

CYBERSECURITY—GETTING IT RIGHT

HEARING
OF THE
SUBCOMMITTEE ON CYBERSECURITY,
SCIENCE, AND RESEARCH, AND
DEVELOPMENT
BEFORE THE
SELECT COMMITTEE ON HOMELAND
SECURITY
HOUSE OF REPRESENTATIVES
ONE HUNDRED EIGHTH CONGRESS

FIRST SESSION

JULY 22, 2003

Serial No. 108-18

Printed for the use of the Select Committee on Homeland Security



Available via the World Wide Web: <http://www.access.gpo.gov/congress/house>

U.S. GOVERNMENT PRINTING OFFICE

98-150 PDF

WASHINGTON : 2005

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

SELECT COMMITTEE ON HOMELAND SECURITY

CHRISTOPHER COX, California, Chairman

JENNIFER DUNN, Washington	JIM TURNER, Texas, Ranking Member
C.W. BILL YOUNG, Florida	BENNIE G. THOMPSON, Mississippi
DON YOUNG, Alaska	LORETTA SANCHEZ, California
F. JAMES SENSENBRENNER, JR., Wisconsin	EDWARD J. MARKEY, Massachusetts
W.J. (BILLY) TAUZIN, Louisiana	NORMAN D. DICKS, Washington
DAVID DREIER, California	BARNEY FRANK, Massachusetts
DUNCAN HUNTER, California	JANE HARMAN, California
HAROLD ROGERS, Kentucky	BENJAMIN L. CARDIN, Maryland
SHERWOOD BOEHLERT, New York	LOUISE McINTOSH SLAUGHTER, New York
LAMAR S. SMITH, Texas	PETER A. DeFAZIO, Oregon
CURT WELDON, Pennsylvania	NITA M. LOWEY, New York
CHRISTOPHER SHAYS, Connecticut	ROBERT E. ANDREWS, New Jersey
PORTER J. GOSS, Florida	ELEANOR HOLMES NORTON, District of Columbia
DAVE CAMP, Michigan	ZOE LOFGREN, California
LINCOLN DIAZ-BALART, Florida	KAREN McCARTHY, Missouri
BOB GOODLATTE, Virginia	SHEILA JACKSON-LEE, Texas
ERNEST J. ISTOOK, JR., Oklahoma	BILL PASCRELL, JR., New Jersey
PETER T. KING, New York	DONNA M. CHRISTENSEN, U.S. Virgin Islands
JOHN LINDER, Georgia	BOB ETHERIDGE, North Carolina
JOHN B. SHADEGG, Arizona	CHARLES GONZALEZ, Texas
MARK E. SOUDER, Indiana	KEN LUCAS, Kentucky
MAC THORNBERRY, Texas	JAMES R. LANGEVIN, Rhode Island
JIM GIBBONS, Nevada	KENDRICK B. MEEK, Florida
KAY GRANGER, Texas	
PETE SESSIONS, Texas	
JOHN E. SWEENEY, New York	

JOHN GANNON, *Chief of Staff*

UTTAM DHILLON, *Chief Counsel and Deputy Staff Director*

DAVID H. SCHANZER, *Democrat Staff Director*

MICHAEL S. TWINCHEK, *Chief Clerk*

SUBCOMMITTEE ON CYBERSECURITY, SCIENCE, AND RESEARCH &
DEVELOPMENT

MAC THORNBERRY, Texas, Chairman

PETE SESSIONS, Texas, Vice Chairman	ZOE LOFGREN, California
SHERWOOD BOEHLERT, New York	LORETTA SANCHEZ, California
LAMAR SMITH, Texas	ROBERT E. ANDREWS, New Jersey
CURT WELDON, Pennsylvania	SHEILA JACKSON-LEE, Texas
DAVE CAMP, Michigan	DONNA M. CHRISTENSEN, U.S. Virgin Islands
ROBERT W. GOODLATTE, Virginia	BOB ETHERIDGE, North Carolina
PETER KING, New York	CHARLES GONZALEZ, Texas
JOHN LINDER, Georgia	KEN LUCAS, Kentucky
MARK SOUDER, Indiana	JAMES R. LANGEVIN, Rhode Island
JIM GIBBONS, Nevada	KENDRICK B. MEEK, Florida
KAY GRANGER, Texas	JIM TURNER, Texas, <i>ex officio</i>
CHRISTOPHER COX, CALIFORNIA, <i>ex officio</i>	

CONTENTS

	Page
STATEMENTS	
The Honorable Mac Thornberry, Chairman, Subcommittee on Cybersecurity, Science, and Research and Development, and a Representative in Congress From the State of Texas	1
The Honorable Christopher Cox, Chairman, Select Committee on Homeland Security, and a Representative in Congress From the State of California	40
Oral Statement	4
Prepared Statement	4
The Honorable Dave Camp, a Representative in Congress From the State of Michigan	
The Honorable Donna M. Christensen, a Delegate in Congress From the U.S. Virgin Island	46
The Honorable Bob Etheridge, a Representative in Congress From the State of North Carolina	43
The Honorable James R. Langevin, a Representative in Congress From the State of Rhode Island	37
The Honorable Sheila Jackson-Lee, a Representative in Congress From the State of Texas	
Oral Statement	48
Prepared Statement	5
The Honorable Zoe Lofgren, a Representative in Congress From the State of California	1
The Honorable Ken Lucas, a Representative in Congress From the State of Kentucky	47
The Honorable Pete Sessions, a Representative in Congress From the State of Texas	34
WITNESSES	
Steven Bellovin, Ph.D., Technical Leader and Fellow, AT&T Laboratory	
Oral Statement	17
Prepared Statement	19
Shankar Sasry, Ph.D., Chairman, Department of Electric Engineering and Computer Systems, University of California, Berkeley	
Oral Statement	6
Prepared Statement	8
Mr. Daniel G. Wolf, Information Assurance Director, National Security Agency	
Oral Statement	21
Prepared Statement	24

CYBERSECURITY—GETTING IT RIGHT

Tuesday, July 22, 2003

U.S. HOUSE OF REPRESENTATIVES,
SUBCOMMITTEE ON CYBERSECURITY, SCIENCE,
AND RESEARCH AND DEVELOPMENT,
SELECT COMMITTEE ON HOMELAND SECURITY,
Washington, D.C.

The subcommittee met, pursuant to call, at 10:05 a.m., in Room 2118, Rayburn House Office Building, Hon. Mac Thornberry [chairman of the committee] presiding.

Present: Representatives Thornberry, Sessions, Camp, Cox [ex officio], Lofgren, Jackson-Lee, Christensen, Etheridge, Lucas, and Langevin.

Mr. THORNBERRY. The hearing will come to order. This oversight hearing of the Subcommittee on Cybersecurity, Science, and Research and Development will hear today on the topic of “Cybersecurity—Getting It Right.” This is the next in a series of hearings that this subcommittee has had on cybersecurity. We have had virtually unanimous recommendations from previous witnesses that, among other things, research and development is a key role for the Federal Government. And we are here today to hear from some outstanding witnesses to help guide us in that research and development for the future.

Before proceeding further, let me turn to the distinguished Ranking Member of this subcommittee, the gentlelady from California, for any opening comments she would like to make.

Ms. LOFGREN. Thank you, Chairman Thornberry, for scheduling this hearing today and for your wonderful leadership of this subcommittee.

When the subcommittee was formed back in February, Chairman Thornberry and I met to discuss our common agenda and priorities. And at that meeting we both agreed that the subcommittee should spend considerable time studying incredibly complex sets of issues surrounding cybersecurity, and we decided to embark on a mission to educate and inform the members of the subcommittee. We felt the need to establish a knowledge base before we attempted to tackle any possible policy directives or legislative initiatives.

Soon after our initial meeting, we began this educational process. At our first meeting, we heard from Dr. Charles McCreary on the work being done within the Science and Technology Directorate at the Department of Homeland Security. Soon after that, we began a series of hearings on the cybersecurity issue. First, we looked into threats, vulnerabilities, and possible responses to cyber attacks. Last week, we heard from industry leaders on their experiences.

In addition to these hearings, we have held several briefings on cyber issues, including a classified briefing on cyber threats. Chairman Thornberry and I have also had individual meetings with academics, business leaders, and public policy experts. All of these meetings and hearings have been quite informative, and helped the members of this committee to get a handle on the scope of the issues we face. I believe that this subcommittee is beginning to have a solid understanding of the cyber question, and I am sure we are going to build on this foundation today.

Today, we will explore the research agenda that will help us to better secure cyberspace. Our panelists represent academia, the national security community, and industry, and all are well-versed on cyber issues. Scientific research and innovative technology may hold some of the most promising solutions to our IT vulnerabilities, and I believe that we can stay one step ahead of hackers and cyber terrorists if government works in a coordinated way with the private sector.

I look forward to learning more about the advanced technology programs that currently exist and the ones that need to receive higher priority and funding. I want to hear about the current efforts to share information between the private sector, the government, and academia. Government, and this subcommittee in particular, should play a role in helping these diverse entities work together to reduce all our vulnerabilities and better secure cyberspace.

I am looking forward to hearing from all of our witnesses today, but I especially want to welcome and thank Dr. Shankar Sastry, Chairman of the Electrical Engineering and Computer Sciences Department at UC-Berkley. I have had the pleasure of discussing these issues with Dr. Sastry before, and I appreciate you coming all the way to be with us here today.

Finally, as I mentioned in my opening statement at last week's hearing, I have great concerns about the Bush administration's cybersecurity program. In the last 6 months, the most senior Bush administration cyber officials have left the government. These individuals include Richard Clark, the Special Advisor to the President for Cybersecurity; Howard Schmidt, the Vice Chair of the President's Critical Infrastructure Board and Clark's replacement; Ron Dick, the Chairman of the NIPC; and John Tritak, Director of CIAO. The last two organizations are part of the National Cybersecurity Division at DHS which was created on June 6th of this year. To date, no director has been named for this division. The NCSA is located within the DHS Information Analysis and Infrastructure protection directorate, reporting to the Assistant Secretary for Infrastructure Protection. Some cybersecurity-related R&D activities, however, will take place within the DHS Science and Technology Directorate.

I believe that this situation where it is buried within the bureaucracy is questionable, and that once a person is finally chosen to lead the division, he or she may not receive the high-level access to Secretary Ridge and the White House that is warranted.

The House is going to adjourn at the end of this week for the summer district work period, and when we return in the fall, I look

forward to hearing directly from the Department of Homeland Security on their cybersecurity agenda.

I thank Chairman Thornberry for scheduling this hearing, and I thank him for his leadership and for working so well and honestly with me. And I thank you, too, our witnesses, for their testimony, and finally to the committee staff for their outstanding work.

Mr. THORNBERRY. Let me thank the gentlelady, and express agreement with the concerns that she has raised. We will be hearing from the Department of Homeland Security when we return, and this committee as well as the full committee, I know, will be certainly engaged with them.

The Chair is going to yield his time for an opening statement to the distinguished chairman of the full committee, the gentleman from California, Mr. Cox.

Mr. COX. I thank the Chairman and the Ranking Member. And I will be brief, because we have an excellent panel of witnesses today and I, like you, am anxious to hear from them. I want to thank you both for organizing today's hearing and for your continued diligence in examining the cyber threat, and for this subcommittee's focus on the Department of Homeland Security's mission to counter this new and worrisome threat. I would also like formally to thank our witnesses for making the time to be with us today.

Just as our focus on science, including notably the Manhattan Project, contributed to our victories in World War II and in the Cold War, a similar comprehensive commitment to scientific inquiry, to basic research, and to the development of innovative technologies is necessary if we are going to win the current war on terrorism. For that reason alone, the cyber challenge in particular requires a mobilization of the American scientific community.

As recently reported by the National Research Council, the United States information system vulnerabilities from the standpoint of both operations and technology are growing faster than the country's ability, if not willingness, to respond. This is a critical fault that we have got to address, because technology is at the center of our economy, our civilian and defense critical infrastructure, our communications systems, and indeed every aspect of our way of life.

Superior technology will, therefore, be at the heart of our efforts to prevent and to deal with cyber attacks. We must leverage our superior research community resources to address risks and harden our critical physical and electronic infrastructure.

Under Chairman Thornberry's leadership, this subcommittee has held three hearings and a productive half-day workshop on this issue. During these hearings, representatives from industry, government, and academia have confirmed our understanding the gravity of the cybersecurity threat and of the importance of the Department of Homeland Security's role in addressing it.

The workshop held yesterday morning, which was co-sponsored by the Congressional Research Service staff, not only accentuated the threat, but stressed the importance of the public-private partnership in developing solutions. Today's hearing will increase our appreciation for the research being done to address the cyber

threat. Each of our witnesses today represents a different facet of the cyber research community.

The Department of Homeland Security, to be effective in its analytic and policy mission, must have a clear understanding of the best research being done and where it is going. In exercising oversight, this committee will want to measure the Department's progress over time in coordinating governmentwide cyber programs, in advancing research and development efforts to reduce cyber vulnerabilities, in improving our capabilities to respond to attacks, and in accelerating our efforts to promote computer security awareness training across the country.

I look forward to hearing from our witnesses about research priorities, both in the Federal Government and in the private sector and in academia, and about ways that the Department of Homeland Security can support and capitalize on your efforts.

Mr. Chairman, thank you again for your personal commitment, and also our Ranking Member for your personal commitment and for your exemplary performance and the performance of this subcommittee on this issue. I yield back.

[The information follows:]

PREPARED OPENING STATEMENT OF THE HONORABLE CHRISTOPHER COX, CHAIRMAN, SELECT COMMITTEE ON HOMELAND SECURITY

I would like to thank Chairman Thornberry and Ranking Member Lofgren for organizing today's hearing, for their continued diligence in examining the cyber threat, and for their focus on the Department of Homeland Security's mission to counter this new and worrisome threat. I would also like to thank the witnesses for making the time to share their valuable insights with us today.

As many of you know, the Manhattan Project, launched in 1942, marked the establishment of a sustained and successful U.S. nuclear science program that grew stronger and stronger in subsequent years. This focus on science contributed to our victory in World War II and in the Cold War. The current War on Terrorism requires a similar comprehensive commitment to scientific inquiry, to basic research, and to the development of innovative technologies.

Today, the cyber challenge in particular requires a similar mobilization of the American scientific community. Technology is at the center of our economy, our critical infrastructure, our communication systems, and our way of life. Superior technology will be at the heart of our efforts to prevent a cyber attack. We must leverage our superior research community resources to address risks, and harden our critical physical and electronic infrastructure.

Under Chairman Thornberry's leadership, this Subcommittee has held three subcommittee hearings and a productive half-day workshop on this issue. During these hearings, representatives of the industry, government and academia have confirmed our understanding of the gravity of the cybersecurity threat and of the importance of the Department of Homeland Security's role in assessing it. The workshop held yesterday morning, which was cosponsored by the Congressional Research staff, not only accentuated the threat, but stressed the importance of the public-private partnership in developing the solution.

Today's hearing will increase our appreciation for the research being done to address the cyber threat. Each of our witnesses today represents a different facet of the cyber research community. The Department of Homeland Security, to be effective in its analytic and policy mission, must have a clear understanding of the best research being done and where it is going. In exercising oversight, the Select Committee will want to measure the Department's progress over time in coordinating government-wide cyber programs, in advancing research and development efforts to reduce cyber vulnerabilities, in improving our capabilities to respond to attacks, and in accelerating our efforts to promote computer security awareness training across the country.

I look forward to hearing from our witnesses about research priorities, and about ways that the Department of Homeland Security can support your efforts. Mr. Chairman, thank you again for your personal commitment and for the exemplary performance of your subcommittee on this issue.

THE PREPARED STATEMENT OF THE HONORABLE SHEILA JACKSON-LEE,
A REPRESENTATIVE IN CONGRESS FROM THE STATE OF TEXAS

Mr. Chairman and Mr. Ranking Member, I thank you for convening this hearing today so that we can take another step toward securing our homeland. Today's hearing, "Cybersecurity: Getting It Right," gives the Members of this Subcommittee another opportunity to explore the difficult and ever-changing technology sector, and to hear more invaluable testimony on protecting our information infrastructure.

A common question in our cybersecurity efforts is the issue of information sharing. The technology industry is highly competitive and also highly lucrative. Technology companies that develop innovative ideas can earn millions, if not billions, of dollars. Therefore, there is a substantial interest on the part of the corporation to keep the innovation for themselves and reap all of the financial benefits. In the general market for software and hardware development, research and development secrecy is an expected part of our capitalist economy. In the national cybersecurity arena, however, failure to share information may result in our information infrastructure being more vulnerable to cyber attacks. It is imperative to national security that the technology sector shares the information that will protect our information infrastructure. It is equally imperative that the Members of Congress pass legislation that promotes information sharing while protecting the intellectual property of our technology companies.

In order for innovations to be shared the innovations must be developed. The research and development aspect of national cybersecurity must be fostered to protect our homeland. As the capabilities of the Internet and the remainder of our information infrastructure expands, so too do the capabilities of cyber-terrorists. The complexity of recent computer viruses and the speed with which they spread across our information infrastructure illustrates the formidable task our country faces combating cyber-terrorists. Developing the technologies to counter cyber attacks will be an on-going endeavor. Each advancement in computer technology will bring advancements in the capabilities of cyber-terrorists. New technological defense methods will be required through research and development in order to adequately protect our information infrastructure.

Research and development will also be needed to detect and apprehend those responsible for cyber-terrorist attacks. The nature of the information infrastructure allows criminal actors to operate anonymously. Often the perpetrators of cyber-crimes are not located and are left free to attack our information infrastructure again in the future. If America's cyberspace is to be protected we must be able to locate the perpetrators of cyber-attacks and also develop intelligence methods to detect attacks before they occur. Our national research and development efforts will also be critical to stopping cyber-crimes before they occur.

Mr. Chairman and Mr. Speaker, the task before this Subcommittee is great. Achieving full cybersecurity for our Nation's critical information infrastructure is important for the full operation of our education system, federal, state, and local governments, our financial system, our travel system and every other segment of our society. The Internet has become an integral portion of the daily operation of all of these segments. One successful cyber-attack could have devastating consequences. I look forward to hearing the testimony of our witnesses today, and I thank them for their attendance. I hope that their wisdom will bring us closer to securing our information infrastructure.

Mr. THORBERRY. The Chair thanks the gentleman, and would also join in thanking the Congressional Research Service, Eric Ficsher and his staff, and the folks who participated in yesterday's workshop. It really was an outstanding group.

Now, again let me thank each of our witnesses for taking time to be with us today. We will first hear from Dr. Shankar Sastry, Chairman of the Department of Electrical Engineering and Computer Science from the University of California at Berkley. Thank you for being with us today, sir. And you are recognized for 5 minutes.

STATEMENT OF S. SHANKAR SASRY, PH.D., CHAIRMAN, DEPARTMENT OF ELECTRIC ENGINEERING AND COMPUTER SYSTEMS, UNIVERSITY OF CALIFORNIA, BERKELEY

Mr. SASTRY. Thank you very much, honorable Chairman Thornberry, honorable Ranking Member Lofgren, and distinguished members of the Subcommittee on Cybersecurity, Science, and Research. Thank you very much for the opportunity to testify today.

I would like to testify about areas for investment in cybersecurity, science, research and development, some priority areas for funding, and the role of university, industry, the venture community, and government partnerships in bringing secure and trusted systems to the marketplace.

By way of background, I should say that I served as Director of the Information Technology Office at DARPA from September 1999 to February 2001. My areas of research are in embedded and autonomous software, complex infrastructure systems, and secure network embedded systems.

Let me start with my perceptions of the current funding of cybersecurity research. The most sustained funding for cybersecurity research to date has been through the Department of Defense. In DOD, the largest pool for funding for research has been through DARPA, though there have been some important research initiatives also through the National Security Agency.

The programs have been in three generations. The first generation is to prevent intrusions, and there have been a number of successes that have come out of this, including several sets of cryptographic tools, access control, and multiple levels of security.

In the second generation, if intrusions happen, how does one detect them and how does one limit damage? Examples of successful products that came out of this: firewalls, boundary controllers, intrusion detection systems, virtual private networks, and a public key infrastructure.

In the third generation, which we are now in the midst of, the goal is to operate through attacks. And these goals are intrusion tolerance and graceful degradation. In my opinion, this is the space that we need to be in to be able to have critical infrastructure systems that can weather attacks.

From its high watermark of close to \$100 million of research funding per year for information assurance and survivability research, IA&S, in 2000 the funding for unclassified IA&S research has decreased significantly in the following years. While it is understandable that there are important other priorities in DOD for more focused efforts on command and control networks and other sensitive DOD networks, I feel that, given the scope and magnitude of research that remains to be done, it is critical that the burden of supporting cybersecurity research be picked up by other agencies.

Of course, I also feel that, given the newest generations of manned and unmanned and autonomous systems in the DOD such as the UCAV and in Future Combat Systems and so on, it would also be in the interest of DOD not to scale back its unclassified programs a great deal.

The National Science Foundation. I feel the NSF has been proactive in taking steps to boost funding for cybersecurity re-

search by setting up new programs in trusted computing, and in secure network embedded systems, which is under planning, networking research, and more recently test beds for cybersecurity.

Department of Homeland Security. It is our understanding that the Science and Technology Directorate is planning an initiative in cybersecurity and is organizing program management structures for cybersecurity research centers. The Congress and the administration should be lauded for having taken the visionary step of having formed the Homeland Security Advanced Research Projects Agency, HSARPA, along the DARPA model. In addition, I feel that the idea of having HSARPA work with procurement and operational branches of the DHS to evangelize the adoption of new cyber secure software and systems is a very attractive one. If such a model was successful, it would be useful in reforming possible changes in procurement and operational concept transformation in DOD as well. The community has felt a great deal of enthusiasm about this potential outcome. The outcome we feel would be best achieved if the research centralized in the S&T Directorate at HSARPA interacted directly with the procurement and operational needs of the IAIP, Border and Transportation Security, and the Emergency Preparedness Directorates.

However, a necessary condition for an outcome is an adequate outlay of funds for research and development coupled with acquisitions. In my opinion, the level of investment needs to be somewhere in the range of 100 to \$200 million per year, and we base this number on a road map for research and cybersecurity which we have developed and is present in the full testimony. In the interest of time, I will just talk a little bit about a few highlights of the funding gaps in research priorities for cybersecurity.

The technology needs may be classed into the following categories: unsolved difficult research problems and information assurance and survivability—and a number of these are taken from the so-called Infotech Research Council hard problems list, and they are listed in my testimony.

The second one is about technologies for strong security with strong privacy. The technology needs for strong privacy are completely compatible with the technology needs for strong security. So some examples are selective revelation, where the goal is to minimize revelation of personal data while facilitating analysis through the approach of partial incremental revelation of data. Others include strong audit. And also, rule processing technologies for checking compliance with privacy rules.

In addition, I feel that the emerging infrastructure of the future will be based on wired and wireless network devices ubiquitously embedded in the environment to provide so-called sensor webs of information for monitoring and controlling infrastructure. We need to take steps today to start securing them.

And, finally, the last set of problems comes in under the title of validated modeling, simulation and visualization of critical infrastructures and their interdependencies.

Mr. Chairman, am I out of time? Or—

Mr. THORNBERRY. The gentleman's 5 minutes has expired. The Chair is somewhat lenient with time, however. The gentleman may proceed and conclude his remarks.

Mr. SASTRY. Thank you very much, Mr. Chairman. Perhaps in the interest of time, let me sort of say—to go to the last part of my testimony and talk a little bit about a model for public-private partnerships for rapid technology transfer in cybersecurity.

I think there is clearly a need for cybersecurity research and development, but even more immediate and pressing is the need for transitioning this. The most common complaints that one hears from vendors and service providers are as follows: No one pays for security. Will the Federal Government play the role of market maker in the early adoption of security products? Is there sufficient demand to stimulate new companies around new ideas in cybersecurity? Who will provide road maps to help the investment by established companies and the venture community in cybersecurity products?

So a fundamental organizational problem that exists today is the lack of mechanisms for filling in the gap between the end of successful Federal projects. And I feel that a lot of the Federal investment to date has indeed been a success, but there is a problem in transitioning from the end of a successful Federal project to the venture community and industry in the form of products.

Research prototypes need to be hardened, tested on large-scale test beds, informed and customized by the customer base before we get these into the marketplace. And I feel that the role of public-private partnerships and perhaps the nonprofit sector is in filling this gap between the end of a successful research program and industry and venture update.

And let me just conclude by saying that there are exemplars of successful such partnerships which have been formed by the legislation of this Congress, and so those are in the semiconductor industry. In the semiconductor industry, both the SIA, the Semiconductor Industry Association, and the SRC, the Semiconductor Research Consortium, have facilitated both the funding of rapidly transitioned research to the semiconductor industry and led the continual development of road maps for the electronics industry. DOD funding, both from OSD and DARPA from the earliest days of this research, has been instrumental in maintaining a strategic national component both for competitiveness as well as for maintaining U.S. superiority in a vital sector.

My own sense is that nonprofits are the same ilk as the SIA and SRC. With the same kind of partnership, DHS and DOD could play an important role in developing a mechanism for rapid transition of focused research and road mapping for industry in the investment community.

Thank you very much, Mr. Chairman, for your indulgence. Thank you very much for the opportunity to testify. We are really delighted as a community to see your attention to all of these important issues. Thank you very much.

[The statement of Dr. Sastry follows:]

PREPARED STATEMENT OF DR. SHANKAR SASTRY

Honorable Chairman Thornberry, Honorable Ranking Member Lofgren, and members of the subcommittee on Cybersecurity, Science, and Research, thank you for the opportunity to testify today, regarding areas for investment in cybersecurity research and development, priority areas for funding, and the role of university-industry-venture-government partnerships in bringing secure and trusted systems to the

market place. By way of background, I should say that I am currently the Chairman of Electrical Engineering and Computer Sciences at the University of California, Berkeley where I have been a professor for over 20 years. I have also served on the faculties of the Massachusetts Institute of Technology (1980–1982), where I began my academic career as an Assistant Professor, and Harvard University where I was a Gordon Mc Kay chaired professor in 1993–1994. From November 1999 to March 2001, I served as the Director of the Information Technology Office (ITO) of the Defense Advanced Research Projects Agency (DARPA) in the DoD. The responsibilities of this office included planning and managing the investment in all areas of information technology, including the information assurance and survivability portfolio of programs. My areas of research are embedded and autonomous systems and software, complex infrastructure systems, secure networked embedded systems, and high confidence systems and software. I have recently led the organization of a collaborative multi-university cybersecurity research consortium named, and a testbed for network defense called the national cyber Defense Technology Experimental Research network (DETER).

To answer the questions asked by you, I will divide my testimony into the following areas:

1. Current Funding of Cybersecurity Research,
2. Research Gaps and Funding Priorities for Cybersecurity Research,
3. A collaborative university research program in Ubiquitous Secure Technologies led by Berkeley partnered with Stanford, Cornell, Vanderbilt, Carnegie Mellon, and San Jose State Universities, and Smith College,
4. Testbeds for Cybersecurity,.
5. A model for public-private partnerships for rapid technology transfer in Cybersecurity

1 Current Funding of Cybersecurity Research

There has been Federal funding of Cybersecurity research thus far primarily by the Department of Defense and the National Science Foundation, though there has also been some research funded by NIST, Department of Energy and NASA as well. The community has followed with interest the testimony given by the DARPA Director, the NSF Director and Undersecretary for Science and Technology at DHS to the House Science Committee. The community feels grateful to the House Science Committee, its staff and its Chairman, the Honorable Mr. Bohlert, as well as this Subcommittee on Cybersecurity, Science and Research and Development, its Chairman, the honorable Mr. Thornberry and ranking member the Honorable Ms. Lofgren for their close attention to the needs of cybersecurity research. I will limit my own remarks to the perceptions of the community and also my own experience with helping to manage the cybersecurity portfolio at DARPA.

Department of Defense. The most sustained funding for cybersecurity research to date has been through DoD. In DoD, the largest pool of funding for research has been through DARPA, though there have been important research initiatives that have been managed by the National Security Agency. Some very important University Research Initiatives in Critical Infrastructure Protection (CIP-URI) were funded through DDR&E as five-year programs primarily in 2001. Modest 6.1 core programs in cybersecurity research at AFOSR, ARO and ONR also exist. The Information Assurance and Survivability (IA&S) programs at DARPA are the largest and most successful Federal investment to date. This suite of programs has gone through three generations listed below with some exemplars of successful outcomes:

1. 1st Generation (Prevent Intrusions): Trusted Computing Base, Access Control, Cryptographic Tools, Multiple Levels of Security
2. 2nd Generation (Detect Intrusions, Limit Damage): Firewalls, Boundary Controllers, Intrusion Detection Systems, Virtual Private Networks, Public Key Infrastructure
3. 3rd Generation (Operate Through Attacks) Goals are Intrusion Tolerance, Graceful Degradation, Big Board View of Attacks, Security Tradeoffs and Metrics, and hardening of the core infrastructure.

The first generation was aimed at preventing intrusions as much as possible, the second generation with detecting intrusions when they occur and limiting the amount of damage that they cause. The third generation of programs, which is most critical to critical infrastructure protection, consists of developing the ability to operate through attacks without failing catastrophically. A very large number of existing security solutions were developed by companies either as spin-offs of DARPA research or as an integral part of DARPA research programs in Generations 1 and

2. We are currently in the 3rd generation of programs and a research and development base has been energized to address what remain as difficult technical problems in IA&S. From its high watermark of close to \$ 100M of funding for IA&S in 2000, the funding for unclassified IA&S research at DARPA has decreased significantly in following years. The DARPA investment has also had the extremely desirable effect of involving the Service Laboratories (such as AFRL and Navy SPAWAR), and the services operational commands in bringing their requirements to the community. While it is understandable that there are other important priorities in the DoD for more focused efforts in IA&S for command and control and other sensitive DoD networks, given the scope and magnitude of research that remains to be done in cybersecurity, it is critical that the burden of supporting cybersecurity research be picked up by other agencies. In addition, given the important strategic nature of IA&S research for new and emerging DoD systems, including the newest generations of unmanned and autonomous systems (such as the UCAV and in Future Combat Systems), it would not be in the interests of DoD to scale back its unclassified programs a great deal.

National Science Foundation NSF has been proactive in taking steps to boost funding for cybersecurity research by setting up new programs in Trusted Computing and in Secure Network Embedded Systems (under planning), networking research, and testbeds for cybersecurity. These investments, primarily in the Directorate of Computer and Information Science and Engineering (CISE) have been timely and strategic. Nonetheless it is the perception of the community that the level of funding for cybersecurity and Critical Infrastructure Protection could be greater. A point about the synergy between funding between DARPA and NSF is in order here. From the early days of networking when NSF picked up the ARPA net and helped fund it while it grew into the modern Internet, and early DARPA funding on high performance computing was sustained by NSF funding, there has been a rich legacy of cooperation in funding information technology research between the two agencies on Fairfax Avenue in Arlington, Virginia. It would be extremely desirable to have this synergistic relation continue in the area of cybersecurity.

Department of Homeland Security. It is our understanding that the Science and Technology Directorate of DHS is planning its initiative in cybersecurity and is organizing program management structures for cybersecurity research centers. The Congress and the administration should be lauded for having taken the visionary step of having formed the Homeland Security Research Projects Agency along the DARPA model. In addition, the idea of having HSARPA work along with procurement and operational branches of the DHS to evangelize the adoption of new cybersecurity software and systems is a very attractive one. Such a model, if successful, would be very useful in informing possible changes in procurement and operational concept transformation at the DoD as well. The community has felt a great deal of enthusiasm about this potential outcome. The outcome would be best achieved if research centralized in the Science and Technology Directorate, at HSARPA, interacted directly with the procurement and the operational needs of each of the Information Analysis and Infrastructure Protection (IAIP), Border and Transportation Security, and the Emergency Preparedness Directorates. There are some synergies to be gained for example by engaging with the research needs of the National Communication Systems, with road-mapping activities for cybersecurity, or by using secure sensor webs for border patrol and monitoring programs

However, a necessary condition for such an outcome is an adequate outlay of funds for basic research and development coupled with acquisitions. In my opinion the level of investment needs to be somewhere in the range of \$100–200 M per year. I base this number on a roadmap for research in cybersecurity, which we have developed (details are included in the next section of this testimony). I feel that the DARPA model is an especially appropriate model for funding research and development in cybersecurity. Once again HSARPA may wish to involve groups in the other directorates the way DARPA involves service laboratories and commands as “agents” for contracting the work and thereby helping the transition of research into products. Thus, one could view customers in the IAIP Directorate helping program managers in HSARPA shape the programs for their needs. While HSARPA will need to have programs that have short term and intermediate term payoff, one can visualize the role of the NSF in helping HSARPA as an executive agent in its early years while it is being fully configured. In the steady state a relationship between HSARPA and NSF along the lines of the DARPA–NSF model would be highly desirable, with NSF providing longer term sustained funding.

Other Agency Funding for Cybersecurity. Since the needs of different mission agencies in cybersecurity are somewhat different it would be important to have funding

from NASA, DoE, and other mission agencies for their own needs. Additionally the role of the National Institute of Standards and Technology (NIST) could be an important one in managing testbeds, whetting and developing cybersecurity standards and best practices. NIST has also been an important executive agent for managing DoD programs and could continue to do so for DHS.

2 Funding Gaps and Research Priorities for Cybersecurity

The technology recommendations for suggested areas of funding given here were developed by a group of researchers, industry participants and the venture community over the last two years in a series of workshops, meeting and studies:

1. 25th June 2002, Meeting with a large sample of participants from Venture firms, DoD; OSD, DARPA, ONR, NSA, the President's Critical Infrastructure Protection Board, large industry participants such as IBM, HP, Oracle, Symantec, Microsoft, Intel, non profits such as SRI, I3P, hosted by me in Palo Alto
2. 18th September 2002, Meeting with industry leaders and Mr. Richard Clarke Head of the President's Cyber Security Protection Board on the details of the Presidential Cybersecurity Plan held at Palo Alto.
3. 19–20 September 2002. Sztipanovits (Vanderbilt), Stankovic (Virginia), and I ran the NSF/OSTP workshop on New Technologies for Critical Infrastructure Protection and Cybersecurity in Leesburg, Virginia with technology recommendations for the White House Office of Science Technology and Policy. OSTP report of this workshop will be released shortly.
4. October 7–8 Workshop on Testbeds for Security, Squires (Chief Scientist of HP) led a meeting on networking research testbeds.
5. August 2001, NSF Workshop on New Directions in Security, Doug Tygar, Berkeley
6. August 2002, DARPA Information Sciences and Technology study on Security with Privacy, Doug Tygar.

While the whole list of participants is too long to list, I would especially like to acknowledge the help of former colleagues at DARPA, Terry Benzel, Doug Tygar, and Ruzena Bajcsy of the University of California Berkeley, Janos Sztipanovits of Vanderbilt University, Jack Stankovic of the University of Virginia, Teresa Lunt of PARC (formerly Xerox PARC), Pat Lincoln and Victoria Stavridou of SRI, Patrick Scaglia and Steven Squires of HP, Robert Morris of IBM, David Tennenhouse of Intel, Jerry Fiedler of Windriver Systems for their help in developing these recommendations.

Computer trustworthiness continues to increase in importance as a pressing scientific, economic, and social problem. The last decade has seen a rapid increase in computer security attacks at all levels, as more individuals connect to common networks and as motivations and means to conduct sophisticated attacks increase. In today's environment there is heightened awareness of the threat of well-funded professional cyber hackers and the potential for nation-state sponsored cyber warfare. Cyber attacks are increasingly motivated by the financial gain and global politics. A parallel and accelerating trend of the last decade has been the rapidly growing integration role of computing and communication in critical infrastructure systems, such as financial, energy distribution, telecommunication and transportation, which now have complex interdependencies rooted in information technologies. These overlapping and interacting trends force us to recognize that trustworthiness of our computer systems is not an IT issue anymore; it has a direct and immediate impact on our critical infrastructure. Security is often a collective enterprise, with complicated interdependencies and composition issues among a variety of participants. This poses a challenge for traditional competitive economic models. Clearly there is an acute need for developing much deeper understanding of and scientific foundation for analyzing the interaction between cyber security, critical infrastructure systems and economic policy.

The fundamentals of reliable infrastructure have not been adequately worked out for complex networks of highly interacting subsystems, such as the power grid and the airspace-aircraft environment. These are complex, often dynamically reconfigured, networks. The primary challenge for future generations of these systems is to provide increasingly higher efficiency, while assuring joint physical and logical containment of adverse effects. Increasingly, autonomous but cooperative action is demanded of constituent elements. Examples include the technology needed to support aircraft in high-capacity airspace, enabling the execution of parallel landing pat-

terns under terminal area control. A deregulated power grid draws new market participants. These new players may produce highly variable efficiency, potentially adverse environmental effects, and they may pose hazards to system-wide stability. This trend towards autonomous, cooperative action will continue, with the demands of current and next-generation systems for open, interoperating, and cooperating systems. The achievement of a satisfactory level of interoperable functionality is both enabled by, and dependent upon, advances in information and control infrastructure for coordinated operation. Furthermore, entirely new capabilities, such as networks of devices for pervasive sensing and actuation are becoming viable, and the control and communication technologies for their effective use must be fully developed and integrated into distributed infrastructure systems.

Although reference frequently is made to the next generation of technologies as “intelligent agent” systems or self-healing or self-reconfiguring or autonomic systems, this terminology conceals a complex of carefully integrated systems and software concerns. There is no panacea; services must be carefully engineered from the ground up in order to safely support a facade of highly autonomous action. Advances in software and information technology have improved the potential for a better substrate for future, more reliable infrastructures. The technology needs may be classed into the following categories:

1. Unsolved Difficult Research Problems in Information Assurance and Survivability. The areas of research highlighted here are:

- a. Intrusion and Misuse Detection: methods need to be automatic, predictive, have a low false alarm rate, and possibly identify the adversary.
- b. Intrusion and Misuse Response: methods should provide a shared situational awareness, automatic attack assessment, a dynamic reconfiguration of the system and possibly an automated counter attack.
- c. Security of foreign and malicious code: desired attributes for systems that protect against malicious mobile code include confinement of access and capability and encapsulation of the code.
- d. Controlled sharing of information: the ability to dynamically authorize the sharing of information and automated data tagging.
- e. Distributed Denial of Service (DDoS) and Worm Defense: solutions are needed for modeling, measurement and analysis of attacks, detection of the attacks, attribution, dissipation of the attack, and possible retribution.
- f. Secure Wireless Communications
- g. New and Emerging Challenges
 - i. Peer to peer computing
 - ii. Security in ubiquitous and nomadic computers
 - iii. Human factors and ergonomics in security
 - iv. Networks surveillance and hygiene
 - v. Insider threat detection, monitoring and response

2. Technologies for Strong Security with Strong Privacy

- a. Selective Revelation: the goal here is to minimize revelation of personal data while facilitating analysis through the approach of partial, incremental revelation of data.
- b. Strong Audit: the goal here is to protect abuse by watching the watchers: everyone is subject to audit, there is cross-organizational audit, and usage records are tamper proof. Possible new technologies include encrypted searches and crypto-protocols.
- c. Rule processing technologies: there is need for a formal language for expressing privacy rules and tools for automated checking of compliance, a privacy toolbar for helping users. A related technology is the one needed for digital rights management

3. Secure Network Embedded Systems. The emerging infrastructure of the future will be based on wired and wireless networked devices ubiquitously embedded in the environment to provide “sensor-webs” of information for monitoring and controlling infrastructure networks. The embedded software, which will be present in these complex systems, needs to have the following attributes:

- a. Automated Design, Verification and Correctness by Construction. A large number of infrastructures suffer from being difficult to configure correctly and the resulting glitches are frequently as serious as cyber attacks. In addition they need to be fault tolerant: such systems are referred to as High Confidence Systems.
- b. Layered Security for Embedded Systems: the defenses need to be in depth to protect from attacks from the physical layer up through the applications layer:

- i. Physical Layer: protection from attacks like jamming and tampering
- ii. Link Layer: protection from unfairness and over frequent collisions of packets
- iii. Networks and Routing Layer: protects from attacks due to greed, homing, misdirection and black holes.
- iv. Transport Layer protection from attacks such as flooding and desynchronization.

4. Validated Modeling, Simulation and Visualization of Critical Infrastructures and their Interdependencies

- a. Tools for the assessment of the level of risk
- b. New modeling and simulation tools for complex systems
- c. Development of simulation testbeds for teaming exercises, response preparation and assessment.

3 A Collaborative University Research Program in Ubiquitous Secure Technology

Here I describe a sample collaborative university research program that is focused at research problems in many of the areas described above. It is important to note that activities of this scale need to be engaged in by the scientific community in groups rather than as individual institutions. At Berkeley we have found it important to build such partnerships and consortia for research and development. We have put together a team of some of the strongest research universities led by Berkeley and including Stanford University, Vanderbilt University, Cornell University, Carnegie Mellon University, along with San Jose State University, Smith College, Fiske University to develop a Team for Research in Ubiquitous Secure Technology (TRUST) to radically transform the ability of organizations (software vendors, operators, local and federal agencies) to design, build, and operate trustworthy information systems for our critical infrastructure. TRUST will bring together a research team with proven track record in relevant areas of computer security, systems modeling and analysis, software technology, economics, and social sciences. The research team will be advised and supported by vendors of information technology and critical infrastructure (utility, telecommunication, finance, and transportation) protection providers and stakeholders.

3.1 Technical Research Program

Our multidisciplinary approach allows solutions to emerge from an integrated view of computer security; software technology, analysis of complex interacting systems, and economic policy in the following areas:

Composition and computer security—Computer security attacks today occur on a minute-by-minute basis. Organizations producing individual components, such as routers or central office switches, have increasingly devoted energy to protecting those components against attack. However, protection of individual components does not always result in protection of the entire systems: different machines and different systems running on a single network often have complex interdependencies—and a malicious attacker can exploit those interdependencies for example in denial of service attacks, inter-machine authentication failures, and routing disruptions. Attackers can attack systems where different software programs must interact on a single operating system (examples include e-mail with attachments leading to e-mail worms, buffer-overflow problems caused by unexpected use of software function libraries, and windowing systems displaying bogus, malicious systems messages.) Modularization can increase the problem: when common IT components are integrated with specialized applications and embedded systems, deep knowledge of the underlying computational model is needed to avoid vulnerability. TRUST will bring together an integrated scientific approach to composition and computer security.

Privacy—As a large amount of commercial and communication activity has moved to the Internet and World Wide Web, privacy concerns have increased both for individual users and organizations. Users perceive they have little control over information, and often those perceptions are correct—organizations are unable to accurately describe policy procedures and privacy-information crimes such as identity theft have increased sharply. Even disclosure of apparently innocuous information, such as an e-mail address, leads to unsavory activities, such as spam, which in turn can grow to a magnitude that can cause systemic problems. Organizations also have a need for privacy—not only to protect their customers, but also in cross-organiza-

tional exchanges including auctions and communications. Privacy is a challenging problem because when information is shared (laterally, between organization, or vertically, between different subsystems) each of the individual components involved in the sharing, the mechanism for sharing, and the consequences of the sharing, all present opportunities for invading privacy. Issues related to privacy emerge as a result of interaction between technology and economic policy, such as in online bidding on energy markets or dynamic allocation of the frequency spectrum. To tackle privacy, TRUST will develop solutions to the complex tradeoff between technology, economic policy and security. This will require a new look at the fundamental underpinnings of information management, storage, and retrieval.

Critical infrastructure protection—Critical infrastructure systems are large networks that move energy, information and material. Information technology is used to monitor, control and manage these systems by means of vast networks of computing equipment. Faults caused by natural disasters or malicious attacks can cause these networks to completely fail, leading to widespread damage. Critical infrastructure protection requires making systems that are highly robust and available in the presence of hostile attacks. TRUST will approach computer security from a holistic systems view, considering a union of concerns including physical design, performance, power consumption, reliability and others. For example, we don't just consider secure and highly available communication between sensor devices and SCADA (Supervisory Control And Data Acquisition) centers, TRUST will consider the potential impact of feasible security attacks on the power distribution network, and the impact of signal encryption on feedback control loops. Anecdotal evidence and the findings of more systematic red team activities such as the Joint Chiefs' Eligible Receiver program, strongly suggest that the United States is highly vulnerable to attacks on its critical infrastructure—including key utilities (gas, water, and energy), communications services, finance, transportation, medical coordination, government services, and emergency services. Even in a single organization, such as a national telecom service provider, critical infrastructure protection is difficult, because these systems are highly complex and involve so many components that even their designers cannot understand all the interactions. The interaction of different critical infrastructure systems, and their interaction with public (critical or non-critical) systems, creates complex dependencies and control paths. Today, we have no good way of detecting these interdependencies, although hackers have proven themselves highly capable of finding attack opportunities and exploiting subtle vulnerabilities.

TRUST will take a systems view which raises a broad set of trust questions: they range from protecting individual privacy to protecting large complex interacting critical infrastructure, from embedded systems to networks, and they have a strong focus on security problems arising from composition. Not only is a large effort necessary to take the broad view—and to anchor this view in the context of large-scale operational environments - but this work requires strength from a wide variety of disciplines both inside computer science (cryptography, programming languages, distributed systems, networking, human-computer interfaces, logic and model checking, configuration, software engineering, etc.) and outside computer science (economics, policy, law, statistics).

3.2 Economics, Public Policy, Societal Challenges

Solutions to today's problems are an essential requirement to fulfilling the vision of ubiquitous computing. Many of today's security vulnerabilities in networked embedded systems and SCADA are very specialized and hence visible to only a few. However, as society increasingly employs the use of software agents to control and organize multiple aspects of day-to-day life these security vulnerabilities will become impediments to their widespread adoption. A vision for the future of information technology in society, implies that the presence of ubiquitous computing will bring with it access to interfaces that will become part of every day interchange for a wide class of citizens.

Investigations need to be directed so as to lend maximum benefit to social questions such as those in the area of economics and incentives. These are particularly pressing as questions of liability and insurance are moved up in the nations business and legislative agenda. Issues of liability have become an important topic given the cost of security incidents. Economic and legal analysis suggests that a due care standard provides appropriate incentives, but how should the standard be set in practice? Without a clear understanding of sufficient standards or best practices, insurance companies do not have a clear basis on which to offer insurance policies covering security incidents. The interaction between liability, insurance, and care has been

examined extensively in the law and economics literature. However, new questions that arise in the context of information security as “accidents” are often deliberate attacks. Hence an analysis of the incentive of attackers must be better understood and modeled. In addition to these incentive problems, there are also a number of purely economic issues that need to be better understood. How can one quantify the benefits and costs from various security policies? How do public and private security policies interact? What are the nature and size of “transactions costs” associated with security? TRUST will address these questions in the course of our effort. It is anticipated that the research results will provide a solid basis for the establishment of policies, procedures and eventually case law for industry and government in managing the risk of computer security incidents.

3.3 Education and Outreach

American prosperity in the new millennium and increasing national security concerns make it important to increase the number of students who will join the nation’s technical enterprise as researchers. This is crucial in the cyber security space as there is currently a severe shortage of trained scientists (and almost no women and minorities) in the information security field. Additional need arises from our concerns about the “weakest link” of security. If even one user makes a serious error, it can endanger all the systems connected to his or her machines. We have a need to raise the level of security awareness of all people who use computers and depend on their results—namely, all citizens. TRUST brings a strong focus on educational outreach activities through its members many activities. Educational activities will be integrated with TRUST research, through graduate programs, summer programs and directed research projects with under represented educational institutions.

4 Testbed Research

As discussed earlier, over the past ten years, there has been an increasing investment in research aimed at developing cyber security technologies, by government agencies (NSF, DARPA, DoD) and by industry. However, the Nation still lacks large-scale deployment of security technology sufficient to protect our vital infrastructure. One important reason is the lack of an experimental infrastructure for developing and testing next-generation cyber security technology. Neither existing research network infrastructures (Abilene, vBNS) nor the operational Internet meet this need, due to the inherent risks of testing malicious behavior in operational networks. New security technologies have been tested and validated only in small- to medium-scale private research laboratories, which are not representative of large operational networks or of the portion of the Internet that might be involved in a security attack.

To fill this critical gap, we will build an experimental infrastructure network to support the development and demonstration of next-generation information security technologies for cyber defense. This cyber Defense Technology Experimental Research Network (DETER Network) funded jointly by the National Science Foundation under its Networking Research Program in Computer and Information Sciences and Engineering (CISE) directorate and the DHS Science and Technology Office will provide the necessary infrastructure networks, tools, methodologies and supporting process—to support national-scale experimentation on emerging security research and advanced development technologies.

Once again, we at Berkeley have led in putting together a broad based coalition of partners including the University of California Davis, University of Southern California-Information Systems Institute, Network Associates Laboratories, SRI, Menlo Park, the Pennsylvania State University, Purdue University, Princeton University, University of Utah, and industrial partners Juniper Networks, CISCO, Intel, IBM, Microsoft, and HP. The DETER project will create, operate, and support a researcher- and vendor-neutral experimental infrastructure that is open to a wide community of users. Furthermore, the DETER project will apply scientific benchmarks and measurements to both the creation of the experimental infrastructure itself and to validation of the experimental results. Two important defenses that we will develop on this testbed are:

1. Distributed Denial of Service Attacks—One major objective of the DETER network is to make scientific advancements in 1) understanding the effects of sophisticated, large-scale DDoS attacks and 2) defending against them. Techniques and soft-

ware capable of disabling large portions of the Internet for hours or days could be developed relatively easily today by sophisticated hackers or nation states. However, because such an attack has never been observed “in the wild”, the scientific and operational communities’ understanding of the underlying scientific phenomenon is at best fragmentary and speculative. Internet infrastructure components that are pushed to their limits by such attacks may exhibit non-linear or unstable behaviors that diverge from predictions derived from models, simulations, overlay networks, and scaled down demonstrations. As a result, we cannot accurately predict the impact of a large-scale attack on different points in the Internet topology. We plan to conduct experiments to improve understanding of the scientific phenomenon of a sophisticated large-scale DDoS attack. with special attention paid to the following factors:

- Detection—What kinds of DDoS attacks can the mechanism detect, how accurately, and under what conditions?
- Mitigation—What kinds of DDoS attacks can the mechanism mitigate (via blocking or rate limiting), how effectively, at which locations in the networks, and under what conditions?
- Autonomy vs. Coordination—To what extent does the mechanism’s effectiveness depend on deployment in multiple locations with communication and coordination across locations, and how effective can the mechanism be if such coordination is not possible?
- Collateral Damage—To what extent does the mechanism impede benign traffic, and under what conditions, i.e., does it do more harm than good?

2. Worm Defenses—Worms present a substantial and growing threat to the Internet and to large government and commercial enterprise networks. The recently released SQL Slammer (Sapphire) worm provided a stark illustration of the dramatic speed and potential impact of a simple worm, spreading to more than 75,000 hosts within ten minutes and causing ATM failures, airline flight cancellations, and widespread network outages. The DETER Network can play a crucial role in supporting study of the behavior of these worms and evaluation of new worm defense technologies. Worm behavior is currently only poorly understood. Through testbed experimentation, researchers can study different models of worm propagation (e.g., random scanning, target-list, coordinated, hybrid) and their effects on propagation rates in a realistic network environment. They can further study effects of the network congestion caused by worm propagation through a large network, determining how such congestion affects legitimate applications and the worm itself as infection spreads.

5 A Model for Public-Private Partnerships for Rapid Technology Transfer in Cybersecurity

The issues in transitioning cybersecurity research and development are immediate and pressing. There has arguably been a market failure in bringing cybersecurity technologies to the market. The most common complaint that one hears from vendors and service providers run something like: “No one will pay for security.” or “Security is every one’s second most favorite priority”, or “Security products suffer from the paradox of the common good”. “Will the Federal government play the role of market maker in early adoption of secure products?” “Is there sufficient demand to stimulate new companies around new ideas in cyber-security?” “Who will provide roadmaps to help the investment by established companies and the venture community in cyber-security products?” However, there is reason to feel optimism for change, provided that some steps are taken immediately. Experience gained from the national response to the potential perils of the Y2K conversion are worth revisiting in the context of cybersecurity, with especial attention to the role of the mandatory SEC filings for corporations to explain their Y2K strategy.

A critical issue for cybersecurity is the ability to quickly transition products from the laboratory and the research community to industry. A fundamental organizational problem that exists today is the lack of mechanisms for filling in the gap between the end of a successful Federal research program and the investment by the venture community and industry in products. Research prototypes need to be hardened, tested on large scale test beds, informed, customized and modified in response to the needs of a diverse set of customers before they can attract capital to allow them to be integrated into products. In addition industry, especially systems integrators and the larger IT companies would benefit from roadmaps informed by this technology transition. The term public-private partnerships is used to describe the need for cooperative arrangements among academia, industry, venture capital, and government with individual stake holders in the infrastructures to bring the newest

products to the market place and then to the infrastructure stake holders. It is important for the research and development community to play a role in developing the relevant non-profits and trade groups to pursue transfer of ubiquitous secure technology. It is important for us to continue to hold focused workshops and seminars on particular topics relating to infrastructure protection and cyber-security. Research and Development will need to learn and evolve with results, using an iterative investigate-develop-educate-apply cycle. It is critical to develop science, technology and proof of concept prototypes that will be tested through models that emerge from a series of analytical and case studies, experimentation and simulations. For example, through participation with the Secret Service's New York City and San Francisco Electronic Crimes Task Force it has been possible for the cybersecurity research community to develop an understanding of the needs of cybersecurity for the financial community.

A success story in public private partnerships, which has all the hallmarks that would be desirable for cybersecurity, is in the area of semiconductor manufacturing. The Semiconductor Industry Association (SIA) and Semiconductor Research Consortium (SRC) are fine examples of non-profit organizations, which have facilitated both the funding of rapidly, transitioned research to the semi-conductor industry and led the continual development of roadmaps for the electronics industry. DoD funding, both from the OSD and DARPA, from the earliest days of this research has been instrumental in maintaining a strategic national component both for competitiveness and also for maintaining US superiority in a vital industry sector. My own sense is that non-profits of the same ilk as the SIA and SRC, with the same kind of partnership with DHS and DoD, could play an important role for developing both a mechanism for rapid transition of focused research and road mapping for industry and the investment community. Once again, I feel here that for strategic national security reasons that DoD partner with DHS in co-funding such ventures.

6 Concluding Remarks

Thank you Mr. Chairman and Committee members for the opportunity to provide this testimony to the House Subcommittee on Cybersecurity, Science, Research and Development, of the Committee on Homeland Security. We laud you for holding this very important set of hearings and for engaging in a matter of deep national and homeland security. The research community offers the Subcommittee our full support and cooperation, and every success in your deliberations.

Mr. THORNBERRY. I thank the gentleman. And I neglected to say at the outset that each of your full statements will be made part of the record. And also, let me compliment each of you on your full written statements, because they did a very good job of directly addressing the questions in which this subcommittee is interested, and I appreciate that very much.

Let me now turn to our next witness. Dr. Steve Bellovin is a member of the National Academy of Engineering at the National Research Council. He is also a technical leader and fellow from AT&T Laboratory. Dr. Bellovin, thank you for being with us. And you are now recognized for 5 minutes.

STATEMENT OF STEVEN BELLOVIN, PH.D., TECHNICAL LEADER AND FELLOW, AT&T LABORATORY

Mr. BELLOVIN. Thank you, Mr. Chairman, Ms. Lofgren, and members of the committee. I am delighted to come to help you.

I should add, one of my other roles, I am Security Area Director for the Internet Engineering Task Force, which is the group responsible for most of the standards used on the Internet today.

We face a very serious cybersecurity problem. Usually we can protect an individual high-value system, though it is hard. I run my own personal computers as tightly as I know how to; in the last 2 years, probably there were a dozen different ways that, if some-

one sent me the right message at the right time, they could have taken over this system. And this is run about as tightly as anything can be and still be connected to public networks.

We cannot protect all of the machines, and we simply don't know how to. We don't even know what the magnitude of the threat is even from ordinary hackers, let alone nation states and possible cyber terrorists. The available data on what kinds of attacks, on the number of attacks, is simply lacking. We need more research to help us understand what is going on, because you need different defenses against cyber terrorists than you do against ordinary hackers.

Most of the security problems we see today are caused by buggy software. Buggy software is probably the oldest unsolved problem in computer science. I have no reason to think it is going to be solved in my professional lifetime. If we design a software correctly, though, we can restrict our attention to the crucial pieces for security and probably get those rights. Software reliability has improved. It is no longer unusual to see a server that has been up for a year or more. But we have to design software with that sort of division in mind. We know somewhat of how to do that, but not nearly enough.

We need new mathematical formal frameworks for assessing and measuring the security of a system. A locksmith can tell you how long a safe can resist an attack with certain kinds of tools. A computer scientist can't do the same.

Pure research on cryptography, basic research on cryptography is probably not a priority. It is not that cryptography is not important—I have done a lot of cryptographic research myself—but we have far more science there than we have currently applied. We need a great deal of effort on technology transfer from the theoreticians to the practitioners; and on engineering, taking the cryptographic mechanisms and actually engineering them to be used on deployed systems.

I would note that open standards are better for this because they promote diversity. The lack of cyberdiversity, like the lack of biodiversity, leaves us very vulnerable to a single infection vector, a single attack vector. This is a very serious issue in the computer industry today, because many other trends push towards one source rather than many.

If we have all the security technologies, it is often too hard to use. We need to do a lot of work on the human factors of computer security. Most people don't configure the systems securely because, frankly, it is too hard to do so. I find it hard sometimes myself, and I am a professional in this field, trying to understand some of the messages and prompts that I get.

We need incentives for vendors to develop more secure systems. That is, both security features and more reliable, less buggy software. And we need incentives for end users to use these secure systems and these secure features.

We need to improve systems administration. This isn't a sexy area, but most actual penetrations are caused by failure to apply available patches to correct known vulnerabilities. It is once the patch comes out that most of the activity takes place. Not always, but that is the large, vast majority of system penetrations. But no

responsible system administrator will patch a production system without testing it. System administration is not a prime area for research; it seems too mundane. Nevertheless, if we can have better tools for automating the administration, for testing systems, and, by the way, for improving the resources available to system administrators both in government and in industry, this has got the potential for a very large payoff. This is some low-hanging fruit.

Security also depends on authentication. Authentication is a subtle business. It is hard to get right. If you get it wrong, you may have a system failure, you also violate individual privacy. It is important to pay attention to both of these factors when designing systems.

There are no simple answers to the cybersecurity problem. There is no one technology that is going to solve it for us. There are a number of areas, however, that if we put in the appropriate resources, I think we can make a lot of progress and get systems not absolutely secure—there is no such thing—but markedly more secure than they are today.

Thank you, Mr. Chairman, Ms. Lofgren, members of the committee.

Mr. THORNBERRY. Thank you, Doctor.

[The statement of Mr. Bellovin follows:]

PREPARED STATEMENT OF MR. STEVEN M. BELLOVIN

Cybersecurity Research Needs

1. Introduction

It is quite clear that cybersecurity is vital to our nation's safety. A wide variety of National Research Council reports, summarized in *Cybersecurity Today and Tomorrow—Pay Now or Pay Later* [1], have illustrated the threat in no uncertain terms.

Although there are things that the information technology profession—software vendors, network operators, and end user sites—can and should do today to improve computer security, the simple fact is that there are limits on how good a job it can do. Even with unlimited financial resources, and the best will, we could not do an adequate job. Quite simply, we do not know how to mount an adequate defense. It is usually possible to protect an arbitrary resource; it is not currently possible to protect all critical resources.

2. Threats

The types of defenses that are necessary depend on the nature of the likely attacker. Schemes that will keep out the stereotypical “hacker”—i.e., the bored teenager with too much time and too few morals—are not very effective against a nation-state. The former typically use tools downloaded from someone more competent; the latter could develop its own custom tools, and combine them with physical world techniques such as “the three B—bribery, blackmail, and burglary”—or terrorist attacks.

We do not have an adequate categorization of the threat model. Too little research has been done on who launches what kind of attacks. It isn't an easy thing to do; apart from the fact that most attacks are never detected, many organizations are reluctant to disclose their vulnerabilities. But we need to know the attackers' capabilities if we are to devise adequate defenses.

3. Basic Research Questions

Most computer security problems are caused by buggy software [3]. It would be naïve to assume that the problem was solvable now, when it hasn't been solved despite efforts stretching for more than 50 years. Nevertheless, we must continue to focus effort on it. If nothing else, the need now is to solve a subtly different problem: making a small subset of software correct, rather than software as a whole. We may

be able to achieve it; today's operating systems are far more reliable than those used a generation ago.

However, if we are to focus our efforts on the critical software, we must learn how to divide up systems appropriately. We have long known how to do that for operating systems, but many of today's problems come from faulty applications. More generally, we must learn how to build secure systems from insecure components, just as we can produce highly reliable computer systems from unreliable electronic parts.

We need new formal frameworks for analyzing the security of a system, and for specifying its security behavior. We do not have adequate tools for understanding how "strong" a computer system is; at best, we can say that some system can more or less do certain things reliably. By contrast, civil engineers can tell you how much weight a bridge can hold, while locksmiths can tell you how long it will take to break into a safe using a specified set of tools.

Formal, mathematical statements have proved to be powerful tools in some areas of computer science. We need to be able to apply them to computer security issues.

Although basic cryptographic research is important and should be continued, it is not a high priority. As noted, most penetrations cannot be prevented by cryptographic means. It is more important to do a better job using the cryptographic science we have. Note that I say this as one who has published more than a dozen cryptographic research papers.

Most basic research work is done at universities. But it is not possible to scale up the amount of basic security research very quickly. There are not that many professors who are capable of doing such work; there is a limit to how much money each one can profitably use.

4. The Need for Engineering

Although, as noted, there is a need for more basic research, a great deal of prior research has not yet been translated into practice. For example, we have far more cryptographic science than we have network protocols that use this science. We need to support technology transfer to industry groups and standards organizations; we cannot protect our infrastructure with theoretical constructs. (I note that open standards are better; apart from the "many eyes" notion, with open standards there can be multiple independent implementations of the same function. The National Research Council noted that the lack of diversity in platforms was a major risk factor [3].)

More subtly, much security technology is not employed because it's too hard to use. We need research in the human factors of security technology.

Assuming that industry does the necessary cryptographic and human factors engineering, the results must be translated into practice. This may require incentives for software vendors to develop the code, and for end users to employ it.

As noted earlier, most security holes are due to buggy code. That is bad enough; what is worse is that most penetrations exploit bugs for which patches are available but have not yet been applied. The cause is not laziness or incompetence by systems administrators; rather, it's reflective of the immense difficulty of the systems administration task. Patches have a higher bug rate than base code, and may thus be more likely to create new security holes; beyond that, a remarkable amount of code functions because of an implicit reliance on some underlying bug that was present on the development systems. Fixing a bug may, as a side-effect, disable essential applications. No responsible systems administrator will install a patch on a production system without extensive testing, but this behavior leaves the machine vulnerable. We need research to solve this dilemma. Systems administration is not a typical research topic; nevertheless, it is the area with the biggest potential payoff for a relatively modest investment.

It is worth noting that systems administration is often a high stress, low status job. Administrators often struggle to perform basic tasks because of inadequate resources. Measures to improve systems administration, in industry and government, would likely have a significant effect on practical computer security.

5. Privacy

Often, computer security depends on proper authentication of authorized users. Authentication technologies, ranging from passwords to biometrics, are subtle and difficult to use properly. Beyond simple issues of correctness, any authentication technology can be used in ways that violate personal privacy [2]. Both research on cybersecurity and deployment of technology should protect privacy to the extent feasible.

6. Conclusions

There are no simple answers to the problem of cybersecurity. What is needed is a combination of basic research, technology transfer, and applications of new and previously known techniques. We, as a nation, cannot afford to neglect the issue.

References

- [1] Computer Science and Telecommunication Board, editor. *Cybersecurity Today and Tomorrow—Pay Now or Pay Later*. National Academies Press, 2002.
- [2] Stephen T. Kent and Lynette I. Millett, editors. *Who Goes There?: Authentication Through the Lens of Privacy*. National Academies Press, 2003.
- [3] Fred B. Schneider, editor. *Trust in Cyberspace*. National Academies Press, 1999.

Mr. THORNBERRY. There are several areas that you mentioned we will certainly come back to in questions.

Finally, we have Mr. Dan Wolf, Director of Information Assurance at the National Security Agency. Members will remember that Mr. Wolf has helped us before. Really, the first activity of this subcommittee was kind of a Members-only workshop on cybersecurity which Mr. Wolf put on for us.

Welcome back, and we appreciate your being here. You are now recognized for 5 minutes.

STATEMENT OF MR. DANIEL G. WOLF, INFORMATION ASSURANCE DIRECTOR, NATIONAL SECURITY AGENCY

Mr. WOLF. Thank you, Chairman Thornberry, and members of the subcommittee. My name is Daniel Wolf, and I am NSA's Information assurance director.

NSA's Information Assurance Director is responsible for providing information assurance technologies, services, processes, and policies to protect national security information systems. We are also responsible for conducting research and development.

In regards to your theme for this hearing, Cybersecurity—Getting It Right—

Mr. THORNBERRY. Excuse me, Mr. Wolf. Would you pull that microphone just a little closer to you? Some of us are having trouble hearing, including me. There you go. Thank you.

Mr. WOLF. In regards to your theme for this hearing, "Cybersecurity—Getting It Right," I am not sure that NSA has all the answers or we have always got it right, but I am quite confident during our 50 years of deploying communications, and now cybersecurity products, we have learned quite a few lessons. Some people want to keep NSA in a box labeled "for classified information only." They say that NSA's perspective is too narrowly focused on national security systems. However, I believe quite to the contrary. It has been my experience that there is little difference between the cybersecurity that is required for a system processing top secret military information and one that controls a segment of the Nation's critical infrastructure.

The information management principle within the national security community has always been the concept of need to know, but the fundamental information principle for homeland security is need to share. Because the threat always rolls downhill; that is, our adversaries will always attack the weakest link. Information must be protected across the entire system. A three-sided castle is not very safe. The entire community must share the same standards if we are to protect everyone on all four sides of the castle.

Your invitation to this committee outlined a number of areas where you wanted some specific comments and answers. The first was in technical approaches to optimize cybersecurity. I believe that the highest payoff for optimizing cybersecurity would be creation of an interoperable authentication system deployed widely throughout the Federal, national security, first responder, and critical infrastructure community. This authentication system also forms the basis for all of the other cybersecurity services.

It is also important to note here that the most critical infrastructures like this PKI should be built using U.S. technology. I have concerns with foreign software, unknown trust and quality, being integrated into critical U.S. systems.

My next priority to cybersecurity is effective border protection. Just like our national borders or the perimeters of our buildings, we need to protect our cyber borders. Effective border protection includes many different technologies, including firewalls, virtual private networks, high-assurance guards, and of course intrusion detection.

It has also been estimated that over 90 percent of all successful attacks on DOD systems are against known vulnerabilities. System operators struggle to keep up with all the patches that are issued each month. A system left unpatched soon becomes a target like an unlocked sports car with the keys in the ignition. Therefore, we need an automated patch management system.

Your second question dealt with advanced technologies and should they be pursued to outpace attacks. Today, most of the information coordination during a cyber attack occurs at the speed of humans. Code Red infected 50,000 machines in an hour. We need the ability for networks to work together automatically to weather such an attack.

Another significant research topic is attack attribution, the capability to geolocate and identify the source of attacks. Without confident knowledge of who and where an attack was mounted, it is impossible to decide on the appropriate response. A rapid and reliable capability that separates nuisance hackers from more serious threats could increase the overall effectiveness of every cybersecurity practitioner in both the government and the private sector.

Areas needing higher priority and funding. There is little coordinated effort today to develop tools and techniques to effectively and efficiently examine either source or executable software in large applications. We need a national software assurance center to pull together representatives from academia, industry, Federal Government, national labs, the national security community, sharing techniques to solve this growing threat. It could liken us to the Manhattan Project that was mentioned earlier. This is a significant problem, I believe.

In today's environment, the need is particularly acute for ways to counter security vulnerabilities found in popular commercial operating systems. While many of these vulnerabilities can be fixed by properly configuring the system, the goal is to configure these systems to be as secure as possible right out of the box. I am happy to learn from your last hearing that some equipment vendors are now offering the security standards as the default configurations.

NSA, working with DISA, NIST, the NIPC, the former NIPC, the FedCert, SANS, CIS, developed a set of consensus benchmark security standards. These standards provide a sort of, if you want to call it, preflight checklist of security settings. The benchmark standards represent an effective model based on agreement between and among security experts. NSA is proud to be part of this project and will continue to support the community in establishing security standards.

The fourth area was in the role of transfer among government, academia, and industry. NSA requirements for cybersecurity products for national security uses are identical to the requirements found in other mission-critical systems; for example, homeland security and a critical infrastructure protection. We have developed a number of programs leveraging commercial information technology. My written statement provides the details, but let me just highlight a few of these programs.

The National Information Assurance Partnership, or NIAP, is a U.S. Government initiative designed to meet security testing, evaluation, and assessment needs of both information technology producers and consumers.

Another is the NSTISSP 11. This is a national security community policy requiring the acquisition of information assurance products that have been validated in accordance with either common criteria or other approved methods.

Another is the Centers of Academic Excellence in Information Assurance Education. This program promotes higher education and information assurance, and produces a growing number of professionals with IA expertise in various disciplines. Fifteen universities have been designated as centers of academic excellence to date. We need this type of program for our workforce development. We must invest in our future, our people's future.

And the next area is perspective on leveraging national security standards for homeland security. The key to success for protecting the homeland is secure interoperability. NSA has created a number of secure interoperability standards for national security use that are directly applicable for homeland security and public safety. Some sectors are already adopting these standards. If we are going to share information, these things are extremely important.

In conclusion, it has been my pleasure to share the work of my agency with the committee today. I believe that much of the research and development initiated by NSA for use in the national security community is directly transferrable to the needs of homeland security. We must change our fundamental assumptions from "need to know" to "need to share." We must share policies and processes across the community. Cybersecurity products and technologies have been the focus of my remarks today, but technology alone will never be good enough to protect us. It is ultimately getting cybersecurity right is more about what you do than what you buy.

Thank you for the opportunity to speak to you today.
[The statement of Mr. Wolf follows:]

PREPARED STATEMENT OF MR. DANIEL G. WOLF

Thank you Chairman Thornberry and the members of the Subcommittee. I am honored to be here and pleased to have the opportunity to speak with your committee to discuss cybersecurity research from the point of view of the National Security Agency as we conduct our mission to address threats to the security of critical U.S. Government information systems.

I also would like to thank the Chairman and other members of the Subcommittee for their strong interest and attention to this vital area. In my opinion, your leadership is important for raising awareness of the serious security challenges we all face in our age of interconnected, inter-dependent digital information networks.

My Name is Daniel Wolf and I am NSA's Information Assurance Director. NSA's Information Assurance Directorate is responsible for providing information assurance technologies, services, processes and policies that protect national security information systems. We are also responsible for conducting the research and development of information assurance technologies and systems.

I would like to note that NSA's Information Assurance Directorate and its predecessor organizations have had technical and policymaking responsibility regarding the protection of national security telecommunications and information processing systems across the Executive Branch since 1953.

In regards to your theme for this hearing: "Cybersecurity—Getting It Right." I am not sure that NSA has all of the answers or that we always have gotten it right—but I am quite confident that during our 50 years of deploying communications and now cyber security products we have learned quite a few lessons. We have had tremendous successes and our share of failures. We also have gained a deep understanding and respect for the challenges the nation must overcome to begin to tame cyberspace.

Some in government and industry want to keep NSA in a box labeled "for classified information only." They suggest that NSA's perspective is much too narrow due to our focus on the stringent requirements of national security systems. However, I believe quite the contrary. It has been my experience—and my testimony will soon address—that there is little difference between the cybersecurity that is required for a system processing top-secret military information and one that controls a segment of the nation's critical infrastructure.

Both systems require the element of assurance or trust. Trust that the system was designed properly. Trust that it was independently evaluated against a prescribed set of explicit security standards. Trust that it will maintain proper operation during its lifetime, even in the face of malicious attacks and human error. It has been my experience that effective cybersecurity must be baked into information systems starting at the R & D phase. Trust cannot be sprinkled over a system after it is fielded.

Homeland security presents another reason to suggest that cybersecurity requirements must converge. The information management principle within the national security community has always been the concept of need-to-know. But the fundamental information principle for homeland security is need-to-share. With need-to-share we must develop technical solutions for secure interoperability that may be called on to tie top-secret intelligence systems to a local first responder system.

Because the threat always rolls downhill, that is to say, adversaries always attack the weakest link. Information must be protected across the entire system. A three-sided castle is not very safe. Therefore, I contend that in almost all cases the cybersecurity requirements found in national security systems are identical to those found in e-commerce systems or critical infrastructures. It follows then that the research challenges, security features and development models are also quite similar.

With these similarities in mind, NSA has been working hard to converge these cybersecurity markets through a series of programs and research initiatives. Our goal is to leverage our deep understanding of cyber threat and vulnerability in a way that lets us harness the power and innovation provided by the information technology industry. We believe that the resulting cybersecurity solutions will protect all critical cyber systems, regardless of the information they process.

I think it will be useful for me to provide a brief description of NSA's cybersecurity responsibilities and authorities. I will then turn to the specific questions you asked me to answer in your invitation.

NSA Information Assurance Background

When I began working at NSA some 36 years ago, the “security” business we were in was called Communications Security, or COMSEC. It dealt almost exclusively with providing protection for classified information against disclosure to unauthorized parties when that information was being transmitted or broadcasted from point to point. We accomplished this by building the most secure “black boxes” that could be made, employing high-grade encryption to protect the information. In the late 1970s, a new discipline we called Computer Security, or COMPUSEC, developed. It was still focused on protecting information from unauthorized disclosure, but it brought with it some additional challenges and threats, e.g., the injection of malicious code, or the theft of large amounts of data on magnetic media.

With the rapid convergence of communications and computing technologies in the early 1980s and especially with the explosion of the personal computer, we soon realized that dealing separately with COMSEC on the one hand, and COMPUSEC on the other, was no longer feasible, and so the business we were in became a blend of the two, which we called Information Systems Security, or INFOSEC. The fundamental thrust of INFOSEC continued to be providing protection against unauthorized disclosure, or confidentiality, but it was no longer the exclusive point of interest.

The biggest change came about when these computer systems started to be interconnected into local and wide area networks, and eventually to Internet Protocol Networks, both classified and unclassified. We soon realized that in addition to confidentiality, we needed to provide protection against unauthorized modification of information, or data integrity. We also needed to protect against denial-of-service attacks and to ensure data availability. Positive identification, or authentication, of parties to an electronic transaction had been an important security feature since the earliest days of COMSEC, but with the emergence of large computer networks, data and transaction authenticity became an even more important and challenging requirement.

Finally, in many types of network transactions it becomes very important that parties to a transaction cannot deny their participation, so that data or transaction non-repudiation joined the growing list of security services often needed on networks.

Because the term “security” had been so closely associated, for so long, with providing confidentiality to information, we adopted the term Information Assurance, or IA, within the Department of Defense to encompass the five security services of confidentiality, integrity, availability, authenticity and non-repudiation. I should emphasize here that not every IA application requires all five security services, although most IA applications for national security systems—and all applications involving classified information—continue to require high levels of confidentiality.

Another point worth noting is that there is an important dimension of Information Assurance that is operational in nature and often time-sensitive. Much of our work in IA is found in providing an appropriate mix of security services that are not operational or time-sensitive, e.g., education and training, threat and vulnerability analysis, research and development, assessments and evaluations, and tool development. However, in an age of constant probes and attacks of networks, an increasingly important element of protection deals with operational responsiveness in terms of detecting and reacting to these time-sensitive events. This defensive operational capability is closely allied with and synergistic with traditional IA activities, but in recognition of its operational nature is generally described as Defensive Information Operations, or DIO. NSA’s responsibilities in this area have grown considerably since the late 1990’s.

To meet this DIO challenge, NSA’s National Security Incident Response Center (NSIRC) provides real-time reporting of cyber attack incidents, forensic cyber attack analysis, and threat reporting relevant to information systems. Through round-the-clock, seven-days-a-week operations, the NSIRC provides the Departments of Defense, the Intelligence Community, Federal Law Enforcement, Department of Homeland Security and other Government organizations with information valuable in assessing current threats or defining recent cyber intrusions.

NSA’s responsibilities and authorities in the area of information assurance are specified in, or derived from, a variety of Public Laws, Executive Orders, Presidential Directives, and Department of Defense Instructions and Directives. The Secretary of Defense is the Executive Agent for National Security Telecommunications and Information Systems Security. The Director of NSA has broad responsibilities

in providing for the security of national security¹ telecommunications and information systems processing national security information, including:

- Evaluating systems vulnerabilities
- Acting as the focal point for cryptography and Information Systems Security
- Conducting Research and Development
- Reviewing and approving security standards and policies
- Conducting foreign liaison
- Assessing overall security posture
- Prescribing minimum security standards
- Contracting for information security products provided to other Departments and Agencies
- Coordinating with the National Institute of Standards and Technology (NIST); providing NIST with technical advice and assistance

While protecting the confidentiality of classified information via extremely strong cryptographic systems was a major part of NSA's mission in the past, our mission has changed emphasis considerably over the last ten years. We now spend the bulk of our time and resources engaged in research, development and deployment of a full spectrum of IA technologies for systems processing all types of information. NSA's days of just building "crypto for classified" are long gone.

Specific Issues Related to Cybersecurity R&D

Your invitation outlined a number of areas where you wanted specific comments and answers.

1. Technical approaches to optimize cybersecurity.

I believe that the highest payoff for optimizing cybersecurity is the creation of an interoperable authentication system deployed widely throughout the federal, national security, first responder and critical infrastructure community. The typical approach used is a public-key-infrastructure (PKI) system with a smart card that contains your cyber credentials. This is the type of system that NSA and DISA have built for DoD. A national PKI system is required that allows for strong authentication in cyberspace for homeland security.

If we have this national system in the future—then when a first responder connects to a DHS website to access information or upload a report—we will know exactly who they are. We can then assign various privileges according to the role that the person is assuming for that specific information transaction. This authentication system also forms the basis for all of the other cybersecurity services from protecting the control of Supervisory Control and Data Acquisition (SCADA) systems to encrypting your email and passwords.

It is also important to note here that the most critical infrastructures, like a PKI, should be built using U.S. technology. I have concerns with foreign software of unknown trust and quality being integrated into critical U.S. systems.

My next priority for cybersecurity is effective border protection. Just like our national borders or the perimeters of our buildings, we need to protect our cyber borders. Effective border protection includes many different technologies.

- The most important technology is a firewall. Firewalls help networks resist attacks by establishing a strong but resilient border between our protected network and the external Internet.
- We also need encrypted tunnels, also called virtual private networks or VPN's. These devices sit between critical networks to protect the information as it moves between secure networks over unprotected pipes.
- Another necessary border security technology is called a "guard". A guard is used when we need to share information between security domains. Consider the case of an intelligence report that is created on a top-secret network. It must be sanitized to unclassified and then sent to a local police department. It would be dangerous to allow this information to move between security domains without review. High assurance "guards" are designed to automatically and safely allow certain information packets to flow between systems but stops all others.
- Finally, effective borders require the ability to detect and respond to intrusions. Just like a security camera on a bank, cyber intrusion detection systems

¹The Computer Security Act of 1987 defines national security systems as telecommunications and information systems operated by the US Government, its contractors, or agents, that contain classified information or, as set forth in 10 USC Section 2315, that involves intelligence activities, involves cryptologic activities related to national security, involves command and control of military forces, involves equipment that is an integral part of a weapon or weapon system, or involves equipment that is critical to the direct fulfillment of military or intelligence missions.

monitor the flow of information around your border and detect suspicious activity.

The best way to protect a system from attack is to eliminate its vulnerabilities. The best way to eliminate vulnerabilities is to improve the way we write software. High on my research priority list is the need for assured software design tools and development techniques. We also need to improve computer operating systems by including functionality to enhance their ability to defend themselves from attack.

The elimination of vulnerabilities is the goal but the reality is that we are a long way from achieving this goal. Attacks are common and vulnerabilities are discovered daily. It has been estimated that over 90 percent of all successful attacks on DoD systems are based on vulnerabilities that are already known and that have an updated software fix or “patch” available. The rare system operator can keep up with all of the “patches” that are issued each month. A system left un-patched soon becomes a target like an unlocked sports car with the keys in the ignition. Therefore, another way to optimize cybersecurity is with an automated patch management system.

This system would also use strong authentication as provided by a PKI but the software producer would sign the new application instead of a person. The patch would be automatically and safely sent to your system. The PKI guarantees that it is comes from an authentic source and has not been corrupted.

2. What areas of advanced technology should be pursued to outpace attacks?

Research is required to improve a cybersecurity system’s ability to modify itself on-the-fly. New attacks are constantly emerging and new vulnerabilities are discovered even in the most carefully designed systems. The ability to update must be safely executed and as transparent to the user as possible.

NSA is working on a multi-year, nearly \$3B development program called Cryptographic Modernization (CM) that has some of these features. There are over 1.3 million cryptographic devices in the U.S. inventory. Over 75% of these systems will be replaced during the next decade. Future security systems are being designed to use the network to safely program and reprogram their operating characteristics automatically and transparently to the user.

Research is also needed to learn how to build cybersecurity systems that can continue to operate even while under attack. Resilient systems, like those being investigated by DARPA and others will be needed in the future. The goal is to have a system that degrades gracefully instead of causing a cascade of insecurity.

I would also suggest that considerable research is needed to effectively coordinate information during a cyberattack. Today, most of this coordination occurs at the speed of humans. But attacks are carried out in seconds and are often carried out automatically.

The CODE RED attack in 2001 infected 50,000 machines per hour, ultimately causing billions of dollars in damage. We need a capability for our networks to work together automatically to weather an attack. Incident information formats, automatic remediation algorithms, the ability to learn attack specifics from intrusion detection devices and other network sensors and then share this info with other networks without human intervention are high priority requirements.

Another significant research topic is the ability to enhance attack identification methods. Most intrusion detection or system misuse systems today rely on patterns or signatures to identify the bad behavior. This works well for known attacks but is useless against novel attacks. The ability to detect attacks and misuse from anomalous behavior is needed.

The ability to detect suspicious or anomalous behavior is also useful to identify insider attacks. Studies have estimated that 50 percent of the most damaging attacks come from insiders. An insider is unlikely to use sophisticated attacks because they already have an account on the system—but the ability to monitor system use during off hours or track users accessing unusual accounts provides vital clues for detecting insiders.

Continuing with the cyber attack theme—I believe that one of the hardest problems we must solve in cybersecurity is attack attribution. That is the capability to geolocate and positively identify the source of attacks on the Internet. Without confident knowledge of who and where an attack was mounted, it is impossible to decide on the appropriate response. A rapid and reliable capability that separates nuisance hackers from more serious threats would increase the overall effectiveness of every cybersecurity practitioner in both government and the private sector. Effective attribution by law enforcement leading would also deter the casual hacker and allow resources to spent on more serious cases.

3. Suggest advanced technology programs needing higher priority & funding.

A significant cybersecurity improvement over the next decade will be found in enhancing our ability to find and eliminate malicious code in large software applications. Beyond the matter of simply eliminating coding errors, this capability must find malicious software routines that are designed to morph and burrow into critical applications in an attempt to hide. There is little coordinated effort today to develop tools and techniques to examine effectively and efficiently either source or executable software. I believe that this problem is significant enough to warrant a considerable effort coordinated by a truly National Software Assurance Center. This center should have representatives from academia, industry, federal government, national laboratories and the national security community all working together and sharing techniques to solve this growing threat.

We also need the ability to trust the hardware platforms we use for critical applications. Most microelectronics fabrication in the USA is rapidly moving offshore. NSA is working on a Trusted Microelectronics Capability to ensure that state-of-the-art hardware devices will always be available for our most critical systems.

The DoD is currently undertaking a major program called transformational communications. This program is developing the military communications infrastructure of the future and it will be delivering high-bandwidth, secure, multi-faceted digital capabilities across the defense enterprise and down to the individual warfighter. Many new cybersecurity requirements are being generated by this initiative and they will require significant R&D resources. For example, additional key management infrastructure capabilities, techniques for multi-level security networks, and ultra-high bandwidth encryption are a few of the new technologies being driven by this requirement. It is important to note that the results of this program will be dual-use. The technology being developed will have application for solving many of the same challenges that are found in homeland security systems.

In today's Information Technology environment, the need is particularly acute for ways to counter security vulnerabilities found in popular commercial operating systems and applications. While many of these vulnerabilities can be fixed by properly configuring the system, the goal is to configure these systems to be as secure as possible "right out of box." Building on the hugely popular security configuration guides for Windows 2000, NSA, working with Defense Information Systems Agency, the National Institute of Standards and Technology, the FBI's National Infrastructure Protection Center (now at DHS), the General Services Administration's FedCert, the SANS Institute, the Center for Internet Security and vendors—developed a set of consensus benchmark security standards. These standards provide a sort of "preflight checklist" of security settings.

The benchmark standards represent an effective model based on agreement between security experts, system operators and software vendors. A number of standards for the most popular technologies are being adopted by many government and private sector CIOs.

I am happy to learn from your last hearing that some equipment vendors are now offering the security standards as the default configuration. I also understand from your hearing last week that industry gave high marks to the great work being done by the Center for Internet Security. NSA is proud to be a part of this project and will continue to support the community in establishing security standards. This consensus approach may not eliminate every vulnerability, but by working together, we can harden our systems against common attacks.

4. Role of technology transfer among government, academia, and industry?

NSA is motivated by a sincere belief that the requirements for cybersecurity products and services for national security uses are identical to the requirements found in other mission critical systems e.g., homeland security and critical infrastructure protection. We have developed a number of programs and policies targeted leveraging the commercial information technology.

- The National Information Assurance Partnership (NIAP) is a U.S. Government initiative designed to meet the security testing, evaluation, and assessment needs of both information technology producers and consumers. NIAP is collaboration between the National Institute of Standards and Technology and the NSA in fulfilling their respective responsibilities under the Computer Security Act of 1987. The partnership, originated in 1997, combines the extensive security experience of both agencies to promote the development of technically sound security requirements for IT products and systems and appropriate metrics for evaluating those products and systems. The long-term goal of NIAP is to increase the level of trust consumers have in their information systems and networks through the use of cost-effective security testing, evaluation, and

assessment programs. NIAP continues to build important relationships with government agencies and industry in a variety of areas to help meet current and future IT security challenges affecting the nation's critical information infrastructure.

- NIAP also produces cybersecurity specifications, called protection profiles that have already been developed for low and medium assurance applications and are periodically updated. The profiles are available on the NIAP website for anyone to use to describe the features needed for cybersecurity applications.
- NSTISSP #11 (National Security Telecommunications and Information Systems Security Policy #11) is a national security community policy governing the acquisition of information assurance products. The policy mandates, effective 1 July 2002, that departments and agencies within the Executive Branch shall acquire, for use on national security systems, only those products that have been validated in accordance with the either the Common Criteria, or other approved methods. Additionally, NSTISSP #11 notes that departments and agencies may wish to consider the acquisition of validated COTS products for use in information systems that may be associated with the operation of critical infrastructures as defined in the Presidential Decision Directive on Critical Infrastructure Protection Number 63.
- The Information Assurance Technical Framework Forum (IATFF) is a NSA sponsored outreach activity created to foster dialog between U.S. government agencies, industry, and academia seeking to provide their customers solutions for information assurance problems. The ultimate objective of the IATFF is to agree on a framework for information assurance solutions that meet customers' needs and foster the development and use of solutions that are compatible with the framework. The forum serves to increase awareness of available security solutions and allows attendees to establish contacts with other individuals and organizations dealing with similar problems. The Information Assurance Technical Framework document, currently in its third revision that provides over 500 pages of technical guidance for protecting information and information systems.
- The Centers of Academic Excellence in Information Assurance Education Program is an outreach effort designed and operated by NSA in the spirit of Presidential Decision Directive 63. The program goal is to reduce vulnerability in our National Information Infrastructure by promoting higher education in information assurance, and producing a growing number of professionals with IA expertise in various disciplines. Fifty universities have been designated as Centers of Academic Excellence to date. NSA has also been using the skills found at the service academies in a number of interesting ways. One exciting program is the service academies competition for attacking and defending networks. We also sponsor visiting professors in IA. We need this type of program for our workforce development - we must invest in our future.
- NSA is also working to transfer techniques to cybersecurity service providers. One of the services that NSA offers under this authority is system security assessment. Since NSA has limited resources to meet the ever-growing demand for INFOSEC Assessments, a training and certification program was developed as a partnership between NSA and private INFOSEC Assessment providers.
- NSA also created the INFOSEC OUTREACH Program to combine the substantial Information Systems Security talents of government and industry partners. The program provides insight into secure design, security evaluation, and the security considerations of system certification. Working together, the partnership of government and industry can meet the increasing demands for state-of-the-art secure telecommunications and information systems.
- NSA and the International Information Systems Security Consortium (ISC)² developed a new Information Systems Security Engineering Professional credential for information security professionals who want to work on national security systems. The new certification will serve as an extension of the Certified Information Systems Security Professional, offered by (ISC)² for information security.

5. How are research priorities and programs determined in the national security area?

We base our priority decisions on a number of factors. The first factor is determined by the technologies and systems most used by our customers. For example, we recently started a comprehensive R&D program to enhance the security of PDA's and wireless 802.11 networks over the last two years because of the explosion of the use of these systems by our DoD customers.

We also maintain a large number of cooperative research agreements with many of the most important technology vendors to help us keep ahead of their development cycles. We also work with small firms ensuring that their innovative technologies are fully informed by our cybersecurity expertise. This insight allows us to program for anticipated cybersecurity enhancements of our systems, or in the best case, influence our industrial partners, large and small, to add additional IA features during development.

Our researchers also participate in R&D agenda setting panels and boards with the NSF, DARPA, National Laboratories, and industry associations. We collaborate with the R&D functions in our customer's organizations. All of this information is used in making an R&D priority and programming decision.

NSA is also unique in that we have considerable insight into the threat presented by various adversaries from our intelligence activities. Threat profiles are developed and these, in part, drive our research agendas.

6. Share your perspectives on leveraging national security standards for homeland security needs?

National security standards are developed for—and are intended to be leveraged for all critical cybersecurity requirements.

- In order to promote secure interoperability between wired and wireless systems NSA initiated an industry and government consortium to agree on a common signaling plan called the future narrowband digital terminal (FNBDT). Although in reality it is not just narrow band anymore but a broad specification, FNBDT includes a common voice processing capability, a common signaling protocol, a common crypto-algorithm base, and a common key management process. FNBDT has become the primary security standard for cell phones, military radios and many emerging public safety communications devices intended to serve homeland security missions and first responders all around the world.
- We also created the High Assurance IP Interoperability Specification (HAIPIS), which will ensure interoperability with all future generations of IP network encryptors. The IP, or Internet protocol, is the backbone of the worldwide Internet. This new cybersecurity specification has become extremely popular and new products, based on this specification are being released regularly.
- Many of the technologies that we are suggesting for homeland security requirements were developed to support coalition military warfare. These systems were designed to cost-effectively support a highly mobile and constantly changing set of information sharing partners. We are confident that they are exactly what many homeland security applications require.

Conclusion

It has been my pleasure to share the work of my agency with the committee today. I believe that much of the research and development initiated by NSA for use in the national security community is directly transferable to the needs of homeland security. We all need to work together to shape the demand side of the market. Everyone needs trustworthy technology. We cannot afford to cut corners.

We must change our fundamental assumption from need-to-know to need-to-share. We must share policies and processes across the community. Cybersecurity products and technologies have been the focus of my remarks today but the technology alone will never be good enough to protect us because—ultimately—getting cybersecurity right is more about what you do than what you buy. Thank you for the opportunity to speak before the subcommittee today.

Mr. THORNBERRY. I thank the gentleman, and all the witnesses, for their testimony. It is rather remarkable to me how much consistency there is really between among all three of you.

At this time, I would yield to the gentlelady from California for questions.

Ms. LOFGREN. Thank you, Mr. Chairman. And as I have in past hearings, I am really struck by how fortunate we are in this subcommittee to be able to really call on some of the smartest people in the whole country, and then they come and share with us. So it is a delight to listen to each of you.

I have many questions, but let me just start in with Dr. Sastry, because one of the concerns I have, you mentioned HSARPA as an encouraging element of the new Department and one with great promise. Before you were leading the Department at Berkeley, you

ran the technology, the cyber part for DARPA. And I am wondering if you can reach back to that part of your experience and give us some advice on what we might do to actually get HSARPA up and running.

Right now there is, I believe, a recently hired deputy director, and that is it. I mean, it was last month you couldn't even call the division because there wasn't a phone number or an office. And there is no director, there is no employees. If you were the czar, what would you do to jump-start that effort so it could be as productive for the country as DARPA was?

Mr. SASTRY. Thank you very much, the Honorable Ms. Lofgren. I had the good fortune to serve under the deputy directorship of Jane Alexander, who is now the Deputy Director of HSARPA; she was the Deputy Director of DARPA. So I think we are fortunate to have some leadership with experience in the DARPA model.

The way I would configure HSARPA is perhaps quite substantially along the lines of the DARPA model with a few differences. The way DARPA programs are organized are they are mission-oriented in the sense that they are 3-to 5-year programs with very definite outcomes. And so even in the information assurance and survivability suite of programs, we had one on secure systems, we had one on fault tolerant networks, we had one on coalitions. And each one of those was separately organized, bite-sized pieces of research. And in addition, the way those were informed by the needs of the services and the needs of the service labs was to have the service labs be the individual CTARs of the technical contractors for executing the contracts.

So I feel that the IAIP Directorate, the Board of Security Directorate, and the Emergency preparedness directorate could provide staff to be the executors of the contracts that come out of HSARPA, very much in that model.

Now, the questions about how one ramps up quickly to this is a very important one, and I think it will take some time to hire the right program managers and to have adequate turnover, the way DARPA does, so as to keep new ideas coming into the agency. One suggestion is to actually use existing mechanisms of partnership with NSF the way DARPA does, or with DARPA itself in the short run, to be able to ramp up to such a state where it has its own program managers.

The one thing I do differently from DARPA is, because there are sort of short-and intermediate-term needs which have to be met in the other directorates, I think I would really have a separate office which concentrates on the technology transition issue. And the technology transition issue would be about setting up the correct structures to make sure that, as the programs mature, those get taken up. And I alluded to some mechanisms that I thought were useful.

Ms. LOFGREN. Mr. Wolf expressed concern about foreign software or software developed offshore and its reliability. Do you, Dr. Bellovin and Dr. Sastry, share that concern?

Mr. BELLOVIN. I am concerned about all software's reliability and correctness. I am not in the position to understand how much greater the threat is when it is coming from elsewhere, but we are dealing with a screen door, not a vault door in a lot of the software.

Patching systems—I was asked this question leading up to Y2K. A lot of the Y2K intermediation work was done offshore. I was asked if I was concerned about that, and my answer was, I am concerned about anybody patching systems regardless of who they are, because patches have a much higher bug rate, hence, vulnerability rate, than base code.

So I think if we had the technology to examine any code, no matter where it was, for security and assurance, or vendor back doors which sometimes are put in for maintenance purposes, we would be in a lot better shape. And I would leave to professionals to understand how much greater the threat is from overseas.

Mr. SASTRY. If I could amplify on that, I fully agree with Dr. Bellovin. I think that one has to be worried about all software. And one of the problems about these complex systems has been that even though one can trust individual pieces, when you put them together, the overall systems tend to suffer from all kinds of problems. So I think that there are some glints of hope. But I think that the technologies for guaranteeing that software, whether it is written overseas or in the United States, is in fact more or less correct by construction, are in their infancy.

One specific one that has come out of Carnegie-Mellon is called proof-carrying code. And this is the notion of providing code which comes with its own certificate so one can independently prove to one's self that it works the right way. The drawback has been that it is not scalable to large systems.

Now, I think that there is an area of research about how you compose and put together large systems. And this is perhaps what we have to do on the fly today to reduce vulnerabilities. And so I guess there are no easy answers.

Mr. WOLF. If I could add a comment to that. Really, there are two pieces to that. One is certainly the quality of the code. And as was referenced earlier, certainly there is a lot of buggy code out there. But the other is the trust factor. And when you think about the globalization of IT and the people that are writing code offshore now, there is a wide variety, many of whom you can say that we trust, and there are others that you might not have so much trust in.

And frequently my organization is asked, for example, by law enforcement to look at code and say, is there a back door in this? Is there something malicious in it? That is a very difficult problem, and the tools aren't necessarily there to do that right now. And so that is the reason that we have talked a lot about the idea of a national lab that looks at software. Certainly, you know, the goal would be that you write codes so that up front the code is good and you have trusted code trusted modules. But in many cases we don't have that luxury. And if you think about the critical infrastructure of Wall Street or the power grid in the east coast, and you look at who wrote some of that code, you might be a little concerned.

Ms. LOFGREN. I am intrigued by this, and I don't know if we will have time for a second round. But I am wondering whether some of the research—I don't think that is a function you would want the Federal Government to provide, and yet it might work nicely with the research that is being discussed, maybe the test bed research that was referenced in the testimony, so that you might

have—I mean, the last thing you want is the heavy hand of the Federal Government on the creative element, and yet we might want some way to examine and have a test bed research component for critical elements of the infrastructure.

Is that sort of what the two doctors are proposing?

Mr. SASTRY. So, I think test bed research is really a lot of what is needed to take ideas from the research stage into systems that work. So, the specific kinds of test beds that I alluded to certainly for network defense, distributed denial of service and worm attacks, are coming in with an increased frequency. There are a lot of different solutions that the research community is putting out, but very few service providers have faith in them simply because they haven't been tried out on systems of adequate magnitude. So also in this software verification the questions of how much faith you can put in proof-carrying code, which is a piece of code that you add to a piece of software to check whether it is actually meeting the functions that it was supposed to and whether or not it has back doors.

So I think that a test bed activity is one of the things that is needed to fill the chasm between research and what comes out of a university or what comes out of other research agencies, research groups, and products.

And then the questions about the regulations. I think that while it is true that it is not completely clear whether one ought to be heavy-handed in the regulation, I do think that as in the Y2K case, the Federal Government had a very, very important role in 1997 by the SEC asking for companies to file their plans for what they were doing with Y2K.

Ms. LOFGREN. If I may. I don't disagree that the Federal Government must play some role. The question is, what is that role? And I think we have discussed many times, and I think there seems to be consensus among most of the members of the subcommittee, that a heavy-handed regulatory role is probably not the optimal role for the government to play, but there is a role for the government to play.

Mr. BELLOVIN. There is a need for test beds. The fundamental problem of software is scale. We can do small things well, both developing and testing; we can't do large things well. That is where a test bed, an opportunity to try certain things at scale in an experimental setting would be very, very useful. And there are some things where it is easier than others. Network technology, it works better.

Software. Most of the large software systems are developed by industry. A mass—a software project by definition is very many people over many years with real users and real changes over the life span. That is hard to put into a test bed. Nevertheless, an industry/government/academia cooperation is useful, because industry has the software that everybody is relying on, including the Defense Department. We are all running commercial off-the-shelf software for the most part, and we have to get this right to secure the critical infrastructure.

Ms. LOFGREN. I think I have more than used up my time, and I would like to thank the Chairman for his courtesy and yield back.

Mr. THORNBERRY. The gentlelady is asking some very good questions.

The Vice Chair of the subcommittee, the gentleman from Texas. Mr. SESSIONS. Thank you, Mr. Chairman.

On behalf of this committee, as you have heard us say, we appreciate all three of you being before us today. I think this is an important exercise for this subcommittee and for our own knowledge.

Mr. Wolf, I think I would like to direct my question to you, but I am not sure it would be limited to you. You speak very forthrightly and clearly about effective border protection. And, quite honestly, that makes my mind race. I am a free trader. I believe in goods and services and information flowing back and forth between countries. And I believe one of the most powerful parts about the World Wide Web is its availability to people for commerce and other activities. However, the need of this great Nation to protect itself and its intellectual property, its secrets, and other things that emanate from that is important also. And in my mind, I understand—I think I understand border, but I am not sure that I do, and it is because I really don't have a concept of where all these nodes are that bring traffic into this country to where they share our information.

And standards body. When I was at Bell Labs, we were a part of a standards body organization for switch manufacturers.

I would like for you, if you could, to perhaps go through in a detailed way about what you see as this border or cyber border. And are there things that we as this country should be doing, just like trade agreements, to say—or just like Customs would be at an airport in a foreign country or visitors coming to this country. Should we place a burden upon knowing who is coming here and where they came from? And I know this is hard on a real-time basis. Or even if just information that would travel with that packet that would comment about where someone originated. I think you see where I am coming from. Can you address that?

Mr. WOLF. Okay. And I guess let me start by saying when they talk about border protection, you are really talking about protecting—if I can start, say, with your computer at home, in terms of having a firewall such that you can control in terms of who comes into your computer, who has access to the computer, the kinds of things that come in and go out of your computer. So that is not restricting you from going to anywhere in the world, okay, to look at something on the Internet. But it is meant to stop a hacker, for example, from coming into your computer and stealing your tax information. So we talk about firewalls. And firewalls have a set of privileges that you can identify with them in terms of how strict and how high up you want to put the wall, if I can say it that way.

We also talk about intrusion detection systems. So now if you go a little further out from, say, your home computer and you want to develop a profile of what kind of activities are coming across that boundary, looking for hackers, for example, that is kind of what we would call border protection. In terms of looking for malicious activity, threats, hackers, whether that is a terrorist, a nation state, state, whatever. So you are, if you will, protecting your computer environment, protecting cyberspace.

Now, if you take that a little further to the borders of the United States, that would be a very difficult task to put up, if you will, some kind of protection around the United States, and probably not necessarily a good investment. But you certainly would want to put sensors maybe on the periphery of the U.S. again to look at hackers, to look at people trying to come in to do malicious things to you, and to look also at maybe data that is leaving the U.S. the idea of—and I talk sometimes, and I think in my testimony talk a little bit about the insider. You know, is there information leaving a facility that you wouldn't want to leave? Is somebody on the inside pushing information out to another entity?

So when we talk about border protection, we are really talking about how do you protect your enterprise, what kind of protections do you put around it so that somebody can't come in and do something malicious to your enterprise? So, not really restricting in terms of, you know, the Internet as a whole, but it is more the protections that you want to put in to make sure that somebody isn't doing something malicious to you.

Mr. SESSIONS. So the border could mean any individual computer as opposed to in the border I was describing as the United States of America?

Mr. WOLF. Yes. So we are not necessarily talking geographic. In DOD, we have something called "defense in depth," and we talk about the enterprise level, the information backbone. There are several levels that we talk about in terms of doing protections. So it is not necessarily a physical boundary in terms of around the United States. Although there may be something in terms of implementing a network of sensors to look for hackers, to look for kinds of activities, malicious activity. That may be something that we want to do.

Mr. SESSIONS. Okay. Any of the other gentlemen choose to speak?

Mr. BELLOVIN. Yeah. I am in favor of border protection to the extent it is possible; I was the author of the first book on firewalls in 1994. But it is a much more challenging problem today than it was in 1994, because the amount of interconnection has increased tremendously. A modern corporation will have hundreds to thousands of external links that penetrate its firewall to its outsource functions, to its joint venture partners, to its customers, to its suppliers. All of this is done electronically, and all of this is done by means of mechanisms that bypass the firewall, go through the border.

In other words, we have many more border crossings than we do today. The virtual private network technology that lets me work from my hotel room exactly as if I was inside my office at AT&T works very well; but if the same employee who is telecommuting via VAN is using that same computer to surf the Internet individually, we have a problem because we don't have an effective border. We are moving more towards a motel rather than a hotel model. In the hotel, there are one or two entrances and everyone is walking past the front desk. In the motel, every room has got its own door to the outside. It is a lot harder to secure that, and we are moving more towards that ladder. We have to find a scalable solution to let us protect all of these doors.

I would note that tracing things, where they are coming from outside the country, is a lot harder. The hackers don't use their own computers for the most part. They use their own computers to hack an easy target, maybe in a university someplace or a small company, and use those to hack a few more. Five levels away, that is where they will launch the attack from. The attack may be coming from inside or the outside, but you don't know where the controlling messages came from. And that is what makes it so hard to trace back these things. Authentication credentials, they are stealing the credentials identity today. It would be very hard to fundamentally reengineer things to get around that.

Mr. SASTRY. I share your sentiments about being open enough to, A, have IT products come into the country, and also for us to be able to sell IT products in other parts of the world. And so I think that open standards, which I think is one of your concerns, are in fact better than standards where one erects barriers.

But having said that, I think that one does need to have the sense of being able to dial up and down security so that even if you did have this motel model and sometimes—and physical security with different threat levels and being able to dial up and down security depending on your perception of how threatening the environment around you is, the questions of how to do this are I think are open research issues.

Also, I think that the questions about being able to trust software, I think it is easy to trust individual pieces of software and to be able to test individual pieces of software regardless of where they are written.

On the other hand, the problems are about what happens when you try to compose them. And the biggest single problem is when you put together complex systems—and people inevitably build complicated systems for reasons of functionality—that is when we really don't have guarantees both in security and also in privacy because of the kinds of data sharing that occurs across large systems.

So coming back, I think in the earlier parts of our testimony both Steve and I, Steve Bellovin and I, agreed that really sort of the bottleneck problem is to be able to compose secure systems so as to guarantee that the overall system works. And I think that the way to do that is not actually to stop people from sending software in or for us to be able to sell overseas.

Mr. WOLF. And if I could add one more comment. We talk about border protection and firewalls. You also need to think about what functions you want somebody to be allowed to do on your computer. So it is not just put a border up and protecting it, but it is what do you want them to do. Do you want them to be allowed to look at Web pages? Do you want them to be able to move files around? So there is a whole set of things to go along with that. So it is sort of the motel model in terms of defining what you can do in the motel.

Mr. SESSIONS. I appreciate that, gentleman. That obviously led me right to what Mr. Wolf was talking about, and that is our own systems is our border. And I appreciate the discussion. I yield back.

Mr. THORNBERRY. I thank the gentleman.

The gentleman from Rhode Island, Mr. Langevin, is recognized.

Mr. LANGEVIN. Thank you, Mr. Chairman. I want to thank members of the panel for being here, and your testimony, and really some of the questions I have prepared you have addressed. But I would like to give the opportunity to expand on them a little more. And I will start with asking if you can discuss whether there is sufficient information sharing taking place between researchers who discover most vulnerabilities and the companies who created the products and the DHS. And also, how could the government help to foster an environment where researchers and companies could better work together?

Mr. LANGEVIN. And then, expanding on that point, what do you see as government's role in terms of increasing security and standards setting? Should it be fostered through partnerships and purchasing criteria, or should we take a more active role? I know you discussed this a bit already, but if you can expand upon that. And basically would government-mandated standards, such as the common criteria, be a baseline or hindrance for future innovations? If you could take a crack at those, I would appreciate it.

Mr. BELLOVIN. When it comes to vulnerability reporting, there is pretty good cooperation between the people who find the holes and the vendors. There is sometimes an unrealistic expectation of how soon a problem can be resolved. More responsiveness, at least acknowledgment, would certainly help. I think it is cases of people getting frustrated at reports being ignored. In general that is a path that works well.

Sometimes people have unrealistic expectations about what can be done. You know, the problems are generally subtle, or they wouldn't be there in the first place.

For standard setting, I would suggest the procurement model is much better. We don't know exactly what we are doing. There is a saying, if we know what we were doing, it wouldn't be called research. And to try to mandate certain things is probably premature given the state of the art. The Common Criteria is a useful step forward. As an NRC report a few years ago pointed out, it doesn't really address a lot of the software models we are dealing with today. It is also extremely expensive to produce software that meets these criteria and can continue to meet these criteria over the life cycle of the hardware and software platform.

This has tended to make such systems slower, much less modern, and much more expensive than the commercial off-the-shelf alternatives, which has generally led people to buy the commercial off-the-shelf alternatives, because they don't perceive the threat, there is no particular push back, no incentives, as I said earlier, for people to install the more secure software in most situations.

Mr. LANGEVIN. Okay.

Mr. SASTRY. I share a lot of the comments made by Dr. Bellovin.

Let me talk a little bit about the information-sharing, which is one of your questions. I think that information-sharing is an important step. The ISACs are certainly an attempt to try to get information-sharing across industry sectors.

My perception is that there is a lot of concern in industry about sharing this information, partly because there isn't a lot of sensitivity about how this information would be protected by FOIA requests. Of course, there are ways, there are other transactions, au-

thorities and other procurement mechanisms by which this information could be protected. I think industry needs to be sensitized to the fact that they can, in fact, share this information without its being open to public scrutiny.

My sense also is that there is a certain amount of funding, and I think the Federal role in being able to smooth this information-sharing is not to be underestimated. I think that there is a sense that a lot of especially small companies feel that they are sort of doing that on their own dime. So I think that if they had a greater sense of feeling protected when they shared the information, and also they were given some help, some financial help, for sharing this, I think this would go a long ways to where it is helping the ISACs.

Mr. LANGEVIN. Could you expand on that. How we do that? How we foster that?

Mr. SASTRY. I think there are mechanisms inside DHS, and I think there are questions of appropriation of a certain amount of resources simply for the ISACs. And the other transaction authority is simply the contractual mechanism that can be—that can be chosen to be exercised by the Department of Homeland Security to actually protect the information from FOIA requests.

I think they have the—I do think that they have the OTA authority to do so. The telecom—and the telecom folks that we talked to at BellSouth and others were really quite concerned about being sort of reassured about this, partly because this OTA is not a well-known contracting instrument, and people don't know all of its possibilities, I guess.

Mr. LANGEVIN. Thank you.

Mr. WOLF. A major part of my mission, if you look at my mission statement, is to discover vulnerabilities, because my job is to provide secure systems for the national security sector. So we put a lot of effort into discovering vulnerabilities. And we work very closely with industry. We work very closely with academics in terms of how we do that.

We have various reach agreements such that—with various companies, they are called CRADAs, cooperative research agreements, so that we get access, for example, to source code, and again, with the idea of how do you improve the source code to improve the security. When we find a problem, we go back to the company, we explain what the problem is, and in many cases provide them some of the technology to help improve their product, because, again, we are trying to build product.

That is my main goal is to get product out there for the national security sector. Of course, the byproduct of that is it is dual-use technology. So anything I provide to national security in many cases can be applied other places.

So I would say there is a very close relationship in terms of working with industry on that. I can probably go through many, many examples of successes that we have had in that area.

You mentioned about security settings and benchmarking. I think that is a very, very important thing. I mentioned that in my testimony in terms of how do you configure things out of the box so that they are very secure. And we are very active in that par-

ticular area. Common criteria is something that we strongly support. We put a lot of effort into common criteria.

Common criteria, what it does is it is really, I will say, raising the bar, if you will, in terms of information assurance. It is not the ultimate answer, it doesn't make it perfect, but what it does is it does put products through a fairly rigorous testing for certification, so that given a set of functions that the product is supposed to do, that you have demonstrated that it does do those functions under certain conditions.

Now, again, it doesn't solve all of problems, but it does raise the bar. And common criteria probably needs common criteria 2, some additional things to common criteria. And I share the comments and agree that common criteria can be a little expensive for companies, and that is something we are also trying to work in terms of how we can improve either the timeliness of things getting through the process, or how we can do something in terms of helping in terms of financially. But that is a difficult problem to resolve.

We have reached out to homeland security, in particular Bob Liscouski in the IP, and have talked to him about working with us in NIAP and how we can leverage the kinds of things that he needs to do with the national security sector. So together what we do is we come to the table with a larger, if you will, market share. If we just looked at the national security sector, that is not a big sector in terms of many of these products. So in terms of getting the things through common criteria through NIAP, if there is homeland security and national security, that makes it a much larger market, and makes it more cost-effective in terms of a company going through that and getting that process done.

I guess the other question was about mandated standards. I don't believe we should mandate standards. We should establish standards. We should sort of recommend standards. But I think, you know, one of the problems with standards, and I certainly see it in my sector, we have everything from a small military installation with a small requirement to some large network like the SIPRNET, and to try to mandate one standard in those two extremes is very, very difficult for anybody to meet.

So I think you want to establish a set of standards, recommended standards, and do it that way rather than make it mandatory, because one size does not fit all.

Mr. BELLOVIN. Let me echo that. It if was that simple to ship a secure system, Microsoft and Sun Microsystems and everyone else would have done it years ago. How you use, how you configure a network or system depends on its purpose. A laptop that is used for text editing and e-mails has very different configuration requirements than a software development machine, which is very different than a Web server, which is very different than a database server and so on.

There are about as many different uses of computers and configurations as there are computers, and one size does not fit all.

Mr. SASTRY. If I may just respond to your question of partnerships. And now I will sort of take the academic. I think the problems, the research problems and the development problems, are really too large for just about any group in this Nation. So I think it is especially important for research groups to work in teams. And

at Berkeley we have really found it very, very important to collaborate with large numbers of research groups across the length and breadth of the Nation.

The questions are then about what facilitates this collaboration is really at the academic, at the research level, that we have open standards where we don't use IP protections inside universities for protecting the kinds of software and systems research that we do, but at the same time we allow for industry partners to be able to uptake that information and take it out of the open source development, and then take it and encapsulate it into their products. And so, for instance, in sort of a research center and trust, which we are doing with Stanford, Carnegie Mellon, Cornell and Vanderbilt, we have found it very important that we voluntarily have adopted an open source IP policy amongst ourselves, while making sure that the companies, the industrial partners, can actually take the open source materials that are created, the secure trusted systems that are created, and then go take it into their proprietary products. That is sort of something that I think that the research sector can do in this particular space.

Mr. WOLF. One of the exciting things that is happening in NSA right now is that—

Mr. THORNBERRY. The gentleman from Rhode Island elicited a host of interesting responses, which we certainly may want to pursue, but in the interests of time, let me turn to other Members, because we have gone well over double the 5 minutes.

Mr. LANGEVIN. I thank the Chairman for his latitude in allowing the panel to answer.

Mr. THORNBERRY. I appreciate the gentleman's questions. Excellent questions.

Does Chairman Cox wish to ask questions at this time?

Mr. COX. I do. Thank you, Mr. Chairman. I wonder if I could ask Dr. Sastry and Mr. Wolf whether you agree with the statement made by Dr. Bellovin in his testimony that when it comes to cyber, most basic research is being done in our universities. Is that your opinion as well?

Mr. WOLF. I would—

Mr. SASTRY. I am sorry?

Mr. COX. If you could not hear the question, I am asking whether you agree with Dr. Bellovin's assessment that when it comes to cyber, most basic research is being done in our Nation's universities?

Mr. SASTRY. I would say so, even though there are pockets of excellence in industrial research labs as well, such as Dr. Bellovin's group itself.

Mr. WOLF. I would disagree. I would say it is done in many places. Cybersecurity covers—there are many facets to that. I would point to DARPA, I would point to NSF, I would point to some of the things that NSA is doing. I would point to the national labs. There is some very interesting work being done in the national labs in cybersecurity. Again, some of that is classified research, so everybody doesn't necessarily get to view that.

Certainly in the academic areas, there is lots of work being done, and we partner with the academics, so it is being done in many places. I don't think there is one area that—one organization that

you can point to, one entity, and say that they are doing most of it.

Mr. COX. Well, I ask the question not because I think that Dr. Bellovin would disagree with anything that you just said, but because I think, Dr. Bellovin, one of the points that you are making is that it is—that we know essentially where the researchers are, and that it is difficult to scale up; that we can throw a lot of money at this, but we also have to spend just as much time thinking about which direction we are going, because we can't make it up on volume. We are not going to be able to reproduce all of this. Is that a fair statement of your point, Dr. Bellovin?

Mr. BELLOVIN. Yes, that is it basically. I am not saying there is no basic research. There is certainly a very large need for applied research which does go on very many places. But university research can't be scaled up, basic research can't be scaled up by too much, because there aren't the people to do it yet.

Of course, these are the people who are training the future generations of researchers. So it is very important that we encourage this, because it is not a problem that is going to go away any time soon.

Mr. COX. Well, taking that point, as supplemented and augmented by Mr. Wolf's comments, and we are well aware that we have the Federal piece, some of it is not public, so maybe our estimates of whether majorities here or there might even be a little soft, we are going to—I am going to infer from this, and this is the premise of my next question, that we are going to need to rely on our Nation's universities for some of the big objectives that we are attempting to tackle here, that this is going to be a partnership, and the Federal Government is going to partner with our universities.

And then that takes me to, Mr. Wolf, your next point, and our Ranking Member Ms. Lofgren also questioned you about this a little bit, and that is our need to focus on U.S. technology, and whether this is possible if we have open standards, if we have a lot of people participating, if we are using the private sector as well as universities, it is not all in a black program in the Federal Government; is it realistic to assume that this is possible?

Mr. WOLF. Well, I think it would be difficult to say that we would use all U.S. That wasn't my point. My point was really that there are certainly critical areas where you want to have a good control of, you know, your hardware and your software, maybe in a critical infrastructure, certainly in the national security sector.

So if you have a system, you may want to look at certain areas and put better controls over the—I will say both the quality and the trustworthiness of the software. My comment about, you know, national software assurance laboratory, that may be a way of taking software, wherever it is written, and be able to validate it and say, yes, this is trusted software. The world right now, we are—IT is globalizing. Lots of work is going offshore. The U.S. cannot do everything. As I say, it is globalizing.

So it is a matter of how do you look at software code. How do you validate it? How do you say you trust it? So whether it is U.S. or foreign written, it is really a question of trust. How do you establish trust in the software to make sure that it really does what

it says it does? So it is not only the quality, but also the trustworthiness.

Mr. COX. To the extent that our focus is on firewalls, or at least on that genre of technology that is meant to help networks resist attacks, an additional reason besides our own homeland security that we need to be concerned about theft, about penetration of these programs is that other nation states who are wary of the Internet, don't want their citizens using it, and who are using black boxes and firewalls to prevent their citizens from having access to the outside world would be thrilled to lay their hands on the most sophisticated technology that we have developed at taxpayer expense in order either to prevent their citizens from having access to the Web, or to trace the behavior of their citizens so that when they are doing things on the Internet that the government doesn't approve of, they can land them in jail.

What can we do, therefore, to focus on security of the tough measures that we are trying to develop in our own country? And for this purpose I include both cybersecurity and physical security. And I address that to all three members. My time has expired. I thank the Chairman.

Mr. SASTRY. So your question is really quite interesting. Let me first talk about security and privacy. So the questions about building in privacy with—strong privacy with strong security, my own sense is that the kinds of technology solutions that help foster strong privacy include things like audit, include things like watching the watchers to try to determine who is watching what; also, these questions of selective revelations, which means that queries are answered narrowly so as to selectively reveal information little by little rather than have access to a lot more than is asked for; and then finally the questions about being able to understand if certain privacy standards are being met, and there are a host of new technologies, such as encrypted queries, crypto protocols is what they are called, for being able to enforce that.

So I think that in terms of taking worldwide leadership, I think we can really build in strong privacy into our strong security solutions. And then, of course, the questions of how this may be used overseas, of course those are much more complicated ones, but nonetheless we will have products which have strong privacy safeguards build into it. So, I think that this is one thing that we can do to sort of foster our ideals, while providing strong security.

And I think that this message is somehow a little different from a message which says that you have to give up privacy in order to get security, because the technology indicators are all that—in fact, they are mutually reinforcing, rather than one at the expense of the other.

Mr. WOLF. Not necessarily a complete answer to your question, but certainly one of the things is—at the national security sector is that we do have levels of protection that you put into various systems. So, for example, levels of encryption, where you have the—I will say the high-grade encryption, which is for the most significant and the most sensitive communications, where you may have over levels of encryption that aren't quite as good, but are still adequate to protect the information.

So you can think of that in terms of the products that we are putting out. You may have a higher level of protection in terms of protecting the power grid in a product than maybe the general product that would be available that would be sold overseas. So there are ways that you can do them.

Mr. BELLOVIN. The firewall technology, one of the criticisms of firewalls is that they assume that everyone on the inside is a good guy, is following the rules. This is a problem in industry as well. But in terms of the model you speak of, with repressive governments trying to isolate their citizens from the Internet, in that case it is the people on the inside who are actively trying to get around the firewall technology. And firewalls are not very good at that. There are some that do better than others.

We are better off with strong firewall technology to protect ourselves with multiple overlapping layers of defense in depth to prevent people from the outside getting in, using overt mechanisms to provide insider behavior, ones that don't scale to a whole country, whereas outbound traffic is relatively unrestricted, and you rely on internal auditing. That, I think, would not pose nearly as much of a threat of being used by repressive governments to keep their own citizens from accessing the Internet. So I don't think there is any particular conflict there.

Mr. COX. Well, I am happy to hear that.

Thank you, Mr. Chairman.

Mr. THORNBERRY. Thank the Chairman.

The gentleman from North Carolina.

Mr. ETHERIDGE. Thank you, Mr. Chairman. And let me thank you and the Ranking Member for this meeting, and for our distinguished guests for being here today. It has been very interesting thus far, and I appreciate that.

Gartner, Incorporated, a respected IT consulting organization, has estimated that about 90 percent of the cyber intrusions could be avoided if individuals and companies consistently maintained the security of their computer systems by monitoring use and installing software patches to identify security flaws.

Number one, do you agree with that? And, number two, do you believe that software vendors could make security maintenance a little more user-friendly? If each one of you would just touch on that.

Mr. BELLOVIN. I would guess that it is more like 95 to 98 percent than 90 percent. I very much agree with that statement. But, as I indicated in my written testimony, patching systems, especially production systems, is a much more challenging thing than it should be. I will not update my PC after about April 1st until I have filed my taxes, because I can't take the risk of some unrelated change disabling the tax preparation software I use. And you have got that problem in spades if you are running a corporate Web server, a major corporate or government database and so on.

As Dr. Sastry has indicated, the composition of systems, the components of complex systems working together properly is a very, very difficult and unsolved problem. We don't know how to do this. This is why patching is so hard. It is not that the administrators are irresponsible, or that the vendors haven't supplied good tools,

it is that we don't know how to do it easily, reliably and without breaking something else.

Mr. SASTRY. Mr. Etheridge, if you were like me, when you are installing a computer and you have all of these queries which say, will you do this, will you do this? I think everybody's tendency is just to press, yes, yes, yes, or no, no, no randomly. So I think what you are alluding to is a big, big hot-button item.

So people talking about human computer interaction. So I think the notion of human computer interaction for security to make it easier for people to actually understand what they are doing and be able to configure their systems is—I think is a vast and rather untapped area of research in cybersecurity. If anything is needed right away, it is one of those for the—and I agree with your statistics, too.

Mr. WOLF. Operationally my organization does red-teaming, which is an organization that tries to penetrate networks. So we have customers in DOD that ask us to go look at their networks and to see if we can get into them. And I can verify that your 90 percent is probably correct. It is the networks that haven't been properly patched, configured properly. We look for those kinds of things. That is usually the door that we get in.

If I look at the statistics that come out of the defense—of the DOD networks, that come out of the JTF-CNO, I think their statement is it is about 90 some percent of the attempts to hacks are really trying to get at things that haven't been patched properly.

In my testimony I talked about automatic patching and how that is a significant research agenda item. I believe that needs to be done. How do you make patching much easier for the system administrators? They are overwhelmed with the number of patches and problems and configuration settings that they have to do every day. And the idea of having preconfigured systems coming out of the box that are security-conscious in terms of here are the right settings, I think, is also another step forward.

Mr. ETHERIDGE. As you have noted before, and others before us, that the government, universities and the industry need to encourage more students to get into math, science and all of the science areas of technology in order to produce more graduates who can deal not only with cybersecurity, but with this whole issue of technology that we are dealing with.

And let me go to each one of you on this one, starting with you, Dr. Sastry. Is the academic community acting in a way in retaining the number of scientists needed in the research area as it relates to cybersecurity as we look down the road, and, more specifically, making these systems more user-friendly? Because I think that is the key to getting the security.

Mr. SASTRY. Sir, it has been recognized that human computer interactions for cybersecurity is something that we need to focus on. The realization has kind of surprisingly recently. So in some ways the work is only now beginning.

The questions about training the workforce, I think these are very, very—this is a really a very important item for us, because security, of course, depends on making sure that the entire populace is educated about all the needs of cybersecurity, because, of course, it is only as strong as the weakest link. I think that there

has been in the last 2 years a shift in enrollments. I am in an electrical engineering computer science department. So there has been a shift away from computer science towards computer engineering, which in some ways is encouraging, because it does encourage people to now start thinking about information technology as a technology that is woven into the fiber of our everyday life and into our societal scale systems.

But other disturbing trends are that the percentage of women that are coming into electrical and computer engineering, we have actually given up the advances that we made in the mid-1990s in the last 4 or 5 years. That indeed is subject for concern; so also with other segments of the population. So at Berkeley, we have actually started going out and visiting high schools to try to get them thinking about cybersecurity already in high school, and certainly in Oakland and San Jose and all of the neighboring schools. So your remarks are really on target for our priorities.

Mr. ETHERIDGE. Thank you, sir. I see that I am out of time. But I would be intrigued, because I think it is important in every area of industry as well.

Mr. BELLOVIN. I don't have anything to add on that.

Mr. WOLF. I was just going to comment on our outreach program to educational institutions. We have the Centers of Excellence. We have 15 universities have an IA curriculum. We work with the service academies. We are currently starting to do some things at the community college level, sort of what you were saying in terms of kind of moving up through the lower levels up through the universities. We clearly need to make more people aware of IA in terms of things that need to be done.

Mr. ETHERIDGE. Thank you.

Mr. THORNBERRY. Thank the gentleman.

The gentlelady from the Virgin Islands, Dr. Christensen.

Mrs. CHRISTENSEN. Thank you, Mr. Chairman. I don't expect that—I want to thank you for this hearing as well. I am becoming better informed on the area of cybersecurity, although I am still far from being an expert. My questions are going to be a little different.

Dr. Sastry, in your testimony, you talked about whether the Federal Government would play the role of market maker and asked was there sufficient demand to stimulate new companies around ideas. It would seem to me that a fairly sizable demand would be in the private sector, and incorporations for security and for cybersecurity.

We recently did Bioshield to encourage and expedite the development of countermeasures for bioterrorism agents, which will involve a significant expenditure on the Federal Government's part. Do you foresee in the area of cybersecurity that the Federal Government would have to provide most of the funding, or do you see that there is really a sufficient demand in the private sector that there would be more cost-sharing on the private side, and there would seem more diverse use, other than for homeland security, for government use in these kind of products?

Mr. SASTRY. Thank you very much for your question. I think that the big market, of course, is in the private sector. And the big mar-

ket is in the infrastructures which are certainly not owned by the Federal Government, which are privately owned.

The question, of course, has been about jump-starting this market. So, just to give you an example, there has been a big buzz in the venture community about investing in security for the last 2 years. But, on the other hand, a number of the portfolio companies that come out of the venture community actually have not had a stream of revenue in secure products. So our sense is that since the Department of Homeland Security itself is committed to, in its Border and Security Directorates, IAIP Directorates and the Emergency Protection Directorates, to buy secure products, our sense is that having this—having this sort of as a badge to distinguish these products will actually jump-start the market in the private sector.

I think my own expectation is that that would not—it is not something that one ought to or perhaps could subsidize. On the other hand, I think that if one—when I said a market maker, it was just a question of jump-starting the market by adopting certain sets of secure products in the beginning.

I think the same—and the model, again, is a little bit like the DOD model. So the Internet actually grew from the ARPANET being used for certain DOD applications, and then sort of everybody else sort of jumped onto it, and so also for high-performance computing, which resulted in PCs. So that is sort of the market-maker analogy that I was using.

Mr. BELLOVIN. I would agree that much of the funding and energy has to come from industry. The Government's role is to create the appropriate incentives. If you look at the history of, say, cryptography, there is 100 to 150 years' worth of experience of people saying, I have got a really cryptographic solution and then going bankrupt because nobody wanted to buy it, because they didn't appreciate that they actually needed this technology.

We are sometimes seeing the same thing in the computer security community today. There are solutions that have not been adopted by corporations that don't perceive the threat. It is only in the last few years that more than, say, the financial community and the military have really begun to realize that there is a real threat out there, and a real market.

I note in the last year or so Microsoft has finally gotten religion about security and started to take some very admirable projects and efforts, from what I have heard, internally, doing a very nice job. But it is going to take years for this to have an effect. But the real question, and this is the role for government, is to create incentives for corporations and government agencies to start thinking about security when they design systems and when they procure systems, creating the incentives for them to do so. That is a difficult problem, but that is a role for government.

Mr. WOLF. I would agree with some of the things that have been said so far, but I would sort of focus a little bit on the global IT, the amount that is being spent in the U.S. Government on IT, the amount that is being spent on information assurance kinds of products.

Mrs. CHRISTENSEN. Can I just interrupt your answer to just add, that I understand that less than 1 percent of the science and the

technology budget, or about \$80 million, is being directed to cybersecurity and R&D. Is that adequate? Could you also—

Mr. WOLF. I am sorry. Say that again.

Mrs. CHRISTENSEN. I understand that about \$80 million is directed to cybersecurity R&D in the Science and Technology Directorate budget. It seems like you were going to talk about the amount of government spending. This is in the Department of Homeland Security.

Mr. WOLF. Okay. I am not—

Mrs. CHRISTENSEN. Could you also respond to whether that is adequate?

Mr. WOLF. I think we need to be spending more money in research really and in cybersecurity. I think there is a lot more things. I think we are underfunded in many areas.

The comment that I was going to make is that, you know, we have tried to move from a demand—or a supply side to a demand; that customers are educated in terms of information assurance, in terms of cybersecurity, and they are looking for products and demanding products, that they actually need them.

That is one piece. The other piece is the idea of maybe looking at insurance. If you look at a facility in terms of you evaluated it, is it certified, and then there is an insurance break that goes along with the corporation that, quote, has good system administrators, they have gone through some certification process, you have a reasonable architecture, that is a way in terms of—rather than over-regulating or enforcing standards—that you indirectly, okay—you can create more of a demand for the products.

Mrs. CHRISTENSEN. Thank you.

Thank you, Mr. Chairman.

Mr. THORBERRY. Thank the gentlelady.

The gentleman from Kentucky Mr. Lucas.

Mr. LUCAS. Thank you, Mr. Chairman.

This is a hypothetical, sort of a holistic, big picture question. I would ask each of you to comment on this. Let's assume for the moment that you have been put in charge of cybersecurity for the Federal Government, Homeland Security, and have you been asked to prepare a budget for that job, to do an adequate job, and that you submit this budget, and you get a third of that budget, one-third of the money that you think you need. I would ask you how would you prioritize what you would spend that money on, if you only got a third of the resources that you felt you needed to do the job. I would like for each of you to answer that.

Mr. BELLOVIN. Well, if you are talking about operational networks, I would first put money into systems administration, because, as we said, 90 percent of the attacks are from known holes that haven't been patched. That would be my first priority, to improve the resources for system administration and what they need to do the job. Past that, for research funding, I would start to focus on composition of secure system development.

Mr. SASTRY. I understood your question to be about research money. Of course, for the operational aspects, I would fully agree with getting systems administration to the fore and empowering systems administrators to be more involved in decision-making.

For the research money, the way I see it, it is sort of a world of networks and systems. One has got to protect the systems of the computers, the networks on top of it, and then finally coalitions of systems on top of it. So I think that if the research money was cut in a third, I would make sure that there was coverage at every one of those levels, at the level of individual systems, at the level of networks, and then, of course, at coalitions, of groups of users.

Having said that, I think then the question about a few areas to invest in, I think there the notion of how you build complicated systems which are trustable from pieces that can be trusted, which is the composition that we keep coming back to, needs to cut across all of these layers. Then I think the human computer interaction question that Mr. Ethridge raised, I think that is equally important to me.

And finally, the third thing I would do would be the test beds to make sure that the research got out to companies that could then sort of produce product.

So those are sort of a matrix. I would make sure that the network systems are all populated, and then the three areas—those would be my three pet areas.

Mr. WOLF. I would start, I agree with the operational aspects, to make sure that your operational pieces were secure. So it is the system administrators, it is the patches, it is the kinds of things that we have talked about so far.

The second area that I think I would look at would be sort of my—I will call it my infrastructure. Given that I only have a third of the budget that I need, I would look at my infrastructure and try to build an infrastructure that I could then build on in the future, so—as you get your funding for the following years. So, if you want to call it—maybe it is the—I won't say the key management infrastructure, but it is the PKI, it is the kind of things that you could then build tools and techniques and products and services on in future years. That would be my second area.

And the third, I think that I would take a step back, and I would look at all of my systems, my networks, my—whatever my operation is, and I would try to identify what are the most—I will call them the critical areas and apply the dollars to those as maybe the third venture there.

And, of course, I would also put a piece to research, because I think a lot of times we are very short-sighted when funds are cut—I worked for the government for many years—that we tend to cut the research piece. If you tend to favor the operational piece, but the research piece is your investment in the future. If you don't put dollars towards that, then 5 years from now you will be dead in the water.

Mr. LUCAS. Thank you very much, Mr. Chairman. We have got a vote coming up, so I will stop there.

Mr. THORNBERRY. The Chair appreciates the gentleman.

Does the gentlelady from Texas have questions she would like to ask?

Ms. JACKSON-LEE. Thank you very much to the Chairman and the Ranking Member for holding this hearing.

Mr. Chairman, I ask unanimous consent that my statement be submitted into the record.

Mr. THORNBERRY. Without objection.

Ms. JACKSON-LEE. I appreciate the testimony of the witnesses and their indulgence. I am in a Science Committee mark-up that is going on simultaneously, and so I thank you very much for your patience.

I just want to focus in one area very quickly. We do have votes on. That is the need for the prominence of cybersecurity issues under the Department of Homeland Security. And what we have noted is that the funding has not been where we would like it to be. A Director has not yet been appointed. It all suggests that we need to refocus our attention on this area.

So if you would answer these questions quickly, I would appreciate it. One, my understanding is, or my sense, that as we are going into the 21st century, Y2K we were all focused on what technology, Internet, could do to this Nation. Literally we were in a panic about it being able to stop us in our tracks. After 9/11 we began to focus on some very real concerns about security.

I don't know where we placed the need and the focus of security in this instance, cybersecurity, inasmuch as we are still in the same boat, that the—the attack on our security infrastructure, our technology infrastructure could bring this Nation to its knees. So my question to you is have we focused enough?

The second part of it, with respect to research, have we expanded it enough? I believe we should start expanding our reach to universities around the Nation, research entities around the Nation, and as well make sure we include Hispanic-serving institutions, historically black institutions, Native American-focused institutions, and others in areas that can address the questions of urban and rural security as relates to technology.

And if you would answer those questions, I would appreciate it very much. And I thank the gentlemen for their testimony.

Mr. SASTRY. You have certainly hit the issues that are most important to the research community. Our sense, too, is that it would be useful to have a focused Federal effort in cybersecurity research, and a focused effort which, in fact, involves groups of institutions across the length and breadth of the Nation.

There is a very, very substantial educational agenda, and the educational agenda does indeed need to reach out to every corner, as you have correctly pointed out. I am in complete agreement.

Now, the questions about—I do believe that DHS and HSARPA could be the place where cybersecurity research could be given marquis status and then be adequately funded and adequately managed. And I felt that the DARPA model was actually a pretty effective model for doing this. The Defense Advance Research Projects Agency, the DARPA model, was an executive model for managing—this is HSARPA.

Ms. JACKSON-LEE. You would encourage the creations of consortiums with joint working relationships with universities around the Nation?

Mr. SASTRY. Right. The coalitions, of course, could be created by the institutions themselves, or in the form of research programs in the DARPA model where you actually bring institutions together, and a program manager, a Federal program manager then sort of builds the bridges between those institutions.

Ms. JACKSON-LEE. Do you see the need also for enhancing experts within the minority communities, because we are certainly limited in the Ph.D. candidates and Ph.D. graduates from those communities?

Mr. SASTRY. That is absolutely true. And that is true all the way from the high school level up all of the way through the graduate programs and the faculty as well.

Ms. JACKSON-LEE. Anyone else?

Mr. BELLOVIN. A national research counsel panel I was on noted that—concluded that today there probably could not be a massive disaster caused by a pure cyberattack, something close to the scale of 9/11. It doesn't mean it can't happen in the future. As we become more networked, as industrial processes, so-called SCADA systems, controlled power lines and industrial processes and so on, as things become more networked, the danger will increase. We have a few years before we are there. We need to take precautions right now.

And I would note that everybody's computers can be leveraged for launching attacks. There has been reports in the papers in the last few weeks about personal computers being hacked to serve spammers and pornographers and so on, which means that anybody's computer in every sector of the society, we need to learn how to secure these. And individuals need to learn how to protect things, too.

Ms. JACKSON-LEE. Thank you.

Mr. WOLF. There is a long list of research topics that need to be done, and clearly we need to leverage everybody in terms of working on those topics. So the idea of having some sort of coordinated effort in terms of where research—who is doing what I think is needed. We have done a lot of outreach recently with DARPA, NSF, academics, et cetera, to try to understand where research is being done to leverage all of that.

Second, we are going out to the academic institutions with our list to try to get some help in terms of doing the research, and that is all universities that are out there.

And your other comment about the—sort of the threat. I am not sure we really understand the threat in terms of how serious an attack on the infrastructure of the U.S. could be. I think there needs to be some focus on that.

Ms. JACKSON-LEE. Thank you.

Thank you, Mr. Chairman.

Mr. THORBERRY. I thank the gentlelady.

As the witnesses know, we do have votes on. I am not going to ask you to stay during these votes. So, with each of your permission, what I would like to do is submit some additional questions in writing to you. I think there are a number of areas that you have touched on that I want to follow up, including this whole software verification issue, this issue of translating research into the real world, which I think is a major, important issue. The whole human factors things that you all have talked about, about government research and how it affects the private market, you don't have to write those down, we will send those to you in writing.

Mr. THORBERRY. But needless to say, you all have touched on a number of things that have been very helpful to us. I want to

thank each of you for taking the time to be here and to be with us today, and with that, this hearing stands adjourned.
[Whereupon, at 11:45 a.m., the subcommittee was adjourned.]

