signals by searching with directional antennas and by connecting detectors to metal debris found within the rubble of the building. A technical report on these experiments will be published this summer.

Forensic Analysis of Magnetic Audio Tapes

NIST recently developed a real-time magnetic imaging system that enables crime investigators to "see" signs of tampering in audio tapes, such as erasing and overdubbing. The new system, which permits faster screening and more accurate audiotape analysis than previously possible, was recently delivered to the Federal Bureau of Investigation (FBI) Forensic Audio Analysis, which receives hundreds of audiotapes annually for analysis. Representing evidence from crimes such as terrorism, homicide and fraud, these tapes come from a wide variety of devices, including answering machines, cassette recorders and digital audiotape recorders. The benefits of the NIST system are its speed in correlating sounds with magnetic marks on tape, and the fact that it makes an image without damaging the tape.

Detection of Explosives and Toxic Chemicals

The cost and size of devices for detecting toxic airborne chemicals largely limits them to specialized equipment designed for use by the military or by first responders to chemical spills. In the event of an attack involving toxic chemical agents—such as the sarin gas attack in a Tokyo subway station—such portable detectors typically would not arrive on the scene until after victims had been harmed.

NIST is conducting research on a class of microsensors that has the potential to serve as a cost-effective early warning system for toxic gases and may also be applicable to the detection of vapors from explosive materials. The NIST devices use an array of microscopic hotplates coated with a film that is sensitive to ambient chemicals. A key advantage of this technology is that various types of films can be combined with multiple types of temperature cycles. An array of hotplates can thus produce a "signature" that can be matched against a library of chemical signatures to identify both the type and concentration of the toxic gas. Another advantage is

that the microsensors can be produced inexpensively with electronic processing circuits built in. Preliminary testing at the Army's Edgewood Arsenal has confirmed that 1-part-per-million sensitivity is feasible with actual chemical warfare agents.

Standards Development Organizations

Besides the research done in our laboratories, NIST works with private sector Standards Development Organizations (SDO's) on the implementation of homeland security standards.

- NIST assisted the DHS Science and Technology Directorate, Standards Portfolio in developing and implementing a formal procedure for the adoption of standards.
- NIST is assisting DHS in the coordination of public and private resources for the development of technical standards that support homeland security. The primary focus of this coordination is the American National Standards Institute's Homeland Security Standards Panel, which is co-chaired by Mary Saunders of the NIST Standards Services Division.
- NIST recently leveraged its technical expertise in ion mobility spectrometry (IMS) to establish minimum performance requirements and an associated test method for detectors of trace explosives based on IMS. Although some first responders already use IMS trace detection equipment, a documentary standard was needed to address the wide variety of possible future uses. The standard was developed with input from six detector manufacturers, state and local government agencies, federal agencies such as the U.S. Coast Guard, the Bureau of Alcohol, Tobacco, Firearms and Explosives and the Transportation Security Administration, and security professionals such as the U.S. Secret Service.

Conclusion

As the Committee can see by the few examples I have cited, NIST has a very diverse portfolio of research activities supporting our Nation's homeland security effort. After the terrorist attacks of 9/11, NIST responded to the research challenges it faced. NIST's long history of research supporting homeland and national security is helping to enable the development and effective deployment of new technologies to protect the homeland. Once again thank you for inviting me to testify about NIST's activities and I would be happy to answer any questions you may have.

Senator DEMINT. We'll save our questions until we finish the panel.

Admiral.

STATEMENT OF VICE ADMIRAL CONRAD C. LAUTENBACHER, JR., U.S. NAVY (RETIRED), UNDER SECRETARY OF COMMERCE FOR OCEANS AND ATMOSPHERE; ADMINISTRATOR, NOAA

Admiral LAUTENBACHER. Thank you, Mr. Chairman, Senator Nelson, and staff members. It's a great pleasure and privilege to be able to testify today before you about NOAA's contributions to the national homeland security mission.

NOAA is a science-based agency, but provides service to our country 24-by-7. That 24-by-7 information underpins 30 percent of our GDP, so it's extremely important to our economic security, as well as our physical security. We work hard to ensure that we meet those demands that the economy and society places on us.

We have a list of capabilities, of over 50, that are vital to the security of this Nation. With the time limits that I have, I will mention a few, and there are others that are listed in our—in my formal testimony, for the record.

In addition, because of the importance of this information to the economy, we work very hard at our internal security. We need to ensure that the information provided for the—running the economy

is available 24-by-7, and we have spent the last several years ensuring the continuity of that data to all segments of society.

The first topic I'd like to mention is alerts and public warnings. The National Weather Service branch of NOAA has something called the NOAA Weather Radio. That is the only system in our Nation that goes directly into every home, every school, every fire station, and all of the press. It provides those alerts and warnings that you see across your television that tells you you're going to have a severe thunderstorm or there's going to be lightning or hail or a tornado or a hurricane, flooding. That system is alarmed, and is—now covers 98 percent of our country.

We have signed, this last year, a memorandum of agreement with the Department of Homeland Security to make that part of the national warning system, so that, as of today, all types of hazards that can affect our communities are inserted into NOAA Weather Radio. So, if you have a NOAA Weather Radio, you'll be warned of chemical spills, of any biohazards, of significant local events. It goes into all of our weather forecast offices. And any event, whether it's natural or manmade or of a terrorist nature, will be available for alerting the public on NOAA Weather Radio, All Hazards.

We also have an agreement with the Department of Education and DHS to provide the NOAA Weather Radio to public schools in selected areas. We're looking to make sure that eventually all schools in the United States have these radios available for building emergency plans.

Let me move on to forecasts and dispersion modeling. One of the more interesting issues that we have for natural disasters, as well as manmade disasters, is what happens when chemicals or dangerous substances get into the atmosphere. What types of forecasts do we need to ensure the safety and security of our Nation? We have built numerical models of the atmosphere, which is what we're strong into, as our charge is for weather information. It's used for flight planning, ship routing, energy distribution, as well as many other activities. Our air-dispersion models help emergency planners detect and track chemical, biological, and radiological hazards, as well.

First-responders can use laptop applications that we've developed to be able to tell where a plume, a hazardous plume, will be going, and track it, and use it to be able to develop evacuations and mitigation procedures for our towns and cities across the Nation. We are now conducting a pilot program to integrate realtime weather models with hazardous-plume predictions, so it can be simultaneously provided to all forecast offices and all emergency managers across the country.

We have a special operation going in here, in Washington. We call it DCNet. It is a system for taking data in the urban canyons of our major city here, of Washington, and building models that will allow us to provide the micro-level information for accurate evacuation and homeland security in Washington. During the 2005 Presidential inauguration, NOAA and DHS closely monitored this information, and it was instantaneously available for anything that might need to be covered during the inauguration procedures.

We have conducted major atmospheric dispersion field studies with other federal agencies in a number of cities across the country. We also are doing the same kinds of modeling for fluid mechanical models in the ocean and our coasts, which are very important in harbor areas and for safety of seafood and our water-quality issues for bathers.

Let me move on to remote sensing. We have started to evaluate a Predator B aircraft to look at ways to obtain continuous data for oceanic and atmospheric research, for nautical charting, to tell what's going on, as well as fisheries assessment and enforcement. This is dual-use technology that's of value both to security, as well as to environmental monitoring. We believe that the same systems that we can use for national security are valuable, as well, for environmental monitoring, and we are working together with DHS and the services to further explore the value of remote sensing devices.

The Integrated Ocean Observing System and something called Maritime Domain Awareness. We have a program to develop an Integrated Ocean Observing System. We believe, as we did with the—I mentioned the Predator—use of the Predator—that this is a system of dual usage again. It includes buoys in the water, underwater listening devices, as well as satellite passes, aviation monitoring of the atmosphere around our coasts. That system can pick up a great deal of information for what people in Maritime Domain Awareness call a "common operating picture" of understanding what's going on in our coasts.

We also have built into our capability for surveying our harbors and our coasts. Remember, NOAA is the agency that produces all the charts for bringing the ships—our $1 trillion maritime industry depends on that information. NOAA performed the baseline assessments after 9/11 to ensure that—for our—half of the country—Navy did half, Coast Guard did part, and we did half—to ensure there were no mines or other types of potential hazards in the water to our ports. We are now building a way to do that much more rapidly and safely by the use of autonomous underwater vehicles and autonomous surface vehicles to enhance the speed of survey and ensuring that we understand exactly what's in our port, in our channels, in our harbors as our ships come and go.

We have implemented something called a National Vessel Monitoring System that goes with—it's in concert with an ocean observing system. This was designed to keep track of fishing vessels, the fishing fleet, the civilian fishing fleet that's out there, but it is, in fact, a way to track all sorts of things that are going on. The system, itself, uses satellite communications. A global positioning system reports back to a central command center. And it allows us to keep track of where fishing vessels are, or are not, and what they're doing, so that we can maintain integrity of our fishing rules and regulations. It's also a system that allows us to tell what's going on in any case in those waters, because our fishing fleet goes from the coast of Maine to the Bering Sea in Alaska, and provides realtime data for the Coast Guard to work on for enforcement.

We've also installed radio transmitters on buoys that we have in the near coast that directly connects the Coast Guard to their automatic information system, so that these buoys act as transponders, so that the Coast Guard can gain a picture, operating picture, fur-

ther out into the EEZ and maintain our security defenses farther away from our coasts.

And one last point is response. We have a wide range of response capabilities. And, for instance, after the hurricanes that we had last season, we deployed something we call Navigation Response Teams. These are quick-reaction teams that can go out and open ports and harbors from changes that might have occurred, or at least survey and provide the proper information to our ships and maritime industry that uses the coasts. We can do this quickly. We helped reopen the Gulf Coast ports and their East Coast ports within several days after the hurricanes passed, this last year.

With that, I wish to conclude my testimony and, again, thank the Committee for their support of NOAA and our programs. And I stand by to answer your questions.

Thank you.

[The prepared statement of Admiral Lautenbacher follows:]

PREPARED STATEMENT OF VICE ADMIRAL CONRAD LAUTENBACHER, JR., U.S. NAVY (RETIRED), UNDER SECRETARY OF COMMERCE FOR OCEANS AND ATMOSPHERE; ADMINISTRATOR, NOAA

Mr. Chairman and Members of the Committee, I am Conrad Lautenbacher, Administrator of the National Oceanic and Atmospheric Administration (NOAA) of the Department of Commerce. Thank you for the opportunity to appear before you today to discuss NOAA's contributions to the national homeland security mission. I am proud to lead a team of men and women whose daily activities advance our homeland security and strongly believe NOAA's contribution is of tremendous benefit to the United States.

Although NOAA is best known as a premier science and service agency whose mission is to describe and predict changes in the Earth's environment, NOAA's expertise and services can be applied to many other areas, including national security. NOAA's responsibilities for the environment, safety, and commerce of this Nation span the oceans, coasts, and atmosphere. The capabilities that are part of NOAA's standard daily operations often are vital during times of emergency.

NOAA has established a Homeland Security Program Office to serve as the principle point of contact for NOAA regarding homeland security programs across the entire Agency. This office coordinates homeland security programs, ensures continuity of operations, and prepares for continued delivery of services during emergencies.

NOAA Homeland Security Products and Services

After reviewing the full range of its capabilities, NOAA has identified more than 50 capabilities that could immediately advance the Nation's homeland security efforts. NOAA leverages these already existing programs, technologies, and expertise in new and innovative ways to assist the U.S. Department of Homeland Security (DHS) and has actively partnered with many other agencies (state, local and federal) to address homeland security issues. I will review a few of our contributions.

Alerts and Public Warnings

The National Weather Service broadcasts warnings, watches, forecasts, and other hazard information regarding tornados, flash floods, and other potential life-threatening situations 24 hours a day, 7 days a week, via a nationwide network of radio stations. NOAA coordinates these warnings and advisories with the Federal Emergency Management Agency. Working with the Federal Communications Commission's Emergency Alert System, the NOAA Weather Radio was expanded to serve as an "all hazards" radio network. In June 2004 this system's capabilities were further expanded to allow DHS to send critical all-hazards alerts and warnings directly through the NOAA All-Hazards Network. The NOAA All-Hazards Network consists of over 950 radio transmitters located throughout the United States and U.S. possessions and territories, allowing the transmission of weather watches, warnings, and advisories as well as non-meteorological civil emergency messages to over 97 percent of the population. NOAA Weather Radio/All-Hazards now provides alerts for both natural (severe storms, hurricanes, tornadoes, earthquakes, and volcanic activity) and environmental (chemical spills and bio-hazardous releases) events. The all-

hazards capability is being implemented through agreements with local, state, and federal emergency managers and first responders. NOAA is presently developing a capability to reduce the time it takes for an emergency manager to input a hazard warning into NOAA Weather Radio/All-Hazards. This will reduce the input time from 7 minutes to less than 2 minutes. This capability will allow emergency managers direct access to the Emergency Alert System via NOAA Weather Radio/All-Hazards, and is expected to be fully operational in Fiscal Year 2006.

To complement this new homeland security messaging capability, we will work with DHS and the U.S. Department of Education to provide NOAA Weather/All-Hazard Radios to public schools in select top urban areas and two rural states during National Preparedness Month in September 2005.

In addition to the traditional weather radio that many are familiar with, NOAA Weather Radio/All-Hazards receivers can be integrated into devices to turn on alarms, lights, bed shakers, and other equipment especially useful for the hearing impaired community and those with special needs. RCA/Thomson has developed a new line of televisions, called *AlertGuard,* which integrate a NOAA Weather Radio/All-Hazards receiver into television sets.

DHS is leading the effort to develop a government-wide plan for the Integrated Public Alert and Warning System (IPAWS). Public warnings save lives by informing, reducing fear, and assisting emergency managers. There are many warning systems in place across the country, and while each of these systems can reach the public directly, no one system reaches everyone. NOAA information dissemination systems, including NOAA Weather/All-Hazards Radio, as well as information posted directly on the Internet and supplied to radio and television stations, will be a part of a larger integrated national emergency warning system.

In response to the 2004 Indian Ocean Tsunami, NOAA is committed to expand the U.S. Tsunami Warning Program to protect U.S. lives and property along all coasts (Pacific, Atlantic, Gulf of Mexico, and Caribbean). In order to continue the Administration's commitment to strengthen the Tsunami Warning Program and mitigate potential impacts from a similar tsunami event in the U.S., NOAA will build on its existing foundation of sensors. NOAA will accomplish this by deploying 39 additional Deep-ocean Assessment and Reporting of Tsunamis (DART) buoy systems strategically sited in the Pacific, Atlantic, and Caribbean basins. Data from DART buoys will aid U.S. tsunami forecasters in providing detailed tsunami forecasts. The enhanced program will also aid tsunami hazard mitigation actions including inundation flood mapping, evacuation mapping, and community-based public education, awareness, and preparedness. NOAA will operate and maintain the expanded DART system, new sea-level monitoring stations, and the upgraded local seismic networks from the 24/7 West Coast/Alaska Tsunami Warning and Pacific Tsunami Warning Centers.

Forecasts and Dispersion Modeling

NOAA forecasts include the creation of numerical models of the atmosphere used for flight planning, ship routing, and energy distribution. These numerical forecasts are used to model the dispersion of airborne hazardous materials such as volcanic ash, industrial chemical releases, and radiological accidents.

NOAA's operational air dispersion models help emergency planners detect and track chemical, biological, and radiological hazards in the atmosphere. When an event occurs, first responders can use laptop applications for hazardous material (hazmat) modeling of industrial chemicals on scene and NOAA regional models accessible through the local Weather Forecast Office.

One of NOAA's major contributions in emergency preparation and response is the software program CAMEO (Computer-Aided Management of Emergency Operations). Jointly designed with the Environmental Protection Agency (EPA), CAMEO is widely used by firefighters and serves as a primary tool in preparing for and responding to chemical incidents. An updated version of CAMEO was released in March 2004. It contains a chemical database of over 6,000 hazardous chemicals with chemical-specific information on fire and explosive hazards, health hazards, firefighting techniques, cleanup procedures, and protective clothing. NOAA and EPA are expanding the CAMEO chemical database to include information on weapons of mass destruction. The ALOHA (Areal Locations of Hazardous Atmospheres) atmospheric dispersion model is a computer program used in conjunction with the CAMEO to predict how a hazardous gas cloud might disperse in the atmosphere after a chemical release based on the physical characteristics of the released chemical and atmospheric conditions. The program can display the location of facilities storing hazardous materials as well as buildings of high concern, such as hospitals and schools. ALOHA is being expanded to predict the impact of fires and explosions.

NOAA's Air Resources Laboratory and Hazmat program are in the early stages of developing a Chemical Threat Analysis Planner to improve our ability to evaluate potential threats from hazardous material releases using the HYSPLIT dispersion model in conjunction with the CAMEO database. Additional future developments will fully integrate CAMEO/ALOHA with national-level emergency information management systems including the Interagency Modeling and Atmospheric Assessment Center (IMAAC).

Under the National Response Plan, the IMAAC is the single source of federal hazards prediction information during the response and recovery phase of Incidents of National Significance for atmospheric transport and dispersion of hazardous releases. NOAA is working with DHS to develop procedures to organize and coordinate federal emergency response through this Center, providing decision-makers with custom products and a single point of contact for all-hazards dispersion modeling predictions and assessments. NOAA and DHS are working to integrate CAMEO/ALOHA and HYSPLIT into the suite of IMAAC.

NOAA is conducting a pilot program to integrate real-time weather models and hazardous plume predictions to provide DHS with the ability to identify specific areas to issue targeted homeland security alerts and warnings using reverse 911 technologies. In this pilot program, called Geo-Targeted Alerting System (GTAS), forecasters at the NOAA Weather Forecast Office located in Sterling, Virginia will provide DHS with toxic plume dispersion information. Given the dispersion forecast of a toxic cloud, DHS officials will be able to select several "targeted" warning areas to provide specific public safety information for each area using applications developed by NOAA's Forecast Systems Laboratory.

Monitoring stations have been installed in Washington, DC, to support one of the first dispersion forecasting systems specifically designed for urban areas. These stations, known as DCNet, collect and analyze standard meteorological data (as well as wind speed, direction, and turbulence data) at frequent intervals to help define downwind areas of potential high risk. In doing so, DCNet allows users to gain a better understanding of how hazardous trace gases and particles are dispersed in urban areas. During the 2005 Presidential Inauguration, NOAA and DHS closely monitored this information, which was then immediately available for dispersion model runs in the event of an incident.

NOAA has provided much of the Nation's atmospheric tracer expertise since the 1950s. The center of excellence resides within the Air Resources Laboratory (ARL) at Idaho Falls, Idaho where the ARL Field Research Division is located. In recent years, the ARL team has conducted field studies in Salt Lake City and Oklahoma City, to support the major atmospheric dispersion field studies conducted under the sponsorship of a number of agencies, led by DOE, DHS, and DoD. In the last two years, studies have been conducted in New York City and in Washington, DC Building upon them, the ARL team is about to engage in a new round of fieldwork, again focusing on New York City and Washington, DC The DC work will be concentrating on the Pentagon and its surroundings (sponsored by DoD), the New York project will focus on midtown Manhattan (sponsored by DHS).

The New York City study also involves two other ARL groups, located at Oak Ridge, Tennessee, and Research Triangle Park, North Carolina. The Oak Ridge group is leading the design of a surface meteorological network to help guide the development of local dispersion forecasting (an extension of the DCNet experience in Washington DC), sponsored by DHS. The Research Triangle Park group is conducting Comprehensive Fluid Modeling studies and wind tunnel physical modeling investigations, both sponsored by EPA.

Remote Sensing

NOAA continues to use Light Detection and Ranging or Lidar, a technique similar to Radar, using lasers for mapping terrain elevation features and high quality aerial photography to collect data in support of homeland security surveys. Specifically, these technologies can be used to protect critical infrastructure, aid in disaster response and recovery efforts, verify dispersion modeling and provide support for special security events.

Currently NOAA is evaluating a remotely operated aircraft (ROA) for future science and operational requirements within the Agency related to oceanic and atmospheric research, climate research, marine sanctuary mapping and enforcement, nautical charting, and fisheries assessment and enforcement. The platform NOAA is using is a variant of the General Atomics Aeronautical System's Predator B, a high-altitude, long-endurance ROA that has successfully supported Operation Iraqi Freedom. NOAA worked with the U.S. Coast Guard (USCG) to ensure the common operating areas and requirements both agencies shared were incorporated into the ongoing planning and operational flights. This interaction has resulted in both agen-

cies leveraging their expertise and resources to carefully evaluate the potential benefits ROAs may provide for both agencies' operational requirements.

NOAA demonstrated the support ROAs could provide through streaming video from a ROA operating off the coast of California and provided to the Homeland Security Operations Center (HSOC) in Washington, DC While only an initial demonstration, NOAA fed live video imagery over a satellite Internet connection to NOAA's Boulder, Colorado facility and then directly to the HSOC, showing the potential these platforms can provide for both incident and situational management.

Integrated Ocean Observing System and Maritime Domain Awareness

NOAA has assisted the U.S. Coast Guard and the U.S. Navy in implementing the Maritime Domain Awareness (MDA) Program, to develop a national strategy to ensure interagency coordination of homeland security policy and requirements in marine areas. MDA includes anything associated with the global and coastal maritime environment that could adversely impact the security, safety, economy, or environment of the United States. This knowledge is used both operationally in the planning and execution of homeland security missions, and by researchers supporting the development of new homeland security capabilities.

To meet a wide range of societal needs, our country has embarked on a program to develop an Integrated Ocean Observing System (IOOS). IOOS is the integration of existing and planned observing systems to meet common research and operational agency needs in the following areas:

- Detecting and forecasting oceanic components of climate variability
- Facilitating safe and efficient marine operations
- Ensuring national and homeland security
- Managing resources for sustainable use
- Preserving and restoring healthy marine ecosystems
- Mitigating natural hazards
- Ensuring public health

The backbone network of coastal observations can be of dual use in supporting both civil and homeland security objectives. IOOS will enhance national and homeland security in our coastal waters and ports through improving Maritime Domain Awareness and through improved observations and predictions of the ocean environments in which homeland security operations take place.

On September 24, 2004, Admiral James Loy, Deputy Secretary of the Department of Homeland Security, and Paul McHale, Assistant Secretary of Defense for Homeland Defense, convened the first meeting of the MDA Senior Steering Group. Admiral Loy's opening comments addressed the urgent nature of the job at hand, the need to draw on the resources of supporting agencies, and the move beyond study to deployable capabilities. He made reference to the roll out of the U.S. Commission on Ocean Policy Report and noted the reference to an IOOS. He remarked, "If that's not Maritime Domain Awareness, I don't know what is." Admiral Loy recognizes interagency capabilities can be leveraged for a proactive, forward deployed maritime defense.

As a part of this overall program, USCG and NOAA are developing marine two-way communications systems on NOAA data buoys to relay Automated Identification Signals (AIS) through satellite links to the USCG for vessel tracking. AIS is a shipboard system that broadcasts vessel data such as name, course, speed, and call sign to other AIS vessels and stations for collision avoidance at sea. AIS previously was only carried by VHF signal and therefore had a limited range. The installation of satellite relays on NOAA data buoys will expand the USCG capability to monitor and track vessels approaching U.S. territorial waters well beyond the line of site limit for VHF.

NOAA officers, ships, and Navigation Response Teams surveyed the shipping channels of over 30 strategic commercial ports in 2002 to collect high-resolution imagery requested by the U.S. Navy. These surveys provide the baseline data of pre-existing objects so mine countermeasure assets can be utilized more effectively to determine if a mine has been placed on the sea floor. Using hydrographic survey techniques, NOAA is working with the Navy and USCG to improve our mine detection capabilities in ports. NOAA and the Defense Counter Terrorism Technology Support Office are developing an Underwater Domain Awareness capability for ports, harbors and inland waterways. This partnership will support USCG with rapid response capabilities to better detect and classify underwater threats and enhance their ability to ensure safe and secure waterways critical for the transit of military and commercial vessels. In the next phase of this partnership, we will be focusing on Autonomous Underwater Vehicles and Autonomous Surface Vehicles to improve the speed and flexibility of response and protect survey personnel by pro-

viding greater stand-off during higher risk surveys. Remotely Operated Vehicles will be used for underwater surveys to localize and identify detected anomalous objects.

NOAA has implemented a national Vessel Monitoring System (VMS) program that provides infrastructure, economies of scale and coordination across National Marine Fisheries Service (NOAA Fisheries) regions and offices. The expanded use of VMS provides one of the strongest potential solutions to supplement traditional enforcement activities. This system provides near-real time fishing vessel monitoring, control and surveillance throughout the U.S. Exclusive Economic Zone (EEZ), Pacific Ocean, and Atlantic Ocean. It also provides critical, life saving, information to the Coast Guard in support of their response in Search and Rescue (SAR) missions. VMS uses the Global Positioning System (GPS), satellite communications, and a secure network to monitor fishing vessel compliance. However, this evolving capability could be used for marine enforcement and homeland security requirements since it can identify and track vessels, as well as provide information for a maritime domain common operating picture. An expanded VMS could encompass the entire nation and relay near real-time data to the USCG for enforcement and homeland security purposes. VMS, if fully developed, could provide extensive observational coverage of our Nation's EEZ.

Response

NOAA has a wide range of capabilities in its day-to-day operations that can be used to prepare for catastrophic events. For example, surveying and charting are NOAA activities mandated by Congress. After Hurricanes Frances, Ivan, and Jeanne in 2004, NOAA deployed Navigation Response Teams (NRT) for emergency surveying to quickly reopen Gulf Coast ports, demonstrating the economic, safety, and MDA benefits of rapidly resurveying ports and harbors. The NRTs conduct hazardous obstruction surveys along our coasts to update NOAA nautical charts. They also serve as research platforms testing equipment and developing new ways to effectively and efficiently survey navigable waterways.

NOAA's hydrographic survey vessels are occasionally called upon by the USCG to acquire detailed side scan and multi-beam survey images for search and recovery, as was the case following TWA 800 and the EgyptAir crashes. In 2004, NOAA assisted a USCG investigation by locating and obtaining high-resolution imagery of the Bow Mariner, an ethanol tanker that exploded and sank off the Virginia Capes. This capability is another weapon in the defense against maritime threats, as it allows ports to be re-opened quickly and helps the USCG to design temporary lanes and detours based on depth data. We rapidly disseminate chart updates and critical chart corrections to the mariner, and we can create and distribute temporary charts, overlays and data sets as needed by primary responders like the Coast Guard.

NOAA's Hazmat Scientific Support Coordinators (SSC) work in USCG offices, planning for emergencies and developing port-specific incident response plans. These plans highlight specific problems, such as those faced by chemical facilities in port areas. NOAA also develops computer programs used for both incident-specific planning and routine training. This preparedness training is vital because, when an event occurs, first responders need to have a range of tools they are familiar with and can apply. NOAA SSCs are then able to go on-site during emergencies to bring all of NOAA's support resources to the table.

When discussing NOAA's response capabilities, it would be remiss of me not to mention the NOAA Corps, one of the Nation's seven Uniformed Services. These officers primarily have science and engineering backgrounds, stand ready to support the Coast Guard, Department of Defense (DoD), and any other federal agency that requires assistance in protecting the Nation's security. At the request of the DoD, NOAA has provided a summary of its capabilities, ships and aircraft that could be used in a national emergency. NOAA's Office of Marine and Aviation Operations (OMAO) operates a diverse fleet of research and hydrographic coastal and ocean-going vessels ranging in length from 90 to 274 feet, as well as helicopters and airplanes. OMAO abilities to assist port security efforts include assisting the USCG boarding or inspection parties, supporting port/harbor security, providing sophisticated airborne chemical detection support, conducting hydrographic surveying/sea floor mapping and Geographic Information System (GIS) development, conducting state-of-the-art sonar operations, and providing additional hurricane reconnaissance if U.S. Air Force assets are reassigned.

Space Based Assets

The National Environmental Satellite, Data and Information Service provides real and near-real time satellite imagery through geostationary and polar-orbiting environmental satellites. NOAA acquires and manages the Nation's operational environmental satellites and provides data and information services. Information and obser-

vations from NOAA's orbital assets are used in weather forecasting, aviation and marine operations, agricultural applications, on-scene weather support for incidents, sea surface temperature measurements for the fishing industry, and volcanic ash detection and tracking. However, they can also be used for security purposes.

NOAA satellite imagery detected the smoke plume emanating from New York City following the events of September 11, 2001. Using the NOAA Geostationary Operational Environmental Satellite (GOES), we were able to detect the development and dispersion of that smoke plume. Monitoring the extent and the direction of the plume helped to define areas of potential health risk from hazardous particulates in the plume. NOAA provided emergency satellite frequencies for the health community to relay measurements from air quality sensors at the World Trade Center site.

NOAA licenses and enforces compliance with federal regulations for operating a commercial or private earth observing satellite. Enforcement of the regulations applying to shutter control or restriction of data distribution is essential to ensure national security. NOAA enforces stated limitations of the Kyl-Bingaman Act prohibiting U.S. commercial satellite companies from collecting and releasing imagery of specified areas.

NOAA's orbital assets also support international search and rescue efforts. The satellites carry transponders for search and rescue beacon signals from downed air and marine craft, and from personal locator beacons. NOAA's search and rescue function is part of an international program for detection of distress signals from aircraft, vessels, and personal locator beacons. This global program relies on, and supports, other nations in the collection and processing of search and rescue signals.

Orbital imagery and data are also used for detecting and monitoring of wild fires. Tracking smoke plumes is an important part of the response to a fire event as it may create health problems and visibility issues. Wind and other weather data from the satellites, when paired with the smoke plume detection help us understand the extent of the fire, and support other agencies with firefighting responsibilities. Most frequently, when NOAA satellites detect a plume it is the result of a volcanic eruption. The United States has a number of active volcanoes, notably Mt. Spurr in Alaska, and Mt. St. Helens in Washington, which are in heavy aviation corridors. Eruptive events create very real threats to the aviation industry.

Coordinating Homeland Security Programs

As I have outlined today, NOAA continues to form collaborative partnerships with state, local and federal entities charged with addressing homeland security issues. Through the Homeland Security Program Office, we provide support directly to DHS. NOAA staffs a desk at the Homeland Security Operations Center (HSOC) to provide operational communications, information and resource coordination supporting management of domestic Incidents of National Significance and National Special Security Events. The Homeland Security Program Office plays a vital coordination role as the NOAA point of entry into Homeland Security operations and is responsible for keeping NOAA executive management appropriately informed and engaged.

The Interagency Incident Management Group (IIMG) is a DHS led structure facilitating a comprehensive, integrated and coordinated approach to domestic incident management. The IIMG is collocated and supported by the HSOC staff. IIMG members provide decision-making support to the Secretary of Homeland Security and other national authorities during periods of elevated alert and national-level domestic incidents. Specifically, NOAA provides subject-matter experts supporting chemical, radiological, and nuclear weapons of mass destruction events and natural disasters.

Citizen Corps was launched by DHS "as a community based initiative to engage all citizens in homeland security and community safety and family preparedness through public education and outreach, training opportunities, and volunteer programs." In July 2003 a Statement of Affiliation between DHS and NOAA was signed by Undersecretary Michael Brown and me in order to establish a collaborative partnership raising public awareness about weather and environmental hazards as well as promoting actions for public safety.

NOAA Fisheries' Office for Law Enforcement is dedicated primarily to the enforcement of laws that protect and regulate our Nation's living marine resources and their natural habitat. NOAA Fisheries' special agents and enforcement officers enforce many federal statutes, as well as numerous treaties related to the conservation and protection of marine resources through the prosecution of both civil and criminal violations. Notwithstanding OLE's joint enforcement partnerships with 27 coastal state agencies, the U.S. Coast Guard continues to be OLE's strongest ally in enforcing marine resource laws and fishery management. The cooperative support

from the Coast Guard enables OLE agents and officers to actively respond to suspected violations that might otherwise be unattainable.

With increased emphasis on Homeland Security and inter-agency collaboration, OLE's expertise has also been applied to various task forces and maritime security initiatives nationwide including MDA, border operations and checkpoints, and dock patrols.

Conclusion

In NOAA's unique role as an information provider, we will continue to work closely with our partners to support the Nation with a wide range of services and products from hazardous material spill response capabilities to atmospheric and waterborne dispersion forecasting and support for communities and emergency responders. NOAA also is ready to provide NOAA's ships, aircraft, global observing systems, and professional law enforcement officers to serve the Nation when the need arises. Thank you for inviting me here today to talk about NOAA's homeland security programs.

Senator DEMINT. Thank you.

Dr. Bement?

STATEMENT OF DR. ARDEN L. BEMENT, JR., DIRECTOR, NATIONAL SCIENCE FOUNDATION

Dr. BEMENT. Good afternoon, Mr. Chairman, Ranking Member Nelson, and Subcommittee staff.

Thank you for the opportunity to present testimony on the National Science Foundation's role in advancing science-and-engineering's capability to enhance the Nation's homeland security.

My written testimony details a number of NSF programs that are central to creating knowledge that will have applications in homeland security. It also notes how NSF's research programs relate to threats and countermeasures identified in an April report released by the Office of Science and Technology Policy, entitled "Science and Technology: A Foundation for Homeland Security." I'll touch on a few topics from my written testimony, and will start with disaster response.

For more than three decades, NSF has supported quick-response disaster studies that dispatched scientists and engineers to the aftermath of crises ranging from natural phenomena to manmade. Researchers were in the field within days after both the terrorist attacks of September 11, 2001, and the recent South Asian tsunami, to gather critical data before it was lost to nature and reconstruction. This ephemeral information, including assessments of physical damage to built and natural environments and social responses, is critical to help emergency teams and local leaders better direct future rescue efforts, and is vital to understanding and preparing for future disasters.

Second, on detection of CBRNE materials, especially fissile materials, a critical capability needed to defend against nuclear proliferation and to prevent a nuclear or radiological weapon from entering the country is the ability to detect the presence of illicit fissile materials. To detect such contraband, new sentinel systems and detectors enabled by critical advances in the material sciences must be fielded at home and abroad. It is widely believed that nanotechnology will lead to the advances required to enable these systems.

As a lead agency of the National Nanotechnology Initiative, NSF restructured the program last year, in part to accelerate the realization of new nanostructured materials, and, therefore, hastened

developments to detect chemical, biological, radiological, nuclear, and explosive materials.

Next, to data mining. One subject of intense interest in the academic research community comes under the rubric of data mining. When large amounts of data are available, whether information from scientific equipment, health records, or e-mail traffic, it is important to be able to extract meaning from that information. Data-mining applications and computers, generally, have a difficult time understanding what the language and the message actually means. NSF-funded researchers are developing techniques to provide standardized "who did what to whom, when, and where" versions of messages written in English, Chinese, and Arabic. The underlying techniques have applicability in many areas beyond homeland security, such as financial and healthcare fraud detection.

Next, cybersecurity. In the area of cybersecurity, NSF will be establishing a new collaborative cybersecurity science and technology center this year at the University of California at Berkeley. This new cybersecurity center will investigate key issues of computer trustworthiness in an era of increasing attacks, at all levels, on computer systems and information-based technologies.

NSF-supported basic research in important areas as varied nanotechnology, linguistics, deception detection, genomics, microbiology, engineered systems, and sensor development is critical to develop the knowledge base that will protect us against existing and future threats.

But perhaps the most important investment NSF makes in the area of homeland security is the education of the Nation's future science and engineering workforce. Unfortunately, we now see warnings that America's advantage in scientific and engineering capital is eroding. The obvious alternative to importing S&E manpower to fill the gaps is to grow more of our own. We desperately need to broaden participation in science and engineering by both increasing the fraction of the general population of students in these fields, and by increasing participation by under-represented groups.

I am pleased to note that more than 20,000 minority students receive science and engineering bachelors degree each year from the institutions in the NSF alliances for minority participation. Merely doubling the fraction of these who continue on to the Ph.D. would be a major contribution to America's domestic S&E manpower.

Mr. Chairman, the National Science Foundation is committed to the advancement of studies that have direct impact on our Nation's homeland security. Our dedicated program staff understands the significance that science and engineering have on security. We work to ensure that capabilities at the frontiers of science and engineering today will keep pace with the advances and threats of tomorrow.

NSF works in collaboration with the Department of Homeland Security, the intelligence community, the Department of Defense, the Department of Energy, federal labs, and the private sector to ensure that this wealth of knowledge is effectively transferred into capabilities critical for advancement in many areas, including homeland security.

In an increasingly demanding and unpredictable security environment, NSF will continue to help shape a more prosperous and secure future for ourselves, our children, and future generations.

Mr. Chairman and Ranking Member Nelson, thank you, again, for this opportunity to testify on a topic of great importance, and I would be pleased to answer any questions you may have.

Thank you.

[The prepared statement of Dr. Bement follows:]

PREPARED STATEMENT OF DR. ARDEN L. BEMENT, JR., DIRECTOR, NATIONAL SCIENCE FOUNDATION

Good afternoon. Mr. Chairman, Ranking Member Nelson, and Members of the Subcommittee, thank you very much for the opportunity to present testimony on the National Science Foundation's role in advancing science and engineering's capability to enhance our Nation's homeland security.

As you know, when Congress established the National Science Foundation (NSF) in 1950, it gave the agency a broad mission: "to promote the progress of science; to advance the national health, prosperity, and welfare; and to secure the national defense . . ." As such, much of NSF's activity directly supports our Nation's ability to secure the homeland. NSF plays a critical role in underwriting fundamental research, education and infrastructure at colleges, universities and other institutions throughout the country. This effort produces future generations of world-class scientists and engineers who develop ideas and research tools that address the challenges we face today and those we will face in the future.

Research supported by NSF accounts for approximately 13 percent of federal support for basic research and approximately 40 percent of non-life-science basic research at U.S. academic institutions while representing less than 4 percent of the federal funding for R&D. This work, at the frontiers of knowledge, represents much of our Nation's most advanced capability in materials science research, sensors and the architecture of sensor networks, genomics, cyber-security, data mining, and understanding of human and social dynamics, among others. Much of this work has direct impact upon our Nation's present and future-generation homeland security systems and capability.

The April 2005 report from the Office of Science and Technology Policy (OSTP), *Science and Technology: A Foundation for Homeland Security,* identifies the following areas where our Nation's research communities will play vital roles: (1) Science and Technology For Defense Against Catastrophic Threats and (2) Science and Technology to Counter Terrorism. NSF has supported basic research in these two areas from the Foundation's origins and much of today's capabilities can trace their lineage back to NSF-sponsored fundamental work. Moreover, in response to emerging threats, NSF has increased support for several activities outlined as critical in the OSTP report. What I outline below are some of the activities sponsored by NSF that directly address the topics the OSTP report identifies as critical to advance our Nation's science and technology base for supporting homeland security.

The National Science Foundation Research Portfolio:

CBRNE

As a first example, the OSTP report identifies Radiological and Nuclear Countermeasures as a key component to countering the threat of weapons proliferation, and the 2002 National Strategy for Homeland Security states: "Our highest scientific priority must be preventing terrorist use of nuclear weapons." A critical component capability to defend against nuclear proliferation and inhibit border penetration by a nuclear or radiological weapon is the ability to detect the presence of illicit fissile material. To detect such contraband, new sentinel systems and detectors enabled by critical advances in material sciences must be fielded at home and abroad. It is widely believed among the scientific community that nanotechnology will lead the way to the advanced capability in material sciences required to enable these systems. As the lead agency of the National Nanotechnology Initiative (NNI), NSF directed the 2004 restructuring of the NNI in part to accelerate the realization of new nano-structured materials and therefore hasten developments to enhance our ability to detect Chemical, Biological, Radiological, Nuclear and Explosive (CBRNE) materials.

The OSTP report also identifies early detection of Biological and Chemical Threat Agents as a critical capability required to enhance our Nation's homeland security.

The early detection of Biological and Chemical Threats, like the ability to detect fissile material, requires advanced knowledge of material science and sensor engineering. NSF supports both of these activities within and beyond the NNI.

For instance, NSF funds the Materials Research Science and Engineering Centers program. These centers are located at leading academic institutions in seventeen states across the country and represent a significant portion of our Nation's most advanced work in the area of material science. NSF also co-funds a program titled: Interaction in Chemistry, Materials Research, Molecular Biosciences, Bioengineering, and Chemical Engineering with the National Institute of Standards and Technology (NIST). This program was developed to facilitate the interaction between NSF-sponsored academic researchers and NIST's Chemical Science and Technology Laboratory and Materials Science and Engineering Laboratory. These laboratories house NIST's activity on chemistry, materials research, molecular biology, bioengineering, and chemical engineering, all relevant to advancing our capability for detecting chemical and biological threats.

Sensors and Sensor Networks

In the area of advanced sensors, NSF's Sensors and Sensor Networks program seeks to advance fundamental knowledge in the engineering of materials, concepts and designs for new sensors, networked sensor systems in a distributed environment and the interpretation and use of sensor data in decision-making processes. Like most of the activity sponsored by NSF, the capabilities enabled represent state-of-the art research at the frontiers of knowledge and comprise a significant proportion of our Nation's most advanced work on sensor and sensor systems. This work includes research that investigates networks for health monitoring and damage assessment of the civil infrastructure, both physical and cyber. Flexible and scalable software architectures and frameworks are being developed to integrate real-time heterogeneous sensor data, database and archiving systems, computer vision, data analysis and interpretation, numerical simulation of complex structural systems, visualization, probabilistic risk analysis, and rational statistical decision making procedures.

To highlight some of this advanced activity, NSF sponsored a media briefing last September titled "Sensors: Buildings, Battlefields, and Beyond" which described what many of our Nation's top technology leaders believe is the next generation of the information technology revolution, namely the ability to augment our advanced computational resources with a wide array of geographically-distributed sensor data. Clearly, this focus on sensor and sensor networks will have impact in the area of homeland security.

The OSTP report also identifies Medical Countermeasures to Weapons of Mass Destruction (WMD) as a critical capability where our Science and Technology community can contribute. While most of our Nation's work in this area is supported by the Department of Health and Human Services, NSF has and will continue to play a significant role. NSF, in collaboration with the Department of Agriculture, has funded a program on microbial genome sequencing that provides key information enabling identification and understanding of the life functions and ecology of microbes, some of which have the potential to be used in biological-based WMD. The genome sequence of these microbes, once known, can be utilized to develop countermeasures such as antimicrobial chemicals and vaccines. This jointly funded program also relates directly to protecting our agricultural systems from both man-made and naturally occurring threats, also identified in the OSTP report as a critical initiative.

Agriculture

Protecting agriculture and our food supply represents a unique area where a synthesis of NSF activity contributes to our Nation's homeland security. As stated above, NSF co-sponsors research into microbial gene sequencing and sponsors sensor and sensor networks, both of which are directly related to securing our agricultural supply chain. NSF also supports the Biochemical Engineering and Biotechnology program which funds technology development for the purpose of monitoring and controlling bioprocesses and food processing with a special focus on the safety of the Nation's food supply.

Another area of activity that NSF supports is the Environmental Engineering and Technology program. This program focuses on research with the goal of reducing adverse effects of solid, liquid, and gaseous discharges into land, fresh and ocean waters, and air as a result of human activity. This program also supports research on innovative biological, chemical, and physical processes used alone or as components of engineered systems to restore the usefulness of polluted land, water, and air resources. The understanding of these engineered systems will lead to advanced na-

tional capabilities in the area of remediation, an area directly related to homeland security.

The OSTP report identifies Biometric Identification as a critical need and has created the National Science and Technology Council's Subcommittee on Biometrics. NSF is represented on this subcommittee and also sponsors advanced research at the Center for Identification Technology Research as well as numerous grants to the small business community that advance state-of-the art biometric capability in a commercial setting.

First Responders

To enhance first responder capability, NSF has sponsored work in advanced adhoc networking to enable the rapid deployment of communications networks. Along with the Department of Defense, NSF has sponsored the Center for Robot Assisted Search and Rescue. To advance the first-responders capacity to deal with chemical and biological threats, NSF has sponsored work that led to the development of an advanced material nano-engineered to quickly absorb and destroy a wide array of toxic chemicals. The commercial development of this material also is being sponsored by an NSF Small Business Innovation Research (SBIR) grant. This is one example where original fundamental NSF-supported academic research and the subsequent support from the NSF SBIR program has directly led to a potentially significant advance in the area of homeland security. The small business concern is currently working with the Environmental Protection Agency to develop capability for water remediation.

Information Technology

Another critical area that pertains to homeland security where NSF is actively supporting our Nation's capabilities is in the area of Information Technology. Specifically NSF, in collaboration with the Department of Homeland Security, supports the Cyber Defense Technology Experimental Research network, a collaborative network developed as a testbed for cyber war gaming. NSF also supports the Center for Internet Epidemiology and Defenses, which is dedicated to wiping out worms and viruses that infect thousands of computers and cause billions of dollars in damage. These two centers represent just a small fraction of the Information Technology Research NSF supports that is directly relevant to homeland security.

Computers, especially those that are networked, reside at the heart of systems on which people now rely, both in critical national infrastructures and in their homes, cars, and offices. Today, many of these systems are far too vulnerable to cyber attacks that can inhibit their function, corrupt important data, or expose private information.

To respond to these challenges, NSF established a new program in FY 2004 called Cyber Trust to complement ongoing cybersecurity research and education investments made in the core Computer and Information Science and Engineering programs. The Cyber Trust program promotes a vision of a society in which networked computer systems are more predictable, more accountable, and less vulnerable to attack and abuse. It also foresees systems that are developed, configured, operated and evaluated by a well-trained and diverse workforce and used by a public educated in their secure and ethical operation. As such, the program covers a wide range of research areas. In FY 2006, focused investments in this area will be both in foundation establishment and security-measure development. The former is important since we will only be able to develop predictably trustworthy computer systems if we can model and analyze cyber-trust-related phenomena. Given security threats faced today, we also need to accelerate developing technologies that can immediately address these threats.

I would note that we chose the title "Cyber Trust" because our understanding is that the public not only wants their information systems to be secure, but that they want to *trust* them in all kinds of situations. As a simple example, they need to be able to trust that data will be kept private.

In the area of cybersecurity, NSF announced in mid-April our intention to establish two new Science and Technology Centers (STCs) in Fiscal Year 2005—one a major collaborative cybersecurity project led by the University of California, Berkeley. This new cybersecurity center will investigate key issues of computer trustworthiness in an era of increasing attacks at all levels on computer systems and information-based technologies. The Team for Research in Ubiquitous Secure Technology (TRUST) will address a parallel and accelerating trend of the past decade—the integration of computing and communication across critical infrastructures in areas such as finance, energy distribution, telecommunications and transportation. The center will merge these efforts with investigations of social science questions

involving economics, public policy and societal challenges, human-computer interfaces and privacy, among other issues.

NSF also supports a significant amount of work in the area of data mining and the Intelligence Community has provided supplemental funds to further NSF-sponsored research within this area. For example, novel data mining-based anomaly detection techniques developed under NSF support have been incorporated in the Minnesota Intrusion Detection System (MINDS) that help cybersecurity analysts detect intrusions and other undesirable activity in real life networks. MINDS is being used at the Army Research Laboratory Center for Intrusion Monitoring and Protection and at the University of Minnesota to successfully detect novel intrusions, policy violations, and insider abuse that cannot be identified by widely used signature-based tools. MINDS allows cybersecurity experts to quickly analyze massive amounts of network traffic, as they only need to evaluate the most anomalous connections identified by the system. Further summarization of these anomalous connections using association pattern analysis helps in understanding the nature of cyber attacks, as well as in creating new signatures for use in intrusion detection systems. The underlying techniques have applicability in many areas beyond cybersecurity, such as financial and health care fraud detection.

In addition, NSF has and continues to sponsor research in the following areas related to cyber-security:

a) security of next generation operating systems,
b) forensic and law enforcement foundations,
c) human computer interfaces for security functions,
d) theoretical foundations and mechanisms for privacy, security and trust,
e) improved ability to certify system security properties,
f) more effective system monitoring, anomaly detection attack recognition and defense, and
g) integrating hardware and software for security.

The Federal Cyber Service Scholarship for Service (SFS) is a program co-sponsored by NSF and DHS that seeks to increase the number of qualified students entering the fields of information assurance and computer security. The SFS program provides scholarship money for a maximum of 2 years to outstanding cybersecurity undergraduate and graduate students in exchange for an equal amount of time spent in Federal Government service after graduation. The SFS has supported students who have gone on to either internships or post-graduation employment within, among others, the following agencies: CIA, DoD (Defense Computer Forensics Lab, NSA), DoE, DHS, DOJ (FBI, CIO), NSF and NASA.

Social, Behavioral, & Economic Sciences

The OSTP report, as well as the recently released report by the National Science and Technology Council, *Combating Terrorism: Research Priorities in the Social, Behavioral, and Economic Sciences,* identifies research on cultural and sociological factors that may give rise to an environment conducive to terrorism as well as research into individual behavioral indicators that may correlate with intent to harm as important areas of study for the science and technology community. In this connection, NSF grants have enabled the sophisticated incorporation of geographic and other spatial data into analyses of human behavior, they have advanced our understanding of how networks link people and organizations, and have supported surveys on religious and democratic values in Islamic and third world countries.

In order to better understand the complex dynamics within and among human and social systems and their environments, NSF has recently initiated a 5 year, agency-wide research program in human and social dynamics. Emerging research and tools will provide a window into the human mind that will revolutionize the study of human development and cognition, as well as information processing and decision-making by groups and individuals. Areas critical to homeland security include agents of change, ranging from extremist ideologies to modern technology; the dynamics of human behavior, which includes such topics as effective human-machine interfacing, and decision-making and risk, which has special relevance to preventing, communicating about and recovering from the destructive consequences of extreme events.

The Intelligence Community and NSF are also sponsoring research on the detection of deception that includes investigation and development of behavioral biometrics (measurable behavior traits acquired over time), content analysis in foreign documents and speech, alternatives to the polygraph, and improvements in intelligence analysis by increasing our understanding of thought processes, learning, and decision-making in individuals and teams. Recently, NSF initiated a 5 year research program in human and social dynamics. Emerging research and tools will provide

a window into the human mind that will revolutionize the study of human development and cognition, as well as information processing and decision-making by groups and individuals. Areas critical to homeland security include agents of change, ranging from extremist ideologies to modern technology; the dynamics of human behavior; and decision-making and risk, which has special relevance to extreme events.

Fielding Advanced Capabilities

In addition to the programs outlined above which *directly* support the OSTP-identified areas of vital Science and Technology for securing our homeland, NSF is supporting research at the frontiers for fielding advanced capability for future-generation needs. Some of this work is supported by the Foundation's SBIR/STTR program that, in accordance with the FY05 Interagency Research and Development Priorities announced by the Directors of OSTP and the Office of Management and Budget, created a cross-disciplinary program to address specific opportunities for developing Security Technologies. The SBIR/STTR Security Technologies subtopics were developed in collaboration with the DoD, DHS and the Intelligence Community. With this program, NSF only supports leading edge Security Technologies enabled by the convergence of two of the following three technologies: nanotechnology, biotechnology and information technology. The capabilities envisioned by the convergence of these technologies are considered to be among the most profound in human history and NSF believes that the advancements supported by this effort will lead to capabilities in the years and decades to come.

Conclusion

Mr. Chairman, as you can see from the numerous examples above, the National Science Foundation is committed to the advancement of studies that have a direct impact on our Nation's homeland security. Our dedicated program staff understands the significance that science and engineering have on security and works to ensure that capabilities at the frontiers of science and engineering today will keep pace with the advances and threats of tomorrow. By supporting work that advances the Nation's health, prosperity and welfare, NSF is instrumental in influencing the future of scientific endeavor. NSF works in collaboration with DHS, the Intelligence Community, DoD, DOE, our federal labs and the private sector to ensure that this wealth of knowledge is effectively transferred into capabilities critical for advancement in many areas, including homeland security. The National Science Foundation will continue to participate in a multidisciplinary approach to the challenges faced by the engineering and scientific community in a way that will impact our country for generations to come.

Mr. Chairman, thank you again for this opportunity to testify on a topic of great importance. I hope that I have conveyed the serious approach that NSF has taken to address these issues. I would be pleased to answer any questions you might have.

Senator DEMINT. Thank you.

I'd like to invite Senator Nelson, our Ranking Member, to make a statement and to start the questions.

STATEMENT OF HON. E. BENJAMIN NELSON, U.S. SENATOR FROM NEBRASKA

Senator BEN NELSON. Well, thank you very much, Mr. Chairman. I appreciate very much your scheduling this hearing, and I look forward to working with you this year on these critical issues of safety and welfare, and, in many cases, health, as well. And I appreciate the appearance of our witnesses today.

The first hearing is not necessarily focused on natural disasters, but, whatever we talk about relates to either manmade disasters or natural disasters, because we're talking about preparedness, warnings; and a lot of the technology that is there can serve many different purposes. And I commend all of you for working, as best you can, to share and double-function your technologies to do as much as you can possibly do to make us all safer, in only—in a way that only, I think, you can do that.

Obviously, the ability to extend a warning about a bioterror attack to the public, and also warn them of a tornado—I have visited the National Weather Service, just outside of the city of Omaha, in Valley, Nebraska, just within the last couple of months to take a very close look at what capabilities they have. It strikes me, also, that, while you wouldn't consider an Amber Alert necessarily a weather-related item, because it's not, but the utilization of that kind of technology in similar situations can certainly benefit those who would have that great need, and would keep us all safer and more comfortable. So—and then if we develop lighter, stronger, and more blast-proof materials, I think they could also have another use, and that's perhaps to make our cars safer. You know, so protecting the security of computer networks not only foils cyberterrorists, it also stymies identity thieves that are there at work today.

So, I'm concerned when I hear you say, Dr. Bement, that sometimes science and technology interests are falling off. I know that very often R&D funds are the first that are sliced, in tight economic times, when, in fact, they should be the last funds that are affected.

So, I commend your agencies for using whatever limited resources you have to do as much as you possibly can for safety and security. I must say that I'm concerned about the decline in the number of science and engineering graduates. I must confess that perhaps I was one of those. I was president of my high-school science club, but I took a different route, as you can see. So, I don't know that I deprived our science and technology field of a great mind in that field, but, certainly, we do have to do what we can to build back for more scientific careers. We recognize that, and you can expect a commitment on my part, and, I'm sure the Committee's part, to try to help in any way that we can to rationally effect greater movement toward these science, engineering and technology careers.

Thank you very much, Mr. Chairman.

Senator DEMINT. Thank you, Senator Nelson.

A question from Senator Stevens that I'd like to pass along, Admiral, to you. In the past 2 years, Congress has appropriated a total of 20 million to develop a national alert system, including the distribution of NOAA Weather Radios to schools. How many radios have been distributed to schools so far? And do you have sufficient funding in the budget to complete the task?

Admiral LAUTENBACHER. The radios have not been distributed yet. We're very close to doing that. The money was distributed to the Department of Homeland Security, so we've developed a memorandum of understanding, and have had to determine where we would distribute them. Right now, the plans are following, to start with two rural states, who happen to be Alaska and Mississippi, for Senator Stevens' edification, and then to the top 10 to 15 urban areas, high-security urban areas, as on our—as agreed to by the Department of Homeland Security on their list, starting with New York, Chicago and Washington. So, the plan is, within the next 6 months, to start working our way down the major cities, and then the rural states. And there is not sufficient funding yet to do the entire Nation, but this is a pretty good dent in that task, and we

appreciate the fine support we've had in getting help for this project.

Senator DEMINT. It would be helpful if you kept the Committee informed as to how that progress went and——

Admiral LAUTENBACHER. Yes, sir.

Senator DEMINT.—Senator Stevens is interested.

Admiral LAUTENBACHER. I am interested. We will keep you up to date, sir.

Senator DEMINT. Let me ask you—I guess this could go to all three of our panelists—is there someone, or a group, at the Department of Homeland Security that has called you in? As I hear about the different expertise that you have here today, each expressing the different areas where there might be a threat in the country, I ask how you could bring your expertise, your equipment, your research to bear on that. Is there someone at Homeland Security that's called you in to collaborate on how to protect the country?

Dr. BEMENT. Well, I can start.

First of all, we have a seat on the Interagency Working Group in the National Science and Technology Council that deals with homeland security, and a lot of these questions get addressed in that working group. In addition to that, we are connected with the university program in the Department, and we have a number of joint activities with that function. And, as a matter of fact, just yesterday, as a result of reading my written testimony, a program director at Homeland Security asked to come and talk with us about a possible MOU in his area of expertise. So, this continues to bubble up. We thought we had all the connections made, but we're still finding more as we go along.

Admiral LAUTENBACHER. Yes, I've found similar—we are in the beginning of ensuring effective intergovernmental coordination—agency coordination, in my opinion. We have set up—and we have had contact. We've worked with—the Deputy Secretary has come to talk to us, and we've talked to them. We have set up a NOAA office, or a NOAA desk, in the Homeland Security Operations Center, so NOAA is part of providing the kinds of environmental information that the President and the entire country needs for responding to any mishaps or terrorism that might occur. So, we're part of that.

We have made contact and discussed mutual research and development with the Research and Development Directorate in that area. And we have worked for many, many years with the Coast Guard. Coast Guard, because of our issues with enforcement in the EEZ and fishing rules and regulations, have been—and our navigation responsibilities—have worked hand-in-glove with the Coast Guard forever. So, that arrangement continues to go very strong.

We have formed, together with a number of other agencies, under the Office of Federal Coordinator of Meteorology, who works in the Department of Commerce, to bring all the agencies together—an exhaustive inventory and development of plume and dispersion models that we are helping—what's now called the IMAC come up with the preferred models to use in various situations. So, we are connected with that part of emergency responses, as well. So—and we work, of course, with FEMA, because of the hurricane issues and responses to flooding and the types of things

where you need to have local, quick, rapid response. FEMA is hand-in-glove with—have been hand-in-glove with our folks for many years.

Dr. SEMERJIAN. As I mentioned before, we do have an MOU signed with the Department of Homeland Security. As part of that agreement, we actually have several NIST staff members that are detailed to DHS to both help us coordinate our mutual work and help with the implementation of their mission. We also have seats at various NSDC committees on homeland—on national security, their committees on medical countermeasures, biodiagnostics, biological and chemical preparedness, regional security, infrastructure committees. These are all basically framework that help us coordinate our efforts, and NIST has participation in all of these committees and subcommittees to make sure that our efforts are coordinated.

Senator DEMINT. Let me ask a couple of, I guess, specific application-type questions.

I know we're concerned about the Nation's water supply; what a terrorist could do to poison, or to somehow contaminate, our water supply. I know we have buoys and monitors that we use in the ocean. Have we looked at how to apply that technology to contaminants in water reservoirs across the country?

Yes, sir?

Dr. BEMENT. At the Foundation, we are supporting research in water remediation, as well as air and ground remediation, from various types of attacks, whether they're fissile materials or chemical or biomaterials.

Senator DEMINT. Are you talking about detection or remediation?

Dr. BEMENT. I am talking about remediation, which I thought was the core of your question. Restoring potable water——

Senator DEMINT. No, my question was an alert that the water had been contaminated——

Dr. BEMENT. Oh. Sorry.

Senator DEMINT.—through—I mean——

Dr. BEMENT. Well, in that area, that would go more to our sensor arrays or——

Senator DEMINT. Right.

Dr. BEMENT.—developing advanced sensors for that kind of detection and warning.

Senator DEMINT. Doctor?

Dr. SEMERJIAN. We're working with both CDC and FDA—and there is actually a federal-wide consortium, something called Integrated Consortium of Laboratory Networks and, actually, we have a formal MOU among basically all of the agencies that are involved in this—with the vision of U.S. Homeland Security infrastructure, with a coordinated and operational system of laboratory networks that provide timely, high-quality, and interpretable results for early detection and effective consequence management of acts of terrorism and other events requiring an integrated laboratory response. This is to make sure that we can immediately sample potential attacks at home, and make an immediate decision whether there has been an attack, and how, what the level of contamination is and what kind of mitigation strategies may have to be taken. So,

this is to establish a nationwide network that involves, basically, many agencies' laboratory capabilities so that we can have access and immediate remediation activities to address the issues.

Senator DEMINT. Have we—in your meetings with Homeland Security—I'm just trying to determine how far we've gone. We know our water and food supply is threatened. And it sounds like there could be monitoring devices, detection devices, that might help us determine, at various points along the food chain or water reservoirs—that we could actually detect contaminants before they affected people. And I'm just wondering if we've taken our collaboration with Homeland Security far enough to actually challenge one of your agencies to develop a device that could do that.

Dr. SEMERJIAN. There are—I mean, the issues are different, of course, whether we're dealing with food contamination, food poisoning, contamination, or water-contamination issues. Indeed, DHS is looking at specific technologies to do this. The idea with this consortium was, once an attack, let's say, is detected, can we quantify that and—so that we can evaluate whether it's a major problem or a minor contamination issue, et cetera. But I don't think, at this point, there is a nationwide network of detectors, let's say, located in different places. But I think—my understanding is, DHS is considering such a plan.

Senator DEMINT. OK.

Dr. SEMERJIAN. But I'll be happy to provide you additional information on that.

Senator DEMINT. It would just seem that if—I mean, I can think of ventilation systems in buildings, food supplies, public schools, or grocery stores. If these things were somehow where we had folks, kind of, working to determine if current technologies could help us, with sensors and monitors, could we determine if we had a problem?

Dr. BEMENT. Well, we—at the Foundation, we've been working with other agencies through our SBIR and STTR programs, which support small businesses, high-technology businesses, in developing new security technologies. And a lot of the work that is being done in this area is emerging from these small high-tech companies. And that's the way in which our Foundation would be making a contribution in this area. And a lot of that work does deal with sensors and detection and warning systems.

Admiral LAUTENBACHER. May I add a couple of things?

As I mentioned, this DCNet idea, which are local detectors, those detectors—and there's 11 or 12 of them in this—right in this city, one protecting this area—they can measure chemical incursions in the atmosphere. And they're working on biological, and there are some radiological sensors that could be added. So, that system has great promise for metropolitan areas in determining instant intrusion by some foreign substances into our air system. That system, if it were—we were looking at putting them in New York, as well. So, the technology exists for us to do that for our air monitoring. We also would like to add chemical detectors to our—some of our buoys along the coast, because that would allow us—in our harbors—because that would allow us to get a leg up on—and they have not been added yet, that I know of, not in any great num-

bers—but the technology exists to do that. We could work together to provide that kind of protection for water supply.

Senator DEMINT. Senator Nelson?

Senator BEN NELSON. Thank you, Mr. Chairman.

Admiral you mentioned that you're working on getting the radios to Alaska and to Mississippi. What are your plans, and what are you looking for, in terms of funding, to get that program extended to other states—Nebraska, for example?

[Laughter.]

Admiral LAUTENBACHER. Yes, sir. We understand that, after this pilot program starts—and that's about a 500K program, is what I have right now—that those radios should be starting to arrive, as I mentioned, in September. In a few months, we'll have that in place. And DHS is prepared to add another 1½ million to that, with—you know, continuing the distribution. So, to that, we would add more states, more rural states and more cities, and keep on going. Obviously, I don't have a figure on top of my head, that it would take to do the entire country. I'd be happy to provide that.

Senator BEN NELSON. Well, it might be helpful for us. Obviously, as we look at budgeting—not this year, but in the future—if we're short on the budget, you're not going to get the radios to the locations.

Admiral LAUTENBACHER. Yes, sir.

Senator BEN NELSON. And I—it was right after the tsunami that we had some hearings in which we found out that some of the sensor buoys that were locating earthquakes and identifying earthquakes, give us some advanced warning for tsunami activity, weren't functioning. Do you know whether that situation has been corrected?

Admiral LAUTENBACHER. I believe the situation that you're referring to has been corrected. And let me specify, these were the new technology-six buoys. They're called DART buoys. They are, in my view, from my military days, they are Op/Eval buoys. They are first generation. Three of them were down, and they are all up now. They have all been repaired and put back online. The next set that we will put in the water will be second-generation technology. We believe they'll be much more reliable.

I do want to point out that the ones that were not operational—there was a—there were three buoys in place that were monitoring the dangerous areas, the most dangerous parts of the Ring of Fire around the United States.

Senator BEN NELSON. Well, as it turned out, we didn't have to test them more closely to our—closer to our shores or to the West Coast or anything of that sort, but I think Senator Stevens was more than slightly disturbed by that fact, as was——

Admiral LAUTENBACHER. Yes, sir.

Senator BEN NELSON.—Senator Inouye. So, I'm sure they'll both be relieved, as you are, too.

Admiral LAUTENBACHER. I am very relieved that they're operational. And our intention is to put spares along the Alaskan islands.

Senator BEN NELSON. I think a belt-and-suspenders approach would be excellent.

[Laughter.]

Admiral LAUTENBACHER. Yes, sir.

Senator BEN NELSON. Dr. Semerjian, the World Trade Center report is coming out, I think—or is going to be reviewed by NIST to conclude what is your building and fire safety investigation of the collapse of the World Trade Center. And I wonder if you could tell us a little bit about where you are in that effort as it might relate to the way people design, construct, maintain, and use buildings, so that it would help increase the safety and security, but particularly structural integrity and safety for the future.

Dr. SEMERJIAN. Yes, thank you, Senator Nelson.

We are scheduled to release our report on June 23, at a press conference in New York City, where the specific recommendations will come out, but we are already working with the organizations that will really implement the recommendations that come out of this study. These are the standards/codes organizations, organizations such as American Society for Civil Engineers, a number of other organizations. So—and that will be the first release of the report. That will be the beginning of a public comment period before the recommendations are finalized. But we actually already have a conference scheduled for September, where the findings of the report, and the recommendations, will be discussed, and the implementations with regard to standards and codes will be discussed—shared. I mean, this is clearly something that will—there will be, obviously, a lot of lessons learned, a lot of recommendations and implications for standards and codes. And we will be working with the community out there to make sure that the results are interpreted properly and that appropriate action is taken as a followup.

Senator BEN NELSON. And is it your expectation, certainly without preempting the release later this month, that there will be a great deal of followership with recommendations that—from your discussions with interested groups, such as engineers, that there will be a lot of interest in complying?

Dr. SEMERJIAN. Yes. There has been—I mean, our process has been quite open. We have an advisory committee for our National Construction Safety Team Act. Our discussions are open, so, the community has been listening, following the discussions. They haven't seen the final recommendations, but, certainly, they have been privy to all the discussions. So, there has been quite a bit of information sharing, and our staff have been briefing various communities about our findings. And, all along, we have released our findings—not the recommendations, but the findings have been released, so the community is aware of what our findings are and what would be coming, in terms of recommendations. So, the community has been following the process, and I think they have been quite receptive to a lot of recommendations.

Senator BEN NELSON. The report, will that make recommendations that are, not only related to new construction, but retrofitting current buildings so that those that are in existence right now can be made safer with adjustments and some design work?

Dr. SEMERJIAN. Yes, there are some recommendations that will impact existing buildings, also.

Senator BEN NELSON. Thank you.

One final thing. Is it Bement?

Dr. BEMENT. Bement.

Senator BEN NELSON. Bement. You know, we talked a little bit about research and development cutting back—being cut back with short funds, but I was a little concerned when I saw that the budget request for education and human resources in the budget included $104 million cut from FY05 to FY06, and that the request for math and science partnerships, which is off 24 percent from 2005, and less than half of 2004. Now, you may have an explanation for that. And so, rather than my criticize you for that, perhaps I could just ask you to explain.

Dr. BEMENT. Well, the math and science partnership program was also cut last year, as well. This is the second year. We have retained funds in that program to continue all ongoing efforts, so the mortgages are protected. The thing that has been disabled, essentially, is the startup of any new awards. So, we're protecting the existing programs.

There has also been a concurrent scale-up of activity within the Department of Education, and they are also quite active in math and science partnership. And there has been, all along, a very close working relationship between the National Science Foundation and the Department of Education. In fact, that partnership is getting stronger with the new Secretary.

So, we continue to work together to assure that the available resources are used as effectively as possible to support the overall program in math and science partnerships.

Senator BEN NELSON. But would the actual reduction in your budget be picked up by an increase in their budget, or are we——

Dr. BEMENT. I think it's pretty close to being equal.

Senator BEN NELSON. So, you're not really looking at an overall cut for this kind of education that's so critical to the future.

Dr. BEMENT. I believe that's correct.

Senator BEN NELSON. Well, thank you, Mr. Chairman.

Senator DEMINT. Thank you, Senator Nelson.

Let me go back to the National Weather Radio issue for a second, Admiral. It's clear that it's going to be years before we get these radios in all schools, and probably never, in any great penetration, into homes. Are we looking at other ways to get these messages out? For instance, I know it's very easy to program, on your computer, something that'll pop up. It would seem like it would be fairly easy to send out an alert via e-mail, the Web, or—are we just looking at other ways to deliver this message, rather than actually have a radio onsite?

Admiral LAUTENBACHER. Yes, we have. We, first of all, put out the warnings on a number of media, so they're not just going——

Senator DEMINT. Right.

Admiral LAUTENBACHER.—to the radios. They're going to all of our radio and television stations, they're going to all of the emergency managers. So, the normal or, say, other means that we have for distributing this information are taken into account, so our—we have three or four redundant systems for transmitting this information, both nationally and internationally, for that matter.

Some of the interesting things that are going on: if you happen to buy a Harley–Davidson now, you can get Weather Radio right in your cycle. So, manufacturers are bringing these things in as a permanent feature, or at least an alternative feature, that you can

buy, either in car radios—we've been looking at OnStar, those kinds of things. RCA-Thomson has worked on a television model that'll be part of a standard package.

So, to the extent that we can make it, as you say, part of other things—computers, televisions, radios—we are very big into working on that project.

Senator DEMINT. Senator Nelson, any other questions?

Senator BEN NELSON. No. No, thank you.

Senator DEMINT. Any other comments for the Committee that you'd like us to make part of the record, any of the folks here?

Yes, sir? Doctor?

Dr. BEMENT. I'd like to go back to food security, just for a moment. There are sensor arrays that are being developed under grants of the National Science Foundation that will track biological attacks of agriculture. Furthermore, through our program in microbial genomics, we're studying microbes, the genome sequencing of microbes in order to understand how to develop countermeasures, for such toxic agents as wheat rust, soybean rust, rice blast, and even anthrax. So, this is a very important component of our ongoing program, not only to detect these types of attacks, but also to develop countermeasures against them.

Senator DEMINT. One more quick question for the National Science Foundation. I think you made some comments, as related to data mining, the ability to extract messages from large banks of information. Any other comments in that area? I know that's something that we hear a lot about from the intel community, looking for possible dangers or things that might tip us off. Are there things going on there that would encourage us?

Dr. BEMENT. Well, we have a number of joint efforts with the intelligence community and also with the Department of Homeland Security, where they contribute funding into our ongoing efforts that will do pattern recognition, will understand anomalous incidences that occur in data patterns, to detect intrusive behavior that would jeopardize security, and also would do what we would call Internet epidemiology to deal with worms and viruses. And those capabilities become more robust with time, as we learn more about them and as we also try and develop more robust systems. So, those are some additional activities that are going on.

Senator DEMINT. Well, Senator McCain is back, and I think you had some questions for the panelists.

STATEMENT OF HON. JOHN MCCAIN,
U.S. SENATOR FROM ARIZONA

Senator MCCAIN. Thank you very much, Mr. Chairman. And thank you for allowing me to ask a couple of questions.

Admiral Lautenbacher, you're the guy that said we had to sleep for 20 or 30 years before we'd know anything about climate change. According to the General Accountability Office, Admiral, a report of April 14, 2005—have you seen it, concerning climate-change assessment? The Administration did not meet the reporting deadline?

Admiral LAUTENBACHER. I've seen a few articles. I don't remember the one about the reporting deadline. I've seen a few recent articles on our—on the Administration's reports.

Senator MCCAIN. So, you don't really pay much attention to general Government Accountability Office reports that have direct—that you're the lead organization—with responsibility for it? I suggest you do, Admiral. So, since you haven't taken the time to read a Government Accountability Report that directly affects you, let me give you a couple of quotes.

The Global Change Research Act of 1990 required the Administration to, among other things, prepare a national global-change research plan, a summary of the achievements and expenditures in the area of federal climate-change research. The scientific assessment is to be prepared at least every 4 years. And it goes on as to what report.

I'm sure you—I'd better read it to you, because I don't——

Admiral LAUTENBACHER. I have read that one, sir. I didn't know which you were referring to.

Senator MCCAIN. Oh, OK.

Admiral LAUTENBACHER. I have read that report. I understand what it says.

Senator MCCAIN. All right. Basically, they say you're not complying with the law.

Admiral LAUTENBACHER. Yes, sir.

Senator MCCAIN. Are you complying with the law?

Admiral LAUTENBACHER. I believe that we are complying with the law, yes, sir. We have answered——

Senator MCCAIN. So——

Admiral LAUTENBACHER.—some of the——

Senator MCCAIN. Well, you're complying with the law. Did you submit a scientific assessment on November 2004, 4 years after the previous assessment, as required by the Act?

Admiral LAUTENBACHER. We have been working on the pieces of it, and we believe——

Senator MCCAIN. Did you submit it, a scientific assessment, on November 2004, 4 years after the previous assessment, as required by the Act?

Admiral LAUTENBACHER. No——

Senator MCCAIN. Yes——

Admiral LAUTENBACHER.—sir——

Senator MCCAIN.—or no?

Admiral LAUTENBACHER.—we did not.

Senator MCCAIN. You did not. But you're in compliance with the law. You know, you are really one of the more astonishing witnesses that I have—in the 19 years I've been a Member of this Committee, Admiral, because, clearly, you're in violation of the law when you didn't submit, on November, a scientific assessment, 4 years after the previous assessment, as required by the Act. I'd be glad to send you the language of the Act. Nor have you shown any inclination to do so. Reports are now expected to be completed up to a year later than planned, September 2006. The remaining 12 reports are currently expected to be completed by September 2007. Do you have any response to that, Admiral? Probably not.

Admiral LAUTENBACHER. Yes, sir. We have—we have discussed it with your staff, we have discussed it with many Members. We're trying to look at the best way to do this. It took 10 years to submit the first report. The limit was set at 4 years. This is a difficult re-

quirement to meet on time, and I think we'll come in closer to it than the first report came in.

Senator MCCAIN. Did you ever notify this Committee that you would not be able to meet the requirements of the Act?

Admiral LAUTENBACHER. I think we have. I'll go back and look at it. We certainly——

Senator MCCAIN. I don't think you have——

Admiral LAUTENBACHER.—had discussions with staff——

Senator MCCAIN.—Admiral, and if——

Admiral LAUTENBACHER.—members.

Senator MCCAIN.—If I was notifying the Committee of oversight, I might remember whether I did or not.

Admiral LAUTENBACHER. We did talk with staff members about our ability to——

Senator MCCAIN. Did you——

Admiral LAUTENBACHER.—do that, sir.

Senator MCCAIN.—notify this Committee that you were not going to be in compliance with the Act?

Admiral LAUTENBACHER. I will go back and look at the memorandums that we——

Senator MCCAIN. We have no——

Admiral LAUTENBACHER.—submitted for the record.

Senator MCCAIN.—record of it, Admiral.

Well, Mr. Chairman, I don't mean to drag this out, but the General—Government Accountability Office says that Congress and other users will not know when or where eight areas will be addressed, according to the law. So, we have an agency of government here, responsibility for the oversight of an issue that many people, including Prime Minister Blair, think is the single-most—who is now visiting our President—single-most important issue affecting the world, climate change, and this witness in this agency doesn't care enough to even notify the Committee of oversight that they are unable to meet the statutory requirements of law.

So, I have no choice, Admiral, but to try to act legislatively to try and see that you do obey the law. You know, that's, kind of, a fundamental around here. And so—and I don't know exactly what those courses of action will be, but, believe me, we will explore every one.

And I, again, want to express my deep disappointment at your complete lack of concern about future generations of Americans who are affected by climate change, which overwhelming scientific evidence is now—let me just—because I'm sure you probably didn't read it—"The National Academy of Sciences, along with the national academies of ten other nations, issued a joint statement on the global response to climate change. The scientific understanding of climate change is now sufficiently clear to justify nations taking prompt action. It's vital that all nations identify cost-effective steps that they can take now to contribute to substantial and long-term reduction in net global greenhouse-gas emissions."

And all we're asking from you is a report, and we can't even get that.

Thank you, Mr. Chairman.

Senator DEMINT. Thank you, Senator McCain, and I want to thank all the panelists. Great information today, and we'll be fol-

lowing up. And some of the things that were mentioned that you were going to keep us in the loop on, I greatly appreciate.

Thank you.

[Whereupon, at 3:35 p.m., the hearing was adjourned.]

A P P E N D I X

PREPARED STATEMENT OF DANIEL K. INOUYE, U.S. SENATOR FROM HAWAII

Mr. Chairman, thank you for holding this hearing today to examine the science occurring throughout our federal agencies that can help improve our homeland security.

I firmly believe that research and development at the various agencies within our jurisdiction such as the Coast Guard, the Transportation Security Agency, the Department of Transportation, the National Aeronautics and Space Administration, and of course the three agencies that we will discuss today, have much to contribute in keeping the Nation safe.

Today's hearing will examine the hard science and operational assets of three of our science agencies, the National Oceanic and Atmospheric Administration (NOAA), the National Institute of Standards and Technology (NIST), and the National Science Foundation (NSF) that are improving homeland security.

I would like to thank these agencies for their work. NOAA is leveraging its assets from NOAA weather radio to modeling to environmental monitoring to help our ability to prevent and respond to terrorism.

NIST has become a resource for first responders, builders, and the Department of Homeland Security when it comes to improving technology.

The NSF is funding the basic research that may not come to fruition for ten to fifteen years but which could fundamentally change our understanding of the human dynamics of terrorism, the ability of computer networks to protect themselves, or the ability for sensors to detect multiple threats.

Unfortunately, these agencies that contribute so much are asked to do so with little recognition and tight fiscal resources. I hope that today's "good news" hearing can help us build the case for NOAA, NIST, and NSF and support these agencies' broad and important work