AUTHENTICATED
U.S. GOVERNMENT
INFORMATION
GPO

CYBERSECURITY RESEARCH AND DEVELOPMENT: CHALLENGES AND SOLUTIONS

HEARING

BEFORE THE

SUBCOMMITTEE ON TECHNOLOGY &
SUBCOMMITTEE ON RESEARCH

COMMITTEE ON SCIENCE, SPACE, AND TECHNOLOGY

HOUSE OF REPRESENTATIVES

ONE HUNDRED THIRTEENTH CONGRESS

FIRST SESSION

TUESDAY, FEBRUARY 26, 2013

Serial No. 113–6

Printed for the use of the Committee on Science, Space, and Technology



Available via the World Wide Web: http://science.house.gov

U.S. GOVERNMENT PRINTING OFFICE
79–926PDF WASHINGTON : 2013

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) 512–2104 Mail: Stop IDCC, Washington, DC 20402–0001

COMMITTEE ON SCIENCE, SPACE, AND TECHNOLOGY

HON. LAMAR S. SMITH, Texas, *Chair*

DANA ROHRABACHER, California
RALPH M. HALL, Texas
F. JAMES SENSENBRENNER, JR., Wisconsin
FRANK D. LUCAS, Oklahoma
RANDY NEUGEBAUER, Texas
MICHAEL T. McCAUL, Texas
PAUL C. BROUN, Georgia
STEVEN M. PALAZZO, Mississippi
MO BROOKS, Alabama
RANDY HULTGREN, Illinois
LARRY BUCSHON, Indiana
STEVE STOCKMAN, Texas
BILL POSEY, Florida
CYNTHIA LUMMIS, Wyoming
DAVID SCHWEIKERT, Arizona
THOMAS MASSIE, Kentucky
KEVIN CRAMER, North Dakota
JIM BRIDENSTINE, Oklahoma
RANDY WEBER, Texas
CHRIS STEWART, Utah
VACANCY

EDDIE BERNICE JOHNSON, Texas
ZOE LOFGREN, California
DANIEL LIPINSKI, Illinois
DONNA F. EDWARDS, Maryland
FREDERICA S. WILSON, Florida
SUZANNE BONAMICI, Oregon
ERIC SWALWELL, California
DAN MAFFEI, New York
ALAN GRAYSON, Florida
JOSEPH KENNEDY III, Massachusetts
SCOTT PETERS, California
DEREK KILMER, Washington
AMI BERA, California
ELIZABETH ESTY, Connecticut
MARC VEASEY, Texas
JULIA BROWNLEY, California
MARK TAKANO, California
VACANCY

SUBCOMMITTEE ON TECHNOLOGY

HON. THOMAS MASSIE, Kentucky, *Chair*

JIM BRIDENSTINE, Oklahoma
RANDY HULTGREN, Illinois
DAVID SCHWEIKERT, Arizona
LAMAR S. SMITH, Texas

FREDERICA S. WILSON, Florida
SCOTT PETERS, California
DEREK KILMER, Washington
EDDIE BERNICE JOHNSON, Texas

SUBCOMMITTEE ON RESEARCH

HON. LARRY BUCSHON, Indiana, *Chair*

STEVEN M. PALAZZO, Mississippi
MO BROOKS, Alabama
STEVE STOCKMAN, Texas
CYNTHIA LUMMIS, Wyoming
JIM BRIDENSTINE, Oklahoma
LAMAR S. SMITH, Texas

DANIEL LIPINSKI, Illinois
ZOE LOFGREN, California
AMI BERA, California
ELIZABETH ESTY, Connecticut
EDDIE BERNICE JOHNSON, Texas

CONTENTS

Tuesday, February 26, 2013

	Page
Witness List	2
Hearing Charter	3

Opening Statements

Statement by Representative Thomas Massie, Chairman, Subcommittee on Technology, Committee on Science, Space, and Technology, U.S. House of Representatives	6
Written Statement	6
Statement by Representative Lamar S. Smith, Chairman, Committee on Science, Space, and Technology, U.S. House of Representatives	7
Written Statement	7
Statement by Representative Frederica S. Wilson, Ranking Minority Member, Subcommittee on Technology, Committee on Science, Space, and Technology, U.S. House of Representatives	9
Written Statement	10
Statement by Representative Larry Bucshon, Chairman, Subcommittee on Research, Committee on Science, Space, and Technology, U.S. House of Representatives	11
Written Statement	11
Statement by Representative Daniel Lipinski, Ranking Minority Member, Subcommittee on Research, Committee on Science, Space, and Technology, U.S. House of Representatives	13
Written Statement	15

Witnesses:

Mr. Michael Barrett, Chief Information Security Officer, PayPal, Inc.	
Oral Statement	17
Written Statement	19
Dr. Frederick R. Chang, President and Chief Operating Officer, 21CT, Inc.	
Oral Statement	34
Written Statement	36
Ms. Terry Benzel, Deputy Director, Cyber Networks and Cyber Security, USC Information Sciences Institute	
Oral Statement	46
Written Statement	48
Discussion	62

Appendix I: Answers to Post-Hearing Questions

Mr. Michael Barrett, Chief Information Security Officer, PayPal, Inc.	80
Dr. Frederick R. Chang, President and Chief Operating Officer, 21CT, Inc.	81
Ms. Terry Benzel, Deputy Director Cyber Networks and Cyber Security, USC Information Sciences Institute	83

Page

Appendix II: Additional Material for the Record

Department of Homeland Security letter submitted by Representative Frederica S. Wilson, Ranking Minority Member, Subcommittee on Technology, Committee on Science, Space, and Technology, U.S. House of Representatives 88

National Science Foundation letter submitted by Representative Frederica S. Wilson, Ranking Minority Member, Subcommittee on Technology, Committee on Science, Space, and Technology, U.S. House of Representatives 91

CYBERSECURITY RESEARCH AND DEVELOPMENT: CHALLENGES AND SOLUTIONS

TUESDAY, FEBRUARY 26, 2013

HOUSE OF REPRESENTATIVES,
SUBCOMMITTEE ON RESEARCH
COMMITTEE ON SCIENCE, SPACE, AND TECHNOLOGY,
Washington, D.C.

The Subcommittees met, pursuant to call, at 10:01 a.m., in Room 2318 of the Rayburn House Office Building, Hon. Thomas Massie [Chairman of the Subcommittee on Technology] presiding.

LAMAR S. SMITH, Texas
CHAIRMAN

EDDIE BERNICE JOHNSON, Texas
RANKING MEMBER

Congress of the United States
House of Representatives
COMMITTEE ON SCIENCE, SPACE, AND TECHNOLOGY
2321 RAYBURN HOUSE OFFICE BUILDING
WASHINGTON, DC 20515–6301
(202) 225–6371
www.science.house.gov

Subcommittees on Technology and Research Hearing

Cybersecurity Research and Development: Challenges and Solutions

Wednesday, February 26, 2013
10:00 a.m. – 12:00 p.m.
2318 Rayburn House Office Building

Witnesses

Mr. Michael Barrett, Chief Information Security Officer, PayPal

Dr. Fred Chang, President & Chief Operating Officer, 21CT

Ms. Terry Benzel, Deputy Director, Cyber Networks and Cyber Security, University of Southern California Information Sciences Institute

U.S. HOUSE OF REPRESENTATIVES
COMMITTEE ON SCIENCE, SPACE, AND TECHNOLOGY
SUBCOMMITTEES ON TECHNOLOGY AND RESEARCH
HEARING CHARTER

Cybersecurity Research and Development: Challenges and Solutions

Tuesday, February 26, 2013
10:00 a.m. – 12:00 p.m.
2318 Rayburn House Office Building

Purpose

On Tuesday, February 26, 2013, the House Committee on Science, Space, and Technology's Research and Technology Subcommittees will examine cybersecurity research and development activities, including standards development and education and workforce training, and how they align with current and emerging threats. The hearing will also review the *Cybersecurity Enhancement Act of 2013* (H.R. 756) which reauthorizes cybersecurity programs at the National Institute of Standards and Technology (NIST) and the National Science Foundation (NSF).

Witnesses

- **Mr. Michael Barrett,** Chief Information Security Officer, PayPal Inc.
- **Dr. Fred Chang,** President & Chief Operating Officer, 21CT
- **Ms. Terry Benzel,** Deputy Director, Cyber Networks and Cyber Security, University of Southern California Information Sciences Institute

Overview

Information technology (IT) has evolved rapidly over the last decade, leading to markedly increased connectivity and productivity. The benefits provided by these advancements have led to the widespread use and incorporation of information technologies across major sectors of the economy. This level of connectivity and the dependence of our critical infrastructures on IT have also increased the vulnerability of these systems. Recent reports of cyber criminals and nation-states accessing sensitive information and disrupting services in both the public and private domains have risen steadily, heightening concerns over the adequacy of our cybersecurity measures. GAO found that the number of incidents reported by federal agencies has increased 782 percent from 2006 to 2012.[1] This dramatic increase is attributed in part to the proliferation and increased sophistication of hacking and cyber attack technology.

According to the Office of Management and Budget, Federal agencies spent $8.6 billion in fiscal year 2010 on cybersecurity and the Federal government has spent more than $600 billion on information technology in the last decade. In addition, the Federal government funds more than $400 million in cybersecurity research and development each year.

---

[1] GAO-13-187, Cybersecurity, National Strategy, Roles, and Responsibilities Need to Be Better Defined and More Effectively Implemented; http://www.gao.gov/assets/660/652170.pdf, February 2013

The National Science Foundation and the National Institute of Standards and Technology

NSF is the principal agency supporting unclassified cybersecurity research and development as well as technical education. NSF provides the largest federal investment in cyber-related research and development activities.

NSF has also made significant investments in cybersecurity education and workforce. The Scholarship for Service program provides awards to increase the number of students entering the computer security and information assurance fields, and to increase the capacity of institutions of higher education to produce professionals in these fields. NSF also offers Advanced Technological Education grants educating technicians for high-technology fields with a focus on two-year colleges.

NIST's core cybersecurity focus areas include: research, development, and specification; secure system and component configuration; and assessment and assurance of security properties of products and systems.

Title III of the E-Government Act (PL 107-347), entitled the Federal Information Security Management Act of 2002 (FISMA), tasked NIST with developing cybersecurity standards, guidelines, and associated methods and techniques for use by the Federal Government.

The Administration also tasked NIST in April 2011 with leading the National Strategy for Trusted Identities in Cyberspace (NSTIC), an initiative focused on establishing identity solutions and privacy-enhancing technologies to improve the security and convenience of sensitive online transactions.

Research and Development

Cybersecurity research and development efforts include working on the prevention of cyber attacks, detecting attacks as they are occurring, responding to attacks effectively, mitigating severity, recovering quickly, and identifying responsible parties.

Research and development provides a better understanding of weaknesses in systems and networks and of how to protect those systems and networks. The hearing will explore current government research and development investments to ensure they are properly focused to provide an effective level of cybersecurity. The Subcommittees will also assess the challenges to establishing national research and development priorities that strategically includes near-term, mid-term, and long-term goals.

Education and the Development of Cybersecurity Professionals

Well-trained professionals are essential to the implementation of security techniques in critical computer and network systems. Institutions of higher education are working to create and improve cyber education and training programs focused on ensuring an adequate number of trained professionals. Public awareness is also a critical component when it comes to protecting sensitive information. Federal agencies engaged in cybersecurity activities currently support a

number of cybersecurity education, training, and development programs. The Subcommittees will consider the coordination and implementation of these activities across Federal agencies.

Standards Development

The Subcommittees will examine NIST's current and future role in the development of benchmarks, guidelines, and standards for cybersecurity, in conjunction with other government agencies and the private sector.

Agency Coordination

Since 1991, Federal agencies have been required to set goals, prioritize investments, and coordinate activities in networking and information technology research and development. The Subcommittees will explore what measures have been taken to improve the coordination of federal cybersecurity research and development efforts and the best approach to improve the coordination of private sector critical infrastructure and network cybersecurity.

H.R. 756 the Cybersecurity Enhancement Act of 2013

H.R. 756, the *Cybersecurity Enhancement Act of 2013*, coordinates research and related activities conducted across the Federal agencies to better address evolving cyber threats. By strengthening agency coordination and cooperation on cybersecurity research and development efforts, the legislation addresses certain critical aspects of our nation's overall cybersecurity needs.

In addition to providing coordination of cybersecurity research across the federal government, the bill strengthens the efforts of the NSF and the NIST in the areas of cybersecurity technical standards and cybersecurity awareness, education, and workforce development.

The bill is identical to legislation in the 112th Congress, H.R. 2096, which passed the House by a vote of 395-10.

Presidential Executive Order on Improving Critical Infrastructure

On February 12th, President Obama signed an executive order (EO) on cybersecurity for critical infrastructure. Among other things, the EO encourages information sharing between public and private sectors and directs NIST to lead the development of a framework to reduce cyber risks to critical infrastructure. NIST is instructed to work with industry to identify existing voluntary consensus standards and industry best practices to incorporate into the framework. The Subcommittees will examine NIST's current and future role in carrying out this EO.

Chairman MASSIE. This joint hearing of the Subcommittee on Technology and the Subcommittee on Research will come to order.

Good morning. Welcome to today's joint hearing entitled "Cybersecurity Research and Development: Challenges and Solutions." In front of you are packets containing the written testimony, biographies, and truth-in-testimony disclosures for today's witnesses. Before we get started, since this is a joint hearing involving two Subcommittees, I want to explain how we will operate procedurally so all Members will understand how the question-and-answer period will be handled.

As always, we will alternate between the majority and minority Members and allow all Members an opportunity for questioning before recognizing a Member for a second round of questions. We will recognize those Members present at the gavel in order of seniority on the full Committee, and those coming in after the gavel will be recognized in order of arrival. I now recognize myself for five minutes for my opening statement.

We convene the first hearing of the Technology Subcommittee and the 113th Congress held jointly with my colleagues on the Research Subcommittee. This Subcommittee sits at the intersection of technology and innovation and is uniquely positioned to address topics affecting competitiveness of emerging high-growth industries. I look forward to learning from our witnesses today about cybersecurity research and development challenges, and I look forward to working with my colleagues to determine how we can eliminate barriers to entrepreneurship in our country going forward. In these difficult times, it is important that we continue to empower our Nation's innovators to maintain our economic competitiveness.

I now yield two minutes of my time to the Chairman of the full Committee, Mr. Smith of Texas.

[The prepared statement of Mr. Massie follows:]

PREPARED STATEMENT OF SUBCOMMITTEE ON TECHNOLOGY
CHAIRMAN THOMAS MASSIE

We convene the first hearing of the Technology Subcommittee in the 113th Congress, held jointly with my colleagues on the Research Subcommittee. This Subcommittee sits at the intersection of technology and innovation, and is uniquely positioned to address topics affecting competitiveness of emerging high-growth industries. I look forward to learning from our witnesses today about cybersecurity research and development challenges, and I look forward to working with my colleagues to determine how we can eliminate barriers to entrepreneurship in our country going forward. In these difficult times, it is important that we continue to empower our nation's innovators to maintain our economic competitiveness.

Chairman SMITH. Thank you, Mr. Chairman, for yielding me the balance of your time.

Mr. Chairman, the Preamble to the Constitution states that one of the primary responsibilities of our Federal Government is to provide for the common defense. More than 200 years later, the meaning has changed but the task remains the same. National defense in the digital age no longer just means protecting ourselves with arms against enemies who attack with traditional weapons. It now means protecting America from enemies who launch cyber attacks against our computers and networks.

Cyber attacks against U.S. Government and private sector networks are on the rise. In the last few weeks, some of America's largest companies have been hacked. Even the most sophisticated companies can be vulnerable to cyber attacks. Recent targets include Apple, Facebook, Yahoo!, the New York Times, and the Wall Street Journal. Various agencies of the Federal Government also have been the target of attacks and attempted attacks. Unfortunately, evidence suggests that foreign governments may be among those responsible.

Protecting America's cyber systems is critical to our economic and national security. Americans deserve better protection, and the Federal Government can help make sensitive information more secure. This challenge requires a thorough and comprehensive effort in both the public and private sectors. Private companies are increasing their investment in cybersecurity. Congress should support those efforts. Only Congress can provide the incentives and protections that would permit necessary information-sharing among companies, and more importantly, between private companies and the Federal Government.

Today's hearing examines an important step that we can take to foster the kind of cooperation that this challenge requires. The Cybersecurity Enhancement Act introduced by Committee Members Michael McCaul and Daniel Lipinski coordinates research and development activities to better address evolving cyber threats. The legislation promotes much-needed research and development to help create new technologies and standards that better protect America's information technology systems.

Cyber attacks threaten our national and economic security. To solve this problem, America needs a solution that involves a cooperation of many public and private sector entities. The McCaul/Lipinski legislation helps foster such an effort, which will make our computer systems more secure.

I hope we can learn how to improve the bill today and quickly advance it through this Committee.

Thank you, Mr. Chairman. I yield back the balance of your time.

[The prepared statement of Mr. Smith follows:]

PREPARED STATEMENT OF COMMITTEE CHAIRMAN LAMAR S. SMITH

The preamble to the Constitution states that one of the primary responsibilities of our federal government is to "provide for the common defense." More than two hundred years later, the meaning has changed but the task remains the same.

National defense in the digital age no longer just means protecting ourselves with arms against enemies who attack with traditional weapons. It now means protecting America from enemies who launch cyber attacks against our computers and networks.

Cyber attacks against U.S. government and private sector networks are on the rise. In the last few weeks, some of America's largest companies have been hacked. Even the most sophisticated companies can be vulnerable to cyber attacks. Recent targets include Apple, Facebook, Yahoo! the *New York Times* and the *Wall Street Journal.*

Various agencies of the federal government also have been the target of attacks and attempted attacks. Unfortunately, evidence suggests that foreign governments may be among those responsible.

Protecting America's cyber systems is critical to our economic and national security. Americans deserve better protection and the federal government can help make sensitive information more secure.

This challenge requires a thorough and comprehensive effort in both the public and private sectors. Private companies are increasing their investment in cybersecurity. Congress should support those efforts.

Only Congress can provide the incentives and protections that would permit necessary information sharing among companies, and more importantly, between private companies and the federal government.

Today's hearing examines an important step that we can take to foster the kind of cooperation that this challenge requires. The Cybersecurity Enhancement Act, introduced by Committee Members Michael McCaul and Daniel Lipinski, coordinates research and development activities to better address evolving cyber threats. The legislation promotes much-needed research and development to help create new technologies and standards that better protect America's information technology systems.

Cyber attacks threaten our national and economic security. To solve this problem, America needs a solution that involves the cooperation of many public and private sector entities. The McCaul-Lipinski legislation helps foster such an effort, which will make our computer systems more secure.

I hope we can learn how to improve the bill today and quickly advance it through this Committee.

Chairman MASSIE. Thank you. The Chair now recognizes Ms. Wilson for her opening statement.

Ms. WILSON. Thank you, Chairman Massie, for holding this joint hearing on cybersecurity, and thank you to our witnesses for being here today.

Before I begin, I would like to say that I am pleased to be the new Ranking Member of the Technology Subcommittee. As a longtime educator, principal, teacher, I am a big believer in the power of scientific innovation. Mr. Chairman, I am looking forward to working with you this Congress to help enable innovation that creates jobs and makes our Nation more secure.

Today's hearing is a perfect example of the work this Subcommittee can do to bolster national security. Cyber crimes are ever increasing. In fact, the number of attacks reported by federal agencies increased by 782 percent between 2006 and 2012. The threats to federal systems in our critical infrastructure are not only growing in number but in the level of sophistication. Over the last month alone, the New York Times, the Wall Street Journal, the Washington Post, Twitter, and Facebook have all confirmed that they have been the target of sophisticated cyber attacks. These crimes may include identity theft, intellectual property theft, service disruptions, and even espionage.

We are beginning to suffer the cost of cybercrime. A recent study found that cybercrime now costs a U.S. business 8.9 million on average per year. The problem is so pervasive that security experts now joke that there are only two types of American companies these days: those that have been hacked and those that don't know they have been hacked.

Earlier this month, the President signed an Executive Order that begins the process of strengthening our networks of critical infrastructure against cyber attacks by increasing information-sharing and establishing a framework for the development of standards and best practices. But the President also acknowledged that Congress must act to pass comprehensive cybersecurity legislation.

The bipartisan legislation introduced by our colleagues, Mr. McCaul and Mr. Lipinski, and under consideration today should be a part of this comprehensive package. I am looking forward to hearing any recommendations our witnesses might have about how to improve the legislation.

Additionally, I hope to hear more from our witnesses about their thoughts on the role the Executive Order outlines for NIST. In the past, Congress has asked NIST to bring the private sector together to accelerate the development of voluntary standards. It seems appropriate that NIST be tasked with the similar role in cybersecurity, especially in light of their expertise in this field.

Finally, I would be remiss if I did not mention the potential impact sequestration will have on our ability to deter, defend, and recover from cyber attacks. In a letter to Appropriations, the National Science Foundation indicated that vital investments in research and development would be jeopardized, and that one of the areas that could be impacted by sequestration is research into advances in cybersecurity.

The Department of Homeland Security Science and Technology Directorate plays a large role in the development and deployment

of cybersecurity technologies. The Directorate has indicated that under sequestration, they will have to cut their cybersecurity research by 30 percent, eliminating research and data, privacy, identity management, cybersecurity forensics, and security for cloud-based systems. The need to invest in research and development is critical as cyber threats continue to grow and involve. I hope we will not let sequestration delay and derail these essential investments.

Thank you, Mr. Chairman, and I yield back the balance of my time.

[The prepared statement of Ms. Wilson follows:]

PREPARED STATEMENT OF SUBCOMMITTEE ON TECHNOLOGY
RANKING MINORITY MEMBER FREDERICA S. WILSON

Thank you, Chairman Massie for holding this joint hearing on cybersecurity, and thank you to our witnesses for being here today. Before I begin, I'd like to say that I am pleased to be the new Ranking Member of the Technology Subcommittee. As a longtime educator, I am a big believer in the power of scientific innovation. Mr. Chairman, I am looking forward to working with you this Congress to help enable innovation that creates jobs and makes our nation more secure.

Today's hearing is a perfect example of the work this Subcommittee can do to bolster national security. Cyber crimes are ever-increasing. In fact, the number of attacks reported by federal agencies increased by 782 percent between 2006 and 2012. The threats to federal systems and our critical infrastructure are not only growing in number, but in the level of sophistication.

Over the last month alone, The New York Times, The Wall Street Journal, The Washington Post, Twitter, and Facebook have all confirmed that they have been the target of sophisticated cyber attacks. These crimes may include identity theft, intellectual property theft, service disruptions, and even espionage.

We're beginning to suffer the costs of cybercrime. A recent study found that cybercrime now costs a U.S. business $8.9 million on average per year. The problem is so pervasive that security experts now joke that there are only two types of American companies these days: *those that have been hacked and those that don't know they've been hacked.*

Earlier this month, the President signed an executive order that begins the process of strengthening our networks and critical infrastructure against cyber attack by increasing information sharing and establishing a framework for the development of standards and best practices. But the President also acknowledged that Congress must act to pass comprehensive cybersecurity legislation.

The bipartisan legislation introduced by our colleagues Mr. McCaul and Mr. Lipiniski, and under consideration today, should be part of this comprehensive package. I am looking forward to hearing any recommendations our witnesses might have about how to improve the legislation. Additionally, I hope to hear more from our witnesses about their thoughts on the role the executive order outlines for NIST. In the past, Congress has asked NIST to bring the private sector together to accelerate the development of voluntary standards. It seems appropriate that NIST be tasked with a similar role in cybersecurity—especially in light of their expertise in this field.

Finally, I'd be remiss if I did not mention the potential impact sequestration will have on our ability to deter, defend, and recover from cyber attacks. In a letter to appropriators, the National Science Foundation indicated that "vital investments in research and development would be jeopardized" and that one of the areas that could be impacted by sequestration is research into advances in cybersecurity.

The Department of Homeland Security's Science and Technology Directorate plays a large role in the development and deployment of cybersecurity technologies. The Directorate has indicated that under sequestration they will have to cut their cybersecurity research by 30 percent, eliminating research in data privacy, identity management, cybersecurity forensics, and security for cloud based systems.

The need to invest in research and development is critical as cyber threats continue to grow and evolve. I hope we will not let sequestration delay and derail these essential investments.

Chairman MASSIE. Thank you, Ms. Wilson. I look forward to working with you as well on this Committee.

The Chair now recognizes the Chairman of the Subcommittee on Research, Mr. Bucshon, for his opening statement.

Mr. BUCSHON. Thank you, Mr. Chairman. And good morning to everyone. I am pleased that we are holding a hearing today on such an important topic.

According to a recent report published by the Government Accountability Office, there were nearly 50,000 cybersecurity incidents reported by federal agencies in 2012. Considering that number was 5,500 in 2006, there is no doubt that addressing cybersecurity needs is critical to global economic competitiveness and national security interests of our Nation.

In December 2012, the Center for Applied Cybersecurity Research at Indiana University held a roundtable on cyber threats, objectives, and responses. This issue impacts everyone from children using the Internet in their homes to government and industry officials trying to ensure our domestic infrastructure is protected from cyber terrorists.

During the Research Subcommittee hearing on February 14 on Networking and Information Technology Research and Development, or NITRD, witnesses testified about the cybersecurity threats our Nation faces and emphasized that cooperation is required for stakeholders to research and design ways in which to build and maintain safer computer network infrastructures. The NITRD program, which was the primary subject of that hearing, is the coordinating body which the McCaul/Lipinski Cybersecurity Enhancement Act appropriately utilizes to establish a strategic plan for specific cybersecurity research.

I am encouraged that the legislation we are discussing today enhances the education and development of information technology professionals, including those who work in the areas of computer systems, computer security, and cybersecurity.

I look forward to hearing from our witnesses about their experiences and their recommendations on addressing America's cybersecurity challenges.

I now yield the balance of my time to Chairman McCaul.

[The prepared statement of Mr. Bucshon follows:]

PREPARED STATEMENT OF SUBCOMMITTEE ON RESEARCH CHAIRMAN LARRY BUCSHON

According to a recent report published by the Government Accountability Office, there were nearly 50,000 cybersecurity incidents reported by federal agencies in 2012. Considering that number was 5,500 in 2006, there is no doubt that addressing cybersecurity needs is critical to global economic competitiveness and national security interests of our nation.

In December of 2012, the Center for Applied Cybersecurity Research at Indiana University held a "Roundtable on Cyber Threats, Objectives, and Responses." This issue impacts everyone: from children using the Internet in their homes to government and industry officials trying to ensure our domestic infrastructure is protected from cyber terrorists.

During the Research Subcommittee hearing on February 14 on Networking and Information Technology Research and Development (NITRD), witnesses testified about the cybersecurity threats our nation faces and emphasized that cooperation is required for stakeholders to research and design ways in which to build and maintain safer computer network infrastructures. The NITRD program, which was the primary subject of that hearing, is the coordinating body which the McCaul-Li-

pinski Cybersecurity Enhancement Act appropriately utilizes to establish a strategic plan for specific cyber security research.

I am encouraged that the legislation we are discussing today enhances the education and development of information technology professionals, including those who work in the areas of computer systems, computer security, and cybersecurity.

I look forward to hearing from our witnesses about their experiences and their recommendations on addressing America's cybersecurity challenges.

Mr. MCCAUL. Thank you, Chairman Bucshon.

I want to thank Chairman Massie, Chairman Smith, Ranking Members Lipinski and Wilson for allowing me to introduce this bill once again. Again, I believe this is the third time we have introduced this. Hopefully, the third time is a charm and we will get this important legislation passed. It passed overwhelmingly in two Congresses. I do believe this is the Congress where we will get cybersecurity legislation passed through the House, the Senate, and signed by the White House.

It is imperative as we hear reports almost every day of hackings taking place not only within the critical infrastructures but within our Federal Government. The report about the Chinese military hacking into our military systems, stealing our military secrets, the attacks recently from Iran against Aramco in the Persian Gulf and against our financial institutions in the United States, and of course Russia, one of the most sophisticated countries that continue to hack this country on a daily basis.

Whether it is criminal, whether it is espionage, or whether it cyber warfare, we cannot afford to wait any longer. The White House has acted through an Executive Order. I think it is imperative now that the Congress act and legislate as we are supposed to be doing. It is not a question of if, but when the next—or when a cyber Pearl Harbor will occur. And that is why I have worked very closely with my good friend Congressman Lipinski to bolster our Nation's cybersecurity research and development.

On February the 15th, we introduced this bill once again, H.R. 756, the Cybersecurity Enhancement Act, which is identical to the legislation passed overwhelmingly by the House last Congress. It improves the coordination in government providing for a strategic plan to assess the cybersecurity risk and guide the overall direction of the federal cyber research and development. It updates—and this responsibility is to develop security standards for Federal computer systems and processes for agencies to follow.

Our bill also establishes a federal university private sector task force to coordinate research and development, improving the training of cybersecurity professionals, and continues much-needed cybersecurity research and development programs at the National Science Foundation and the National Institute of Standards and Technology.

Again, I would like to thank my colleague Chairman Smith for allowing me to introduce this bill once again. I appreciate your support for this bill, my colleague from Texas. And I look forward to working with my colleagues on this Committee to find solutions to the challenges of cyber research and development.

And with that, I yield back.

Chairman MASSIE. Thank you, Mr.——

Mr. BUCSHON. I yield back.

Chairman MASSIE. Okay. Thank you, Mr. McCaul. And thank you, Mr. Bucshon.

The Chair now recognizes Mr. Lipinski for his opening statement.

Mr. LIPINSKI. Thank you, Chairman Massie.

I want to thank you, Chairman Smith and Chairman Bucshon, for holding this hearing to examine the serious cybersecurity chal-

lenges faced by our Nation and what we can do to facilitate solutions, including the Cybersecurity Enhancement Act that Mr. McCaul said we recently reintroduced and I know that we have passed this overwhelmingly in a Democratic House. In a Republican House, hopefully, this time we can get it all the way through because our country especially needs it as the threats grow every year.

Now, I want to echo my colleague's remarks about the nature and severity of the challenges we face in cybersecurity in both the public and private sectors. Four years ago, when we began working on this legislation, I said I had no doubt that our use of the Internet and other communication networks would continue to grow and evolve, and that threats from individual hackers, criminal syndicates, and even other governments would grow and evolve, too. Today, it remains difficult to imagine just how much more we will simultaneously benefit from and be made more vulnerable by information technology.

Hacking is no longer just a realm of computer whizzes. Today, anyone can rent a botnet or gain access to other sophisticated hacking tools with just a few keystrokes and less than $100.

Cybercrime threatens our national security, our critical infrastructure, businesses of all sizes, and every single American. As such, reducing our risk and improving the security of cyberspace will take the collective effort of both the Federal Government and the private sector, as well as scientists, engineers, and the general public.

With respect to that collective effort, I need to emphasize the importance of research into the social and behavioral aspects of cybersecurity. People are perhaps the most significant part of our IT infrastructure, but they are also the weakest link. Many cyber attacks are successful because of human error, bad cyber hygiene such as unwittingly opening a malicious email. Having the most sophisticated security systems available won't make any difference if users don't change factory sets of all passwords or if they set easy-to-crack passwords. Understanding the human element and educating users to practice good cyber hygiene is necessary to combating threats and reducing risk.

Mr. McCaul and I are hopeful that our R&D bill will be part of a comprehensive bipartisan cybersecurity bill. Previous efforts to move a larger bill have stalled over some significant policy disagreements, but I am hopeful that we will be able to resolve our differences and I look forward to working with both my colleagues and the Administration to ensure the development of a strong cybersecurity strategy this Congress.

However, I am also concerned that top-line cuts to our federal R&D budgets will have a negative impact on any long-term cybersecurity strategy. So we must also take actions to mitigate the impact of those cuts.

Today, we will hear from witnesses who are actively engaged in efforts to improve the security of our digital infrastructure. I look forward to their valuable insights and the challenges we face in tackling this complex issue and the role of cybersecurity R&D and education in any comprehensive solutions.

I thank you, Mr. Chairman. I yield back the balance of my time.

[The prepared statement of Mr. Lipinski follows:]

PREPARED STATEMENT OF SUBCOMMITTEE ON RESEARCH
RANKING MINORITY MEMBER DANIEL LIPINSKI

I want to thank both Chairman Massie and Chairman Bucshon for holding this hearing to examine the serious cybersecurity challenges faced by our nation. In particular, I look forward to hearing feedback from our witnesses on H.R. 756, The Cybersecurity Enhancement Act, that I recently reintroduced along with Mr. McCaul.

I echo my colleagues' remarks about the nature and severity of the challenges we face in cybersecurity in both the public and private sectors. Four years ago when I began working on this legislation I said that I had no doubt that our use of the Internet and other communication networks would continue to grow and evolve, and that threats from individual hackers, criminal syndicates, and even other governments would grow and evolve too.

Today it remains difficult to imagine just how much more we will simultaneously benefit from, and be made more vulnerable by, information technology. Hacking is no longer just the realm of computer whizzes. Today, anyone can "rent" a botnet or gain access to other sophisticated hacking tools with just a few key strokes and less than a hundred dollars.

Cybercrime threatens our national security, our critical infrastructure, businesses of all sizes, and every single American. As such, reducing our risk and improving the security of cyberspace will take the collective effort of both the Federal government and the private sector, as well as scientists, engineers, and the general public.

With respect to that collective effort, I need to emphasize the importance of research into the social and behavioral aspects of cybersecurity. People are perhaps the most significant part of our IT infrastructure, but they are also the 'weakest link.' Many cyber attacks are successful because of human error—bad cyber hygiene—such as unwittingly opening a malicious email. Having the most sophisticated security systems available won't make any difference if users don't change factory-set default passwords or they set easy to crack passwords. Understanding the human element and educating users to practice good cyber hygiene is necessary to combating threats and reducing risk.

Mr. McCaul and I are hopeful that our R&D bill will be part of a comprehensive, bipartisan cybersecurity bill. Previous efforts to move a larger bill have stalled over some significant policy disagreements, but I am hopeful that we will be able to resolve our differences and I look forward to working with both my colleagues and the Administration to ensure the development of a strong cybersecurity strategy this Congress.

However, I am also concerned that top line cuts to our federal R&D budgets will have a negative impact on any long-term cybersecurity strategy. So we must also take actions to mitigate the impact of those cuts.

Today, we will hear from witnesses who are actively engaged in efforts to improve the security of our digital infrastructure. I look forward to their valuable insight into the challenges we face in tackling this complex issue and the role of cybersecurity R&D and education in any comprehensive solution.

Chairman MASSIE. Thank you, Mr. Lipinski.

If there are Members who wish to submit additional opening statements, your statements will be added to the record at this point.

It is now time to introduce our panel of witnesses. I yield to Ms. Lofgren of California, who will introduce our first witness.

Ms. LOFGREN. Well, thank you very much, Mr. Chairman. And it is indeed an honor to introduce Michael Barrett, who is the Chief Information Security Officer for PayPal, located in San Jose, California. He is the, as I say, the Chief Information Security Officer for PayPal, and in his role, he is responsible for ensuring the security of PayPal's 113 million users worldwide.

Prior to joining PayPal, he was Vice President of Security and Utility Strategy at American Express, where he helped defined the company's Information Security Program, and in prior years, he was President of the Liberty Alliance, an Open Standards Consortium focused on identity management standards and guidelines. He was the driving force behind the introduction and standardization of the Alliance's federated identity concepts, and he also co-chaired its Identity Threat Prevention Working Group.

He was twice named one of the 50 most powerful people in networking by Network World magazine, and it is wonderful that he is testifying today about our bill that focuses on NIST and NSF, but I am also pleased that he has identified in his testimony certain outdated statutes like EPCA, the Electronic Communications Privacy Act, that have prevented anti-cybercrime-related programs, which is also an important service that he is performing for the Committee today.

So thank you for letting me introduce this important witness who comes from back home.

And I yield back.

Chairman MASSIE. Thank you, Ms. Lofgren.

I recognize Chairman Smith to introduce our second witness.

Chairman SMITH. Thank you, Mr. Chairman.

Chairman, our second witness, Dr. Frederick Chang, is a President and Chief Operating Officer of 21CT. 21CT appropriately is headquartered within Texas' 21st Congressional District, which is home to Cyber City USA, otherwise known as San Antonio, thanks in part to technology organizations like Dr. Chang's.

Dr. Chang brings to us today with 30 years of public and private sector cybersecurity knowledge serving as the Director of Research at the National Security Agency and then in an executive role at SBC Communications. Additionally, he has served in academia at both the University of Texas in San Antonio and the University of Texas in Austin. He received his B.A. degree from the University of California San Diego and both his M.A. and Ph.D. degrees from the University of Oregon.

We welcome you, Dr. Chang.

And I yield back, Mr. Chairman.

Chairman MASSIE. Thank you, Chairman Smith.

Our final witness is Ms. Terry Benzel, the Deputy Director of Cyber Networks and Cyber Security of the USC Information Sciences Institute.

As our witnesses should know, spoken testimony is limited to five minutes each after which Members of the Committee have five minutes each to ask questions. Your written testimony will be included in the record of this hearing.

I now recognize our first witness, Mr. Michael Barrett, for five minutes.

STATEMENT OF MR. MICHAEL BARRETT,
CHIEF INFORMATION SECURITY OFFICER, PAYPAL, INC.

Mr. BARRETT. Chairman Bucshon, Chairman Massie, Ranking Member Lipinski, Ranking Member Wilson, and Members of the Subcommittee, thank you for the opportunity to testify today about what PayPal and the eBay Inc. family of companies are doing to protect our users from the growing cybersecurity challenges facing Internet-enabled companies and what our Nation's policymakers can do to assist us in tackling these problems.

My name is Michael Barrett and I am the Chief Information Security Officer for PayPal. EBay and PayPal connects millions of buyers and sellers across the globe through eBay Marketplaces, PayPal, GSI, and other mobile-based businesses. And we believe all sustainable 21st century retail business models will use the Internet and mobile technology. However, as the Internet and mobile platforms become more attractive to consumers and businesses alike, they also attract criminals. Companies like PayPal will continue to work to protect the safety and security of our platform and our users.

However, we believe that the traditional technical measures alone cannot significantly move the trend line and that there are concrete steps that industry and policymakers should take to significantly mitigate the impact of cybercrime. For example, on a daily basis Internet companies are run into sites where they have been compromised and they are used as "phishing" or "spoof sites."

Recognizing the growing threat, PayPal launched an industry standards program called DMARC, which is intended to increase trust and combat email deception and fraud. DMARC allows senders to experience consistent authentication results for their messages at AOL, Gmail, Hotmail, Yahoo!, and any other email receiver implementing DMARC. The program removes the guesswork from the receiver's handling of any failed messages, limiting or eliminating the user's exposure to potentially fraudulent and harmful messages. In its first year, DMARC protected 60 percent of the world's email inboxes and rejected hundreds of millions of potentially fraudulent messages.

In addition to email authentication, we have also been engaged in efforts to create a reliable identity management system. We have participated in two different programs: the National Strategy for Trusted Identities in Cyberspace (NSTIC) and the Fast Identity Online Alliance, or FIDO.

NSTIC is a White House initiative led by the National Institute of Standards and Technology, which is intended to work collaboratively with all interested stakeholders to improve the privacy, security, and convenience of sensitive online transactions. PayPal will be offering more services to our customers over the coming months that directly support both the NSTIC vision, which we expect will

result in many new benefits to both our customers and the Internet overall.

PayPal was also one of the cofounders of the FIDO Alliance, which is intended to address the lack of interoperability among strong authentication solutions, as well as the problems users face with creating and remembering multiple usernames and passwords. By giving the option to replace passwords with authentication methods embedded in hardware, it can be used in biometric tools such as fingerprint scanners, voice and facial recognition, or more traditional security methods. Our goal is to provide an easier and safer solution to every company, vendor, and organization that needs to verify a user's identity.

Although it is the responsibility of industry leaders like PayPal to ensure the safety and security of our platforms and our users, federal policymakers have an important role to play in creating a secure Internet and mobile ecosystem. What we have found from our years of combating cybercrime is that quantifying the forecast is difficult, if not impossible, because many incidents are not reported. Estimates of the magnitude and scope of cybercrime vary widely, making it difficult for policymakers and industry to fully understand the problem and the level of effort that will be needed to combat it.

We recommend that policymakers fund some research that helps fill some of the information gaps that currently exist as it relates to cybercrime. We believe that this research will be a critical tool in arming policymakers, law enforcement, and industry against the growing threat of cybercrime.

In addition, PayPal appreciates the bipartisan efforts of the Committee to create a legislative framework that creates innovative solutions to issues such as cybersecurity R&D, education and workforce training, and standards development. Importantly, it achieves these ends without creating undesired side effects, and we welcome the opportunity to work with the Committee on these priorities.

To conclude, it is our hope that in the years to come the challenges we face today from cybercrime will be a faint memory. But until then, PayPal is committed to partnering with policymakers and private and public stakeholders to ensure that everything we do in our power to create an ecosystem that is safe and secure.

I appreciate the opportunity to testify before the Committee and I look forward to your questions.

[The prepared statement of Mr. Barrett follows:]

TESTIMONY OF

Michael Barrett
Vice President, Information Risk Management
Chief Information Security Officer
PayPal
eBay Inc.

BEFORE THE
United States House of Representatives
Committee on Science, Space and Technology
Subcommittee on Research and Subcommittee on Technology

"Cyber R&D Challenges and Solutions"

PRESENTED
Rayburn House Office Building, Room 2318
February 26, 2013
10:00 AM

Testimony of

Michael Barrett
Vice President, Information Risk Management
Chief Information Security Officer
PayPal
eBay Inc.

Before the

United States House of Representatives
Committee on Science, Space and Technology
Subcommittee on Research and Subcommittee on Technology

"Cyber R&D Challenges and Solutions"

Presented:
Rayburn House Office Building, Room 2318
February 26, 2013
10:00 AM

Chairman Bucshon, Chairman Massie, Ranking Member Lipinski, Ranking Member Wilson, and Members of the Subcommittee: Thank you for the opportunity to testify today about PayPal and what we, and the eBay Inc. family are doing to protect our users from the growing cybersecurity challenges that are facing Internet-enabled companies large and small and what our nation's policymakers can do to assist us in tackling this growing problem.

My name Michael Barrett and I am the Vice President of Informational Risk Management and Chief Information Security Officer for PayPal, a member of the eBay Inc. family. Founded in 1995 in San Jose, Calif., eBay Inc. connects millions of buyers and sellers globally on a daily basis through eBay, the world's largest online marketplace, and PayPal, which enables individuals and businesses to securely, easily, and quickly send and receive online

payments. We also reach millions through specialized marketplaces such as StubHub, the world's largest ticket marketplace, and eBay classifieds sites. And through our company GSI Commerce, eBay Inc. has become the leading provider of eCommerce and interactive marketing services for many of the world's premier brands and retailers, such as Toys R Us, Ralph Lauren and Dick's Sporting Goods.

Additionally, eBay Inc. is actively working to revolutionize global commerce with the recent additions of mobile technology companies WHERE, Milo, Zong and others combined with the seasoned services of eBay Marketplaces Mobile and PayPal Mobile. In fact, in 2012, eBay Inc. generated nearly $14 billion in global mobile sales. PayPal Mobile also experienced great popularity across the globe, with over 17 million consumers in over 80 markets worldwide. Our global consumers bought everything from cars, clothing, shoes, electronics, and toys from eBay and PayPal's mobile applications.

eBay Inc. is a very diverse family of businesses supporting millions of users ranging from individual consumers to merchants and retailers of every shape and size. As enablers of commerce, eBay Inc. and PayPal facilitate consumers buying just about anything whether on or offline. We enable consumers to pay online, pay with a phone, pay with a card from your wallet or pay with nothing but a phone number and a secure pin. All sustainable 21st Century retail business models, large and small alike, will use the Internet and mobile technology tools and it is our hope to be their partner in that venture.

With this growing trend in mind, eBay Inc. and PayPal recognize that our success and the success of our retail partners are dependent on our ability to engender consumer trust and confidence. It is our belief that without trust, the Internet and mobile marketplaces will fail to reach their full potential. Security and trust are mutually reinforcing. It is hard to build consumer trust without ensuring the safety and security of a consumer's personal information, whether it is financial data, transaction history, etc.

To foster that trust, we've worked to meet customer expectations with every product we offer. PayPal and its "shop without sharing" design, was created to offer a secure alternative to

traditional payment systems. Security is one of the fundamental building blocks of the PayPal services. The beauty of PayPal is that it allows consumers to send money or pay for a good or service without ever having to expose their credit card or bank account information to merchants or other PayPal users. It allows consumers to shop online or on their mobile device without having to share the most sensitive personally identifiable information, financial and banking information. Not only does this security-enhancing technology allow consumers to fully enjoy the convenience of online and mobile commerce without worrying about safety and security concerns, but it also allows merchants to receive payments without the cost and potential liability associated with processing and securing financial information.

However, as the Internet and mobile platforms become more attractive to consumers and businesses alike, it also attracts criminals and bad actors that are looking to profit by exploiting Internet companies and users. And unfortunately, their behavior has furthered the perception of certain individuals that the Internet and mobile platforms are unsafe and therefore unsuitable for everyday use. Companies like eBay and PayPal will continue to fight back against this perception and work to protect the safety and security of our platform and our users. However, as cybercriminal activities slowly get worse, we believe that traditional technical measures alone cannot significantly move the trend line in a positive direction and that there are concrete steps that industry and policymakers should take to significantly mitigate the impact of cybercrime and reduce its frequency.

I would like to take the next few minutes to highlight some of the successful security-related programs that my team has engaged in over the last few years and also recommend some areas that would benefit from government engagement.

PayPal's Efforts on Cybersecurity

DMARC: Domain-based Message Authentication, Reporting & Conformance

On a daily basis, Internet companies, including PayPal, run into sites that have been compromised and are being used as "phishing" or "spoof" sites, which are intended to defraud

Internet companies and their users by various means. With the rise of the social Internet and the ubiquity of e-commerce, spammers and phishers have a tremendous financial incentive to compromise user accounts, enabling theft of passwords, bank accounts, credit cards, and more. Unfortunately, email is very easy to spoof and criminals have found this activity to be an opportunity to exploit user's trust of well-known brands. By simply inserting the logo of a well-known brand into an email, spoofers give their emails instant legitimacy with many users.

Recognizing the growing threat from these types of behaviors, PayPal, in coordination with other industry partners, launched a program over a year ago called DMARC, which is meant to increase email trust and combat rampant email deception and fraud, such as spam and phishing. DMARC, which stands for Domain-based Message Authentication, Reporting & Conformance, builds on previous email authentication advancements, with strong protection of the author's address and creating a feedback loop from receivers back to legitimate email senders. DMARC standardizes how email receivers perform email authentication using the well-known Sender Policy Framework (SPF) and Domain Keys Identified Mail (DKIM) mechanisms. This means that senders will experience consistent authentication results for their messages at AOL, Gmail, Hotmail, Yahoo! and any other email receiver implementing DMARC. The program removes the guesswork from the receiver's handling of any failed messages, limiting or eliminating the user's exposure to potentially fraudulent and harmful messages. DMARC also provides a way for the email receiver to report back to the sender about messages that pass and/or fail DMARC evaluation.

In its first year, DMARC:

- Protected 60 percent of the world's email boxes or 1.976 billion of the estimated 3.3 billion email boxes worldwide. Protected 80 percent of US typical consumer mailboxes;
- Has been adopted by the world's largest consumer email providers– AOL, Comcast, Google, Mail.ru, Microsoft, NetEase, Xs4All, and Yahoo!;
- Can claim 50 percent of the top 20 sending domains publish a DMARC policy, with 70 percent of those domains asserting a policy that directs receivers to take action against unauthenticated messages; and

- Rejected hundreds of millions of potentially fraudulent messages. As an example, in November and December 2012, more than 325 million messages were rejected as purporting to be "From" domains with a DMARC reject policy.

Identity Management and Authentication

The Internet, especially with recent rapid mobile and cloud expansion, exposes users and enterprises, more than ever before, to fraud. We at PayPal believe it is critical to know who you're dealing with on the Internet at all times. Therefore, my team has also been very engaged in efforts to create a reliable identity management system to promote identity and stronger authentication. As a company that facilitates secure online and mobile financial transactions, it is critical that we have the ability to authoritatively authenticate our users. We strongly support efforts to create a workable "Identity Ecosystem" — where stakeholders work to protect individuals, businesses, and public agencies from the high costs of cyber crimes, like identity theft and fraud, while simultaneously helping to ensure that the Internet continues to support innovation and a thriving marketplace of products and ideas. To accomplish this goal, we have participated in two different programs, The National Strategy for Trusted Identities in Cyberspace (NSTIC) and The Fast Identity Online (FIDO) Alliance.

As many of you know, NSTIC is a White House initiative, led by the National Institute of Standards and Technology, which is intended to work collaboratively with the private sector, advocacy groups, public sector agencies, and other organizations to improve the privacy, security, and convenience of sensitive online transactions. The program has been mostly led by the private sector, in partnership with the federal government, consumer advocacy organizations, privacy experts, state and local agencies, and others. Organizations representing 18 different business and infrastructure sectors and 70 different nonprofit and federal advisory groups have participated in the development of the "Strategy".

NSTIC differs from past efforts to encourage trusted IDs in several ways. From the outset, the NSTIC has involved the private sector as a partner in the effort. For instance, members of my team have served as significant contributors to the Identity Ecosystem Steering Group (IDESG) and Brett McDowell of PayPal current chairs the IDESG Management Council.

In our work at the IDESG we've worked diligently to ensure that the rules and practices put in place do actually fulfill the promise of NSTIC.

We have consistently advocated that trustworthy online identity is a key component of a healthy Internet ecosystem. PayPal will be offering more services to our customers over the coming months that directly support the NSTIC vision, which we expect will result in many new benefits to both our customers and the Internet overall.

PayPal was also one of the co-founders of The Fast Identity Online (FIDO) Alliance. Formed in July 2012, with Lenovo, Nok Nok Labs, Infineon and others, the goal of the Alliance is to address the lack of interoperability among strong authentication devices as well as the problems users face with creating and remembering multiple usernames and passwords. The FIDO Alliance plans to change the nature of authentication by developing specifications that define an open, scalable, interoperable set of mechanisms that supplant reliance on passwords to securely authenticate users of online services. This new standard for security devices and browser plugins will allow any website or cloud application to interface with a broad variety of existing and future FIDO-enabled devices that the user has for online security.

How it works is that our protocol-based model will automatically detect when a FIDO-enabled device is present, meaning that end users from the banking, corporate, public sector or consumer arenas could be given the option to replace passwords with authentication methods embedded in hardware. It can be deployed in biometric tools such as fingerprint scanners, voice and facial recognition technology, or more traditional security aids such as one-time password (OTP) tokens or trusted platform models.

The FIDO Alliance is a private sector and industry-driven collaboration to combat the very real challenge of confirming every user's identity online. By giving users choice in the way they authenticate and taking an open-based approach to standards, we can make universal online authentication a reality. We wanted to provide an easier and safer solution to every company, vendor, and organization that needs to verify user identity.

The National Cyber Security Alliance and Promoting Education Awareness

As a responsible corporate citizen, we believe that we have an important role to play in education and awareness campaigns that help consumers and businesses protect themselves online. Currently, PayPal is on the board of the National Cyber Security Alliance (NCSA) and we are very engaged in their Stay Safe Online national program. We believe in the NCSA's mission which is to "educate and empower a digital society to use the Internet safely and securely at home, work, and school, while protecting the technology, individuals' use, the networks they connect to, and our shared digital assets".

In cooperation with a number of large Internet companies and major web browser makers, PayPal participated in an education campaign in 2010 to encourage our customers to upgrade their web browser to the latest and most secure version.

Recommendations for Federal Policymakers

Although it is the responsibility of industry leaders, like PayPal, to ensure the safety and security of our platforms and our users, federal policymakers have an important role to play in creating a secure Internet and mobile ecosystem. Here are some of our recommendations for areas where the federal government, and specifically Congress, can lend a helping hand.

Research and Reliable Data

As you know, the Internet offers tremendous benefits and efficiencies to businesses and consumers and over the years this has led to a burgeoning Internet-enabled industry. However, as online business transactions increase and more and more consumers adopt Internet and mobile services, cyber criminals are given greater access to business assets and personal information than ever before, opening up risks for intellectual property theft, identity theft, and other crimes.

What we have found from our years of combatting cybercrime, is quantifying the full cost is difficult if not impossible because many incidents are not reported. Estimates of the

magnitude and scope of cybercrime vary widely, making it difficult for policymakers and industry to fully understand the severity of the problem and the level of effort that will be needed to combat it. However, based on recent studies, cybercrime is definitely a growing problem. For instance, a 2011 government-sponsored study in the United Kingdom found that cybercrime cost £27 billion (about $44 billion) in the UK alone, with businesses bearing three-quarters of that cost. The Federal Bureau of Investigation's Crime Complaint Center (IC3) received 22% more self-reported cybercrime complaints in 2009 than the previous year — and that the dollar value of these incidents was skyrocketing, up 111% in 2009 to more than $550 million. It's clear that business is currently sustaining significant losses to cybercrime, but until we know how much money is being lost, where the money is going and whether or not the responsible parties can be held accountable, it will be hard to create a framework that really addresses the problems.

It is our recommendation that policymakers sponsor research that helps to fill in some of the information gaps that currently exist as it relates to cybercrime. We believe that this research will be a critical tool in arming policymakers, law enforcement and industry against the growing threat of cybercrime.

Increased Resources for Law Enforcement and Greater Workforce Development

The difference between the effectiveness of law enforcement in the physical world and on the Internet could not be more striking. In the real world even minor crimes such as vandalism and burglary resulting in relatively low dollar losses merit at least a visit by a police officer, while online crimes exceeding $25,000 frequently go uninvestigated, much less prosecuted. We believe that this unfortunate reality is mainly due to insufficient funding for cybercrime law enforcement and a general lack of trained cyber experts within law enforcement and policy circles.

We believe that there is a significant increase or a reprioritization needed in the funding of agencies which investigate and prosecute cybercrime offenses. We don't offer a specific proposal for the appropriate funding levels but we believe the case for additional resources will be easily made once better data is available regarding the scope of the problem. We recommend

that policymakers look to find ways to help law enforcement agencies address these resource needs.

In addition, we encourage policy makers to find ways to encourage greater workforce development and training for cybersecurity professionals. Most important for PayPal and eBay is training for computer programmers in secure development practices. While computer science programs have been quite effective in turning out students with the appropriate general programming knowledge and skills necessary for today's jobs, they have not kept up with the demand of security conscious companies who need programmers who know how to develop applications securely and free from technical flaws. While we are seeing progress at a number of institutions we believe substantial investment is warranted in this field.

Increase Enforcement Across Borders

The European convention on cybercrime has represented an extremely important framework for dealing with cybercrime internationally. However, there are two ways in which it has fallen short.

The convention allows nations to cooperate with each other in investigating cases of cybercrime. It permits one state to request that a second state preserves and supplies the necessary data needed to support a particular investigation. However, the mechanisms used to request the data are antediluvian: Multi-Lateral Assistance Treaties (MLATs), and "Letters Rogatory". In all of the cases where we have worked with multi-country investigations, we have never witnessed a case in which the data has been returned to the requesting law enforcement agency in under three months. We have found that six months is more common, and we have heard of cases where the data has been returned more than two years after it was originally requested. Given the speed at which cyber attacks move, this slow response time effectively hobbles the investigating law enforcement agency and frequently cripples investigations. During this time, the criminals are allowed to keep victimizing citizens and law abiding organizations.

We agree that there needs to be some level of supervision, and approval, such that rogue officers (or worse) cannot request arbitrary information from another state, without good purpose. But, in the age of the Internet, most workflow functions can be highly automated. The technology to do this exists, and is readily available. We recommend that policymakers consult our domestic law enforcement organizations who best understand how to fix current practices and make cross border enforcement a more coordinated and streamlined process.

Removing Barriers to Private and Public/Private Cooperation

In our testimony we have highlighted a number of cases where we have partnered with private and public entities to find solutions to the growing threat of cybercriminal activities. Although we have been very successful in some of these cases, we believe that we could accomplish more by working with policymakers to remove some of the barriers that prevent private industry from working together to protect the Internet ecosystem.

One of those barriers relates to information sharing between private companies. We understand and strongly support the need of strong privacy protections for consumers and individual businesses, however, we also believe that outdated provisions of certain laws, such as the Electronic Communication Privacy Act of 1986 (ECPA), have been interpreted in a way that impedes the ability of private industry to work together to combat cybercrime in a way that protects ourselves and our users.

For instance, as I testified, our DMARC program has been very successful in stopping unauthenticated emails from reaching inboxes. However, the DMARC program is not necessarily as effective as it could be because of the limitations the current statute places on private-to-private information sharing, even in cases of security. Not only does DMARC provide a way for email providers to tell whether or not an email is authentic, but it also provides a way for the email receiver to report back to the sender about messages that pass and/or fail DMARC evaluation. This reporting is a matter of common sense. If cybercriminal is using a company's trademark and brand in an unauthorized manner, we believe that company would want to know, and should know, where that email is coming from in a timely manner so that they

can work with the proper authorities to take down the rogue website. Unfortunately, some current interpretations of ECPA prohibit voluntary information sharing of this nature between private companies. Unfortunately, instead of helping to protect companies and consumers from bad actors like its original intent, these privacy laws are serving to immunize illegal actions from further scrutiny. We ask that policymakers review ECPA and other potentially outdated laws that can prohibit companies from meaningfully protecting the security and privacy rights of their users and themselves.

Increase Consumer Education Awareness

It is clear from a variety of sources, that most consumers have little idea how to protect themselves online. However, it is also clear that the problem is much larger than the scope of work happening today. There are many studies that show the majority of Internet users are both afraid of the risk of using the Internet, and simultaneously don't have the information needed to protect themselves online.

While the education efforts from organizations like NCSA are helpful, they are simply not at the scale needed to help hundreds of millions of Internet users across the United States. This area needs to experience significant increase in investment from both private industry and government stakeholders.

In addition, we believe that there should be some consideration of introducing cyber-safety education curriculum into public schools. There are a number of studies showing how these "digital natives" are in fact more trusting of the Internet. Although it is important that we continue to foster adoption of Internet and mobile technologies at a young age, we also think it is necessary to educate children on the potential risks and dangers and how to avoid them. This problem is more tractable than general consumer outreach, as there are formal channels—i.e. schools—by which this group of users can be reached. All that is needed is the development of a formal safety and security curriculum, and an insistence that this topic becomes one of the core areas taught to students.

Establish a Coordinated Internet Safety Framework

When we look at other forms of technical innovation throughout history, we can clearly see that these innovations were coupled with attendant public policy, self-regulation and public reaction that were instructive for understanding the various roles and responsibilities that each stakeholder had to play in order to maintain the safety and benefits of the technology. For instance, today, when you ask an individual the parties responsible for ensuring the safety on our highways, most people would probably be able to instinctively respond with the names of a few of the responsible stakeholders, such as motorists, local and state law enforcement, state and federal departments of transportation, and the National Highway Traffic Safety Administration. Most Americans know this because there is a solid framework that was created and implemented years ago that is intended to keep motorists safe while traveling on our nation's highway system.

However, when you ask that same question, but replace highways with the Internet, the same individual would most likely fail to give a response. Unfortunately, we as a country have failed to adopt a framework for the Internet and mobile ecosystem that clearly lays out the various stakeholders and jurisdictions involved and the roles that each stakeholder has to ensure users safety while they are traveling on the World Wide Web.

We recommend that Congress work with various stakeholders, including consumers, industry, policymakers, regulators, academics, and civil liberty groups, to create a national framework that creates a clear and concise model for how our nation keeps one of our greatest engines of economic growth safe and secure for all users.

The Cybersecurity Enhancement Act

In light of these policy recommendations, I did want to take a few minutes to praise the work that the House Science, Space & Technology Committee has done to address some of the cybersecurity challenges facing our nation. PayPal appreciates the bipartisan efforts of the Committee over the past few years to create a legislative framework that creates some innovative

solutions to issues such as cybersecurity R&D, education and workforce training, and standards development. Importantly, it achieves these ends without creating undesired side-effects.

In particular, we are very appreciative and supportive of the following provisions within the legislation and would welcome the opportunity to work with Members of the Committee on these priorities:

- Section 104 – Social and behavioral research in cybersecurity: This section is well aligned with a number of our efforts and our recommendations in terms of areas that need additional research. In particular, we think that Human Computer Interaction (HCI) topics in security are a new frontier and we applaud the Committee for their consideration of these issues.

- Section 109 – Security automation and Checklists: Improved automation and repeatability are key. We appreciate the Committee's attention to these issues and believe that this work will have a positive impact.

- Section 205 – Strengthen Authentication for Identity Systems: As I testified, this is the wave of the future in terms of improving security of the Internet and mobile ecosystems and this is completely aligned with our work on FIDO and NSTIC.

Conclusion

To conclude, PayPal is committed to providing our customers with the safety and security that they not only deserve, but expect. We recognize that security is a key component of their experience and the trust they place with us. As technology changes, as the world changes, the security measures that we adopt will continue to change. However, my role is to keep up with these rapidly evolving trends and not only surpass the bar that our consumers and employees challenge us to reach on a daily basis, but work to find solutions that will benefit not just PayPal but the entire Internet and mobile ecosystem. It is our hope that in the years to come the challenges we face from cybercrime will be a faint memory. But until then, PayPal is committed

to partnering with policymakers and private and public stakeholders to ensure that we do everything in our power to create an ecosystem that is safe and secure.

I appreciate the opportunity to testify before the Committee, and I look forward to your questions.

Chairman MASSIE. I now recognize our next witness, Dr. Frederick Chang.

STATEMENT OF DR. FREDERICK R. CHANG, PRESIDENT AND CHIEF OPERATING OFFICER, 21CT, INC.

Dr. CHANG. Chairman Massie, Chairman Bucshon, Chairman Smith, Ranking Member Wilson, Ranking Member Lipinski, Members of the Subcommittees, thank you for the opportunity to testify before you today on the hearing on the topic of cyber R&D challenges and solutions.

My name is Frederick R. Chang and I am currently the President and COO of 21CT, Inc., a small high-tech company in Austin, Texas. In prior positions, I have served as the Director of Research at the National Security Agency, in academia at the University of Texas—at both the San Antonio and Austin campuses, and in the telecommunications industry.

I would also mention that I have served as a member of the CSIS Commission on Cybersecurity for the 44th Presidency, and I am currently a member of the Texas Cybersecurity Education and Economic Development Council.

I do not have to tell you that we are under attack in cyberspace. Those of us in the field of security have known about it for some time now, but now the problem has broadened and deepened its scope. Our friends know, our neighbors know, our kids know.

The field of cybersecurity is too reactive and after-the-fact. We wait for something bad to happen and then we respond. We lack the fundamental scientific understanding of causes, of solutions, of countermeasures. Science uses words like evidence, metrics, repeatability, predictability. In cybersecurity these words are not used often enough. Indeed, when it comes to predictability, about the only thing we can predict with a high degree of confidence is that a determined hacker will be able to compromise the target system.

At the turn of the 20th century, life expectancy in the United States was a little over 47 years. A century later, it was nearly 77 years. Why did this happen? A large part of the improvement can be traced to advances in public health and an improved understanding of the science of infectious diseases. After World War II, scientists isolated causes and developed solutions for diseases like polio, measles, and chickenpox. I am not arguing that the cybersecurity problem today is as bad as polio was in the '40s and '50s, but I am suggesting that we know how to make a dent in the problem.

It won't be easy because the problem is truly a daunting one against a highly adaptive adversary. I believe that a broad and interdisciplinary approach will be necessary. I offered a few ideas in my written testimony.

One of the major obstacles to more progress in cybersecurity is a lack of qualified and well-trained professionals in the field. Just as a generation of students became fascinated by and intellectually curious about space, science, and engineering after the launch of Sputnik, we need for that to happen now for a new generation of students about cyberspace science and engineering.

The skills gap comes up time and time again. It was a key issue in our work on the CSIS Cybersecurity Commission co-chaired by

Congressman McCaul and Congressman Langevin, and it was a key issue in our work on the Texas Cybersecurity Council.

And representing a small company with ongoing demand for highly technical cyber hires, it is a constant challenge for us to identify and recruit the necessary expertise. Not only do we need a long-term pipeline of well-trained students to fill the many jobs that will be necessary, but the demand is particularly acute with respect to the requirement for the extremely deep technical skills needed to operate at the very highest levels.

In a CSIS Commission report from 2010, there was an estimate that we have about 1,000 deeply technical people in the United States who can operate at the most elite levels but that we need something like 10,000 to 30,000. The report went on to say we not only have a shortage of the highly technically skilled people required to operate in support systems already deployed, but also and even more desperate—a more desperate charge of people who can design secure systems, write safe computer code, and create the evermore sophisticated tools to prevent, detect, mitigate, and reconstitute from damage due to system failures and malicious acts.

The legislation in H.R. 2096 places front and center two of the items I believe are central to making more progress in improving the Nation's cybersecurity posture: research and development and cybersecurity workforce development.

Let me close by saying that I have suggested some things in my testimony that will take a long time to implement. For example, producing a long-term, robust, and deeply technical cybersecurity workforce or creating a science of cybersecurity could take decades.

I am reminded of an old proverb. The best time to plant a tree was 20 years ago. The second best time is now. It is my sincere hope that 20 years from now we can look back at this time and say that this is when we began to turn the tables on our cyber adversaries and took the advantage back.

Thank you again for the opportunity to speak with you today.

[The prepared statement of Dr. Chang follows:]

Written Testimony of

Dr. Frederick R. Chang

President and COO

21CT, Inc.

Before the

Subcommittee on Technology and the Subcommittee on Research

Committee on Science, Space and Technology

U.S. House of Representatives

Hearing on

"Cyber R&D Challenges and Solutions"

February 26, 2013

Chairman Massie, Chairman Bucshon, Ranking Member Wilson, Ranking Member Lipinski, Members of the Committees, thank you for the opportunity to testify before you in today's hearing on the topic of *Cyber R&D Challenges and Solutions*. My name is Frederick R. Chang and I am currently the President and COO of 21CT, Inc. in Austin, Texas. In prior positions, I have served at the National Security Agency (as Director of Research); in academia (at The University of Texas at San Antonio and at The University of Texas at Austin); and in the telecommunications industry (at SBC Communications, Pacific Bell, and Bell Laboratories). I would also mention that I have served as a member of the CSIS Commission on Cybersecurity for the 44th Presidency and I am currently a member of the Texas Cybersecurity, Education, and Economic Development Council.

You may not have heard of my company 21CT, Inc. before, but briefly we are a small, technology company headquartered in Austin, Texas. We have a 12-year history of maturing

new technologies, starting with early research and going all the way through operational military and commercial use. Our products are focused on the areas of intelligence analytics, computer network defense analytics, and fraud detection.

The Cybersecurity Challenge

Not too long ago, we were anxiously awaiting the arrival of the "Information Superhighway". It promised to improve our productivity, enrich our lives, educate our children and so much more, via e-commerce, e-banking, e-learning, e-government, and the like. The Internet and the world-wide-web are among the most successful technological and commercial advances in human history. Yet with all the progress and success, there is a dark cloud hanging over cyberspace, and that dark cloud is security. Cyber infrastructure is tightly woven into the very fabric of our lives and it would be very hard to imagine going back to an earlier time -- but we are paying a heavy price for our technological dependence and the problem is worsening with the passage of time. Our trust in cyberspace has been taken from us by hackers, cybercriminals and sophisticated cyber attackers who intend to do us harm. We deserve better. We expect our information to be confidential from prying eyes. We expect system resources to be available to us if we are legitimate users of those resources. We expect that our information will not be altered in a way that we do not intend. We expect that it should not be impossibly difficult to protect ourselves in cyberspace if/when the need arises. These expectations are simply not being met today. Attacks on both the public sector and the private sector are rampant. Denial of service, identity theft, and cyber extortion are now all too common. As you are all abundantly aware, financial systems, national critical infrastructure systems, defense systems, and much more are all targets of sophisticated cyber attacks.

Science of Cybersecurity

The discipline of cybersecurity today is too reactive and after-the-fact. In general, something bad has to happen and then action is taken. There is certainly some ability to stop things that have been seen before, but unfortunately new attacks, that haven't been seen before, are all too common. Cybersecurity is not based on a firm science and engineering foundation and I believe it is critically important that such a foundation be created. Some important activity has started along these lines [e.g., 1, 2], but much more is needed. In our school science classes we learned that water at sea level changes from a liquid into a gas at 100 degrees Celsius and into a solid at 0 degrees Celsius. Similarly we learned about gravity and that a freely falling object near the earth's surface will increase by approximately 9.81 meters per second every

second. In science, the notions of laws, principles, experiments, metrics, repeatability, and predictability (among others) are commonly used. These words and ideas are not common in discussions of cybersecurity today, unfortunately. Indeed it has been noted [3] that when it comes to predictability, about the only thing we can predict confidently in cybersecurity is that a sufficiently motivated attacker will be able to compromise the targeted system.

There are at least three different ways to think about the role of science in cybersecurity [4, see also 5]:

1) Universal laws that enable strong quantitative predictions;
2) Systematic generalizations of knowledge;
3) Conduct of research through hypothesis formation and experimentation.

While progress is being made, we have much more work to do in all three areas.

Cybersecurity metrics

"If you can not measure it, you can not improve it."

"I often say that when you can measure what you are speaking about, and express it in numbers, you know something about it; but when you cannot measure it, when you cannot express it in numbers, your knowledge is of a meagre and unsatisfactory kind; it may be the beginning of knowledge, but you have scarcely in your thoughts advanced to the state of Science, *whatever the matter may be."*

These quotes are from the influential 19th century mathematical physicist and engineer Lord Kelvin, and are appropriate in a discussion of cybersecurity metrics. While important work is taking place [e.g., 4], we need improvements in hard, objective metrics and measures of security. Metrics are needed at many very practical levels. At a very tactical level, how do you know if computer system A is more or less secure than computer system B? Is computer system A more secure than it was last month? Last year? At a corporate level, how you do measure the security of your corporate information technology infrastructure? Is it more secure now than it was last year? Do the measures allow a pinpoint assessment of where corporate improvements are necessary? At a much more macro level, what metrics are best used to determine if the industry as a whole is making progress toward improving its cybersecurity posture? How would you measure the effect of an important government policy change in

cybersecurity? Is it making the difference that was intended? It is relatively straightforward to determine the effects of changing the speed limit on traffic accidents. It won't be so clear for cybersecurity. Developing a disciplined, agreed-upon, and readily implementable set of metrics for cybersecurity remains a hard problem. Perhaps we can look for some assistance from other fields -- medical research has successfully employed metrics to improve the science of human health. Measures of human health and cyber health share an important common ingredient: in both cases we are attempting to measure the absence of something bad (human disease or system compromise).

Cybersecurity Research and Development

In the December 2008 report from the CSIS Commission on Cybersecurity for the 44th Presidency [6], we estimated that in 2009 about 0.2% of federal R&D funding would go into cybersecurity. That was several years ago, and no doubt the picture is different today, but at least as of that time, we start from a very small base. Let me highlight just a few areas that I think are important in addition to the science of cybersecurity thrust mentioned previously.

Psychology and security

While travelling in London some years ago, I was nearly pulverized by one of those large red double-decker buses. Being from the United States, before crossing a street, I am accustomed to looking to my left before crossing. In this case, this instinct did not serve me well. I believe that something similar is occurring for many people as we make decisions and operate our computers in cyberspace. The instincts and tendencies that serve us well, the vast majority of the time in the physical world actually betray us in the complex, abstract, virtual world of cyberspace.

Security is very often about the weakest link. Hackers need just one way in. As technical security measures improve (e.g., greater use of encryption), then people increasingly become the weakest link. Hackers often employ a tactic known as "social engineering" to trick computer operators to divulge sensitive information that can be used to compromise a system (e.g., a password). These tactics can be extremely effective and much easier to accomplish than a technical compromise. Indeed the well-known hacker Kevin Mitnick reported in testimony to Congress that he was so successful in social engineering that he rarely had to resort to a technical attack [7]. More generally, there are a well-known set of cognitive biases that people use to assess risk and make decisions [8]. These biases often cloud our reasoning and cause

us to improperly assess risk, in many domains, including in cyberspace. We must take steps to strengthen the weakest link. Gaining a much richer understanding of the cognitive biases at work in the context of decision-making in cyberspace would be just one of many important issues that need research at the intersection of psychology and cybersecurity.

Software assurance

Software is vulnerable – and that is a key reason why cyber compromise is so prevalent today. Modern software systems are exceedingly complex and not only must work correctly in the face of error or mischance, but must also work correctly when an adversary is trying to attack them – and this is exactly the sort of hostile environment that cyberspace creates for software. Software today too often treats security as an after-the-fact problem. The software is developed, tested and released and then a security incident occurs and the software must be patched, after-the-fact. We must move to a model where security is built in to software from the very beginning. How can we make dramatic breakthroughs in methods, procedures, metrics and the like that incorporate building security into software, such that software is built to be inherently resistant and resilient to attack? Can we introduce these new techniques in ways that are cost-effective, that speed time to delivery and that are convenient to use for developers? Can we compose new secure software from component pieces that are not secure? There have certainly been important contributions made in this area of research, but I believe it is time to accelerate and reinforce innovation and progress.

Trustworthy systems

Apparently we don't trust the software on our computers. We have millions and millions lines of software code on our machines in the form of operating systems, device drivers, applications, etc. We know that code may not be secure, so we purchase additional security software in the form of firewalls, anti-virus software, anti-spyware software and the like. Well, security software may be vulnerable as well, so now what? Do we buy a firewall for our firewall? You get the idea. Related to the software assurance topic above is the notion of the need to build systems that are inherently trustworthy. The problem expands in scope rather dramatically when you now must consider building scalable trustworthy systems; systems of systems connected by networks that must all be inherently trustworthy. You want these systems and networks to be highly available, highly reliable, highly resilient, etc. These are very hard problems that will defy easy solution as systems and networks continue to grow in size, scope and complexity.

Economics and cybersecurity

Would you spend $50 on software to help protect my computer? When you purchase anti-virus software for your computer, one of the things that it is supposed to do is help ensure that your computer does not become part of something called a botnet. If your computer becomes a bot, this would mean that unwanted, malicious software has been installed on your computer that allows a hacker (also called the botmaster) to take control of your computer. Once the botmaster has seized control of your computer he/she can command it, for example, to do malicious things to other computers – perhaps mine. So in a very real way, the security of my computer depends on whether or not you have purchased software to protect your computer. It is important to note that this has nothing to do with technology per se but rather with whether economic incentives are in alignment. That is to say, the security of a system may have more to do with economic incentives than with technical capability. Similarly, software companies are capable of making their software more secure but so far they haven't been economically incented to do so. Business factors such as speed to market, enhanced features, improved system performance, and the like, often take priority over security. How much should a firm spend to secure its cyber infrastructure? Does increased spending on cybersecurity result in improved cybersecurity? How should the money be spent? On hardware or software or more staff? What about a cybersecurity insurance policy? Research here will be related to work on metrics. An active field of research has been started in this area – the results are most illuminating -- and much more is needed.

Cybersecurity as a "wicked problem"

In May of 1961 President Kennedy announced a bold national goal, "before this decade is out, of landing a man on the Moon and returning him safely to the Earth." As we all know, that historic mission was successfully accomplished in July of 1969. Early computer security work was starting at around the time Apollo 11 was splashing down in the Pacific Ocean, and now – well over 40 years later – computer security is far from a solved problem. Why has this been so hard? There are many reasons, but recently people have talked about cybersecurity as a "wicked problem" [9]. Wicked in this context does not refer to evil, but rather resistance to solution. Wicked problems are extremely difficult and perhaps impossible to solve and include these properties, among others [10]:

1. The problem is not understood until after the formulation of a solution.

2. Wicked problems have no stopping rule.
3. Solutions to wicked problems are not true-or-false, but rather better-or-worse.
4. Every wicked problem is essentially unique.
5. Every solution to a wicked problem is a 'one shot operation'
6. Wicked problems have no given alternative solutions.

To the extent that cybersecurity is indeed a wicked problem, then I believe that an interdisciplinary research approach is needed. In addition to the disciplines of psychology, computer science and economics described above, what can we learn from the fields of biology, medicine, physics, anthropology, political science and more? I believe these other disciplines will add much to the research dialogue.

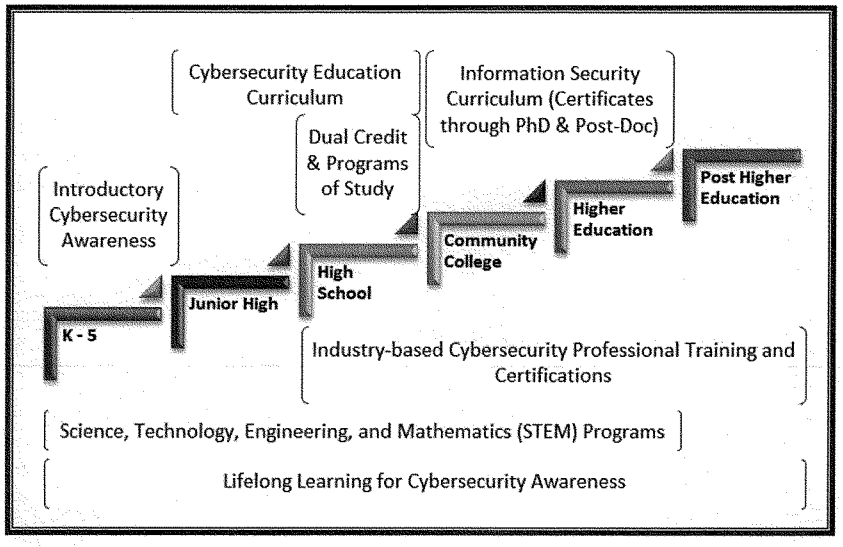
There are other important research topics that are not described here, that are worthy of mention including: secure cloud computing, secure mobile computing, secure hardware, secure hypervisors, secure coding, insider threat, data science, and many more.

The Cybersecurity Skills Gap

"The cyber threat to the United States affects all aspects of society, business and government, but there is neither a broad cadre of cyber experts nor an established cyber career field to build upon, particularly within the federal government."
(Source: Securing Cyberspace for the 44th Presidency, CSIS Commission on Cybersecurity for the 44th Presidency, *Dec. 2008.)*

The cybersecurity skills gap has been discussed extensively over the last few years [e.g., 11] and indeed the continuing shortage of qualified cyber professionals remains a major obstacle in making significant progress in cybersecurity. Representing a small company with on-going demands for highly technical cyber hires, it is a constant challenge for us to identify and recruit the necessary expertise – and this is a consistent theme.

In our work on the Texas Cybersecurity, Education and Economic Development Council [12], the skills gap issue came up time and time again. It was clear to us that the workforce gap would be a long-term problem and we advocated a "pipeline" approach to ensure a long-term supply of well-trained, motivated cybersecurity professionals in the state. This K-through-PhD approach is represented in the figure below and incorporates both professional training and awareness training.



Proposed Texas Cybersecurity Education Pipeline

(Source: Texas Cybersecurity, Education, and Economic Development Council, Dec. 2012)

In addition to a broad-based "pipeline" approach, I believe it is extremely important to take a depth-based view as well. "There are about 1,000 security people in the US who have the specialized security skills to operate at world-class levels in cyberspace. We need 10,000 to 30,000" [11]. This quote is reflective of the fact that while there is a broad and long-term skills gap, the gap is especially large when it comes to the exceedingly deep technical knowledge needed to operate at the highest level. For example, in compromising a system, a sophisticated cyber adversary will do so in a way that avoids detection. Thus to detect the compromise requires a very high level of skill. A national discussion of the cybersecurity skills gap must include innovative ideas as to how to increase substantially the number of cyber professionals with exceedingly deep technical skill.

Comments on H.R. 2096, The Cybersecurity Enhancement Act of 2012

I was asked to comment on H.R. 2096, The Cybersecurity Enhancement Act of 2012, and would offer these brief comments:

1. There is considerable mention of cybersecurity workforce issues in this legislation: training, education, awareness programs, scholarships, and the like. As mentioned previously, the cybersecurity skills gap today is large and represents a major obstacle to significant progress in improving the nation's cybersecurity posture. Initiatives that lead to breakthrough progress in the skills gap are to be applauded. I would note the point I mentioned previously in my testimony regarding the especially large skills gap when it comes to the numbers of people possessing exceedingly deep technical skill and would encourage particular attention in this area. Let me also say that while in academia I had the opportunity to witness the benefits to students of programs like the NSF Scholarship for Service Program and the Department of Defense Information Assurance Scholarship Program. These scholarships are making a difference and I believe they are an important tool in helping to close the nation's cybersecurity skills gap.
2. In section 109 of the legislation there is discussion of the need for security automation and continuous monitoring. These are both important concepts and critical at this time as cyber adversaries will continually adapt their attack vectors, in an effort to thwart the current defensive posture that is in place. I believe it is important to automate what you can, but hasten to point out that, as we all know, automation can never be perfect – something will get through. That leads us to continuous monitoring, which is similarly important, but I would add that there needs to be some consideration given to requiring continuous improvement along with continuous monitoring. We should have the expectation that the networks that are being continuously monitored, become increasingly more resilient over time, as well.
3. Finally, a centerpiece of this legislation is cybersecurity research and development. I mentioned earlier in my testimony the estimate of 0.2% of federal R&D spending going to cybersecurity R&D in 2009. I believe that older estimate is worth repeating here because to the extent that this legislation can raise the trajectory of cybersecurity R&D spending from its historical levels, that would create long-term benefit in our effort to improve the nation's cybersecurity posture. In my testimony I also highlighted the importance of social science research (in psychology and economics, in particular) and indeed social science research and cybersecurity are specifically identified in Section 104. In Section 108 there is a discussion of a cybersecurity university-industry task force to explore opportunities for collaboration in research, development, education and training. As part of those task force deliberations, I believe it would be valuable to have some discussion about the task force potentially creating and then issuing some

cybersecurity research grand challenges – that meet the needs of industry, government and academia. Solutions to such grand challenges could help advance the field and at the same time help solve some enduring hard problems facing practioners in the future. Finally, and more generally, in my testimony I stressed the importance I place in developing a science of cybersecurity. I would mention here that not all cybersecurity research produces a benefit to cybersecurity science. It's a subtle but important point. Among other things, cybersecurity science should tell us something about the limits of what is possible in a particular security domain, and have broad applicability beyond a specific platform, a particular attack or a certain defensive implementation. To be sure, increasing the amount of very high-quality cybersecurity research will produce a tangible benefit, but it would be my hope that some of that high-quality research be directed toward advancing the science of cybersecurity.

Let me close by saying that I've suggested some items in my testimony that will take a long time to implement. For example, producing a long-term, robust and deeply technical cybersecurity workforce or creating a science of cybersecurity, could take decades. I'm reminded of an old proverb: The best time to plant a tree was 20 years ago – the second best time is now. Thank you again for giving me the opportunity to speak to you today.

References

1. JASON Program Office. Science of cyber-security. Report No.:JSR-10-102. The Mitre Corporation, McLean, VA, November 2010.
2. Developing a blueprint for a science of cybersecurity, The Next Wave, Vol. 19, No. 2, 2012, National Security Agency, Ft. Meade, MD.
3. Evans, D. & Stolfo, S. The science of security. *IEEE Security & Privacy,* **9**, 16-17, 2011.
4. Stolfo, S., Bellovin, S.M. & Evans, D. Measuring security. *IEEE Security & Privacy,* **9**, 60-65, 2011.
5. Schneider, F.B. Blueprint for a science of cybersecurity, The Next Wave, Vol. 19, No. 2, 47-57, 2012, National Security Agency, Ft. Meade, MD.
6. CSIS Commission on Cybersecurity for the 44th Presidency, *Securing Cyberspace for the 44th Presidency*, Center for Strategic and International Studies, Washington, DC, December 2008.
7. Mitnick, K. Kevin Mitnick in a hearing before the Committee on Governmental Affairs, U.S. Senate, "Cyber Attack: Is the Government Safe?" March 2, 2000.
8. Kahneman, D., *Thinking, fast and slow.* Farrar, Straus and Giroux, New York, 2011.
9. Lucky, R.W. Cyber Armageddon. *IEEE Spectrum*, vol. 47, no. 9, pp. 25-25, 2010.
10. Rittel, H. & Webber, M. Dilemmas in a General Theory of Planning, *Policy Sciences*, **4,** 155–169, 1973.
11. A Human Capital Crisis in Cybersecurity: Technical Proficiency Matters. CSIS Commission on Cybersecurity for the 44th Presidency, Center for Strategic and International Studies, Washington, DC, July 2010.
12. Building a More Secure and Prosperous Texas: A Report from the Texas Cybersecurity, Education, and Economic Development Council, Austin, TX, December 2012.

Chairman MASSIE. Thank you, Dr. Chang.

I now recognize our final witness, Ms. Terry Benzel.

STATEMENT OF MS. TERRY BENZEL,
DEPUTY DIRECTOR CYBER NETWORKS AND CYBER SECURITY,
USC INFORMATION SCIENCES INSTITUTE

Ms. BENZEL. Thank you, Chairman Massie, Ranking Member Wilson, Chairman Bucshon, Ranking Member Lipinski, and Members of the Subcommittees. I am pleased to offer my perspective on cyber R&D challenges and solutions based on 30 years in the cybersecurity community.

I bring an interesting perspective stemming from Principal at a startup company, Vice President at McAfee Software, and now the Deputy Director of our Cyber Networks and Cyber Security Division at the Information Sciences Institute, a research lab with the University of Southern California's Viterbi School where I direct the DETER project, a cybersecurity research, experimentation, and test facility.

I would like to address four key points today: one, the importance of broadening the purview of cybersecurity R&D; two, the importance of research infrastructure for experimental cybersecurity R&D; three, the importance of new models for technology transfer from university research into commercial practices and products; and four, the importance of higher education for developing next-generation cybersecurity researchers and technologies.

Let me start with the importance of broadening the purview of cybersecurity R&D. All too often our research is narrowly focused on single topics. For example, we have many people conducting excellent research in distributed denial of service, worms, botnets, and Internet routing, each studied individually and deeply. But believe me, our adversaries are not looking narrowly. In fact, they are looking at the combinations of these different kinds of threats and vulnerabilities, as well as combining that with cyber physical systems and social engineering.

We can no longer afford to look narrowly at the hard problems. Even more so, cybersecurity is no longer solely an engineering discipline. We must involve economists, sociologists, anthropologists, and other disciplines. While there has been some progress in these areas by the National Science Foundation, DHS S&T, and others, my first recommendation is we must increase the breadth and scope of strategic cyber R&D and increase opportunities for multi-disciplinary research.

Let me next address the need for research infrastructure for cyber R&D. Historically, we have struggled to prove the value of security technologies. Security is often viewed as the absence of something bad happening. I didn't get broken into, so I must be secure. When I was a Vice President at McAfee Software, I visited large customers—banking, manufacturing, and retail—and I was always asked about return on investment, how much to spend and how best to leverage cybersecurity investments. The truth is we had no easy answers except, of course, to buy our products.

We need to be able to conduct science-based cyber experimentation and tests just as in other scientific disciplines, real hypothesis-based testing, what-if scenarios, repeatable, demonstrable re-

sults. We provide this in the DHS- and NSF-funded DETER project where we provide tools and methodologies for researchers to live in the future creating new capabilities not yet imaginable. We must as a Nation create a paradigm shift in experimental cybersecurity. While NSF, DHS S&T, DOE, and DARPA have all invested in cyber testbeds and ranges, the results are uneven and not widely available.

And this brings me to my second recommendation. Formulate a research strategy agenda to develop a broad multi-organizational cybersecurity experimentation and testing capability.

Let me now address technology transfer. We have had major investments over the last 20 to 30 years, yet we are still inadequately prepared. Much research fails to see the light of day. While historically we have had insufficient awareness of the complexity of cybersecurity tech transfer, we have had scattershot approaches to cyber R&D, and a mismatch between markets and threats. To address these growing demands, it is imperative we create new models of technology transfer where the government-funded efforts help steer strategic cybersecurity R&D and their new university public partnerships.

As I have said already, we need to finally have education. More than just training, we need to educate the next generation of researchers and technologists and we need to do this by offering hands-on exercises and educational opportunities.

Let me summarize. We are beginning to see progress in all of these areas. NSF, DHS, and others deserve recognition for the focus they have brought to strategic programs. However, the current steps are not enough. We are lacking by orders of magnitude. In order to shift the dynamic in the battlefield, the Security Enhancement Act of 2013 includes provisions for these recommendations. Taken together, the four recommendations I have outlined today form a basis for multipronged, sustainable, national projects to address R&D challenges, and I urge you to take action now. Thank you for your time.

[The prepared statement of Ms. Benzel follows:]

Testimony of

Terry V. Benzel

University of Southern California, Information Sciences Institute

Before the House Science, Space and Technology Committee Subcommittees on Research and Technology

Hearing on
Cyber R&D Challenges and Solutions
February 26, 2013

Thank you Chairman Massie, Ranking Member Wilson, Chairman Bucshon, Ranking Member Lipinski, and Members of the Committee, for this opportunity to discuss Cyber Research and Development Challenges and Solutions. I am pleased to add my perspective on the Committee's questions, and my comments on the Cyber Security Enhancement Act of 2013. My remarks are based on more than 30 years in the cyber security research and development community, including:

- Senior positions at a Federally Funded Research and Development Center (FFRDC);
- Senior positions at a startup security company, Trusted Information Systems, that underwent a successful IPO and was acquired by a large enterprise security vendor;
- Vice President of Research at McAfee, Inc., then called Network Associates, and among the five largest software companies in the world;
- Special Projects Director at University of California at Berkeley;
- A consultant to cyber security start-up companies seeking Small Business Investigative Research (SBIR) grants;
- My present position with two roles: Project Investigator on a large DHS S&T - funded cyber security project; and Deputy Division Director at the University of Southern California's Information Sciences Institute, in the Cyber Networks and Cyber Security Division.

Given my experiences, I am passionate about the topics facing this hearing:

- Cyber-security threats to our critical infrastructure,
- The cyber component of homeland security,
- The R&D programs needed to create new cyber-defenses and stronger critical infrastructure,
- The coordination, collaboration and education that are needed for
    - technology transfer from R&D to practical cyber-defenses, and
    - building the next generation of cyber-defenders who will use the new technology created by R&D.

1. Background

First, let me provide some background on my current work. I am the Deputy Director of the Cyber Networks and Cyber Security Division of the Information Sciences Institute (ISI), part of the Viterbi School of Engineering at the University of Southern California (USC). USC is one of the world's leading private research universities and an anchor institution in Los Angeles, a city that is now a global center for technology, international trade and the arts.

The Viterbi School of Engineering has been a leader in the transformation from analog to digital communications since the early 1960s. In fact, ISI was one of the handful of institutions around the globe that created the Internet. Our researchers largely developed the Internet communications protocols that are still in use, administered the domain name system (DNS) for 16 years, and coined the terms "dot-com," "dot-org", "dot-gov" and "dot-net" that are now ubiquitous worldwide.

My comments on R&D, and on technology transfer and education in particular, are based on my whole professional history. They are informed by my work at ISI, which has unique whose unique characteristics are applicable to the issues facing this panel today. In particular:

- Our work spans three complementary and critical areas: **academic**, including research and education; **industrial**, delivering technology-based solutions for government and business partners; and **professional**, offering students unusual, hands-on experience.
    - All these components are required to pursue R&D that is well prepared for tech transfer and use by a well-educated technology workforce.

- Our research work spans *pure fundamental research* to *applied technology* that can be transitioned to practical use in government and industry. Numerous systems developed at ISI have been fielded in operational settings. Many have become the basis of new product offerings, either for startups or acquisition by established technology companies.

- Our reliance primarily on federal funding, our experience with applied projects and our role in educating the next generation of researchers, gives us an unusual, integrated perspective on research, education and technology transfer needs, processes and solutions.

In the cyber-security part of ISI, our work shares all these characteristics. My group's cyber-security work is focused mainly on the DETER Project, which is one of the nation's foremost resources for innovative, experiment-based cyber R&D. In DETER, we are working to address critical strategic issues:

- While cyber-threat growth continues to accelerate, the stream of new and effective cyber-defense technologies has grown much more slowly. The gap

between threat and defense has widened, even as our adversaries deploy increasingly sophisticated attack technology and engage in cyber-crime with unprecedented power, resources, and global reach. Moreover, targets increasingly are attacked with foreign state sponsorship.

- Our nation's cyber-adversaries are focusing not only high-profile commercial and government systems, and not only the traditional critical infrastructures such as the power grid, hydro dams, and nuclear energy facilities, but also new targets that affect individual health and safety: wireless computing and controls in cars, medical devices, home appliances and safety systems, and the emerging smart energy grid that is tying them all together.

Before moving ahead with my remarks and recommendations about the cyber security challenge and the Cyber Security Enhancement Act, I will comment on how my group's current work addresses this cyber-security challenge, including issues of, and promising approaches to, cyber-security enhancement.

The DETER Project

The DETER project is working to fill the cyber-security gap described above. We function both as a research project and as the operator of a major cyber experimentation lab, DeterLab. Our research agenda spans a wide range of innovative methods, technology, and infrastructure for the work of cyber-security researchers. We put our research results and innovations into practice in DeterLab, which enables researchers to experiment with and test their cyber-security advances. One strategic goal for DeterLab is to help researchers dramatically accelerate the pace of their work, shifting from repetitive, small-lab engineering to the repeatable, measurable scientific experimentation and testing that we enable DeterLab users to conduct.

DeterLab is a large-scale facility used by researchers from hundreds of institutions worldwide. We enable researchers to observe and interact with real malicious software, operating in realistic network environments, at scales found in the real world. Researchers use the knowledge they gain from their experiments to devise cyber-defense innovations and to build systems that are inherently more robust. My team continually is developing capabilities that support increases in experiment scale and that refine careful, repeatable controls on that research.

Let me repeat my point about rigorous, repeatable testing and a realistic, large-scale test environment. These capabilities address a historical problem in tech transfer: an innovation that works well in a predictable, controlled environment, but turns out to be much less effective, reliable or manageable in a major, critical government or enterprise IT environment. Without realistic, large-scale resources and research environments, results are unpredictable. As I observed when I worked for security vendors, large enterprise-security companies have been burned time and again by acquiring small security startups that are attempting to commercialize university-bred research. These

products may work well for a few early adopters, but rarely scale up to real enterprise environments in terms of effective protection or practical security management.

In DeterLab, we are continually extending the shared scientific facility to help researchers better prove their work in a realistic setting, and to better prepare for successful tech transfer. We – and our funders at DHS S&T and DoD – believe that realistic, scientific experimentation and testing is critical to advancing the scale, pace, and power of cyber-security R&D. As R&D accelerates, testing proves effective, and the cyber-research community grows, we are becoming better positioned to help bridge the growing cyber-security gap that endangers homeland security and critical infrastructure.

2. Cyber-Security Challenges Facing the Nation

Members of the House of Representatives, I would like to address four key points:

1. The importance of broadening the purview of cyber-security research
2. The importance of research infrastructure for experimental cyber-security research and development
3. The importance of new models for technology transfer from university research into commercial practices and products.
4. The importance of higher education for developing next-generation cyber-security researchers and technologies.

2.1 Broadening Cyber-Security Research

We face threats that are rapidly increasing in scope and sophistication. As was made painfully clear by last week's revelations of Chinese military incursions (by the "Shanghai Group" or "Comment Crew") into US systems, we now face state-sponsored cyber-sleuthing and cyber-terrorism. This unstable environment includes targeted attacks by ad hoc organizations and global cyber-crime syndicates that are escalating their operations against systems critical to our national safety and security.

Cyber security is now a constant challenge for every facet of civilized society. We have become completely dependent on cyber capabilities and, as a result, highly vulnerable to wide-ranging threats. Despite years of research, however, we are still at the losing end of an asymmetric battle. As members of these Sub-Committees, I'm sure you have heard many times that steps must be taken to change these dynamics. As a nation, we must support new forms of research and development, and must ensure that resulting advances are based solidly in experimental science.

But even the best work is meaningless unless a chain of activities works end to end.

- cyber- science must be transformed into meaningful technology;
- that technology must demonstrate its viability in real-world settings;
- real-world viability must become the basis for transferring technology to critical systems that otherwise remain vulnerable;

- critical systems operators must use and manage the new technology effectively;
- Efficacy must encompass the evolving landscape of threats.

If any one of these links falters, then cyber-security innovations will not deliver real value to government and commercial customers. Nor will they serve the ultimate stakeholders in those systems: you and I and our friends and family, all of whom depend on orderly air traffic, reliable electric power, secure personal data, an alert and ready military enterprise, and countless other vital services.

Too often, cyber-security research is narrowly focused on a few specific areas of investigation. Unfortunately, our adversaries also are doing theirR&D, and are planning their attack scenarios, without any of the same constraints. They are looking across multiple threat vectors for system vulnerabilities, within and across different technologies, and picking targets for their strategic value – not simply because they are easy marks.

For example, our community includes scientists conducting very good research on distributed denial of service threats, Internet worms, botnets and Internet routing attacks. Researchers typically specialize in just one of these well-known areas, where innovative countermeasures, protection and hardening are extremely valuable. But our adversaries are constructing attacks that combine these areas into even more potent, multi-faceted weapons. Often, these approaches are amplified with sophisticated social engineering attacks designed to steal the keys to vulnerable systems.

Fortunately, there is substantial progress away from the single-focus syndrome. Federal agency sponsors have been steering researchers toward cyber-security issues that are critical to national, homeland and economic security. One result is more breadth in cyber-security research. Another, perhaps more critical outcome is a shift away from existing, commercial cyber-security problems to those that are not yet subject to rigorous work. The National Science Foundation is pursuing this strategic approach through its Frontier, Large, Medium, and Center focused Secure and Trustworthy Computing Program (SaTC), and through other programs aimed at increasing research breadth and dimensionality. The DHS Science and Technology group funding also is helping shift research to difficult, nationally strategic issues.

Still, studying broadly within our own disciplines is not enough. Cyber-security is no longer solely an engineering discipline. It requires deep involvement from economists, sociologists, anthropologists and other scientists to create the holistic research agendas that can anticipate and guide effective cyber–defense strategies.

- **Recommendation #1:** ***Increase the breadth and scope of strategic cyber-security R&D, and create opportunities for multi-disciplinary research.***

The Cybersecurity Enhancement Act of 2013 includes provisions for addressing this recommendation in sec. 103, Cybersecurity Strategic Research and Development plan, and specifically the call in item 2 for innovative, transformational technologies.

2.2. Research Infrastructure for Experimental Cyber Security Research and Development

Historically, cyber-security R&D has struggled to prove its value. The scientific basis for assessing the relative strength of theoretical and technological cyber-security solutions often has been uncertain. That uncertainty has hampered tech transition and widespread cyber-security adoption.

Corporations and government entities often pose security as a negative, as in: "We didn't get broken into, so we must be secure." In essence, *they define security as the absence of visible insecurity*. Even those that deploy cyber-security solutions may believe in simple, reactive "attack-defend-detect" approaches. Given my previous remarks and those of other cyber-security experts, it may seem puzzling that large-system organizations retain such a naïve position. I'd like to explain from personal experience how this mindset came about, and how a different approach to R&D is shifting the paradigm.

When I was a Vice President at McAfee, I often met with top corporate customers, which typically were large enterprises in banking, manufacturing, retail and other industries. The chief information officers of these organizations typically would ask me about return-on-investment (ROI) for our products. Their concern was how much to spend on, and how to best leverage, their cyber security investments. The truth is that we had no easy answers. At any single point in time, these customers could assess their threats and risks, and make rational choices on what defenses to purchase and why. But the threat environment changes so rapidly that *those choices might be sensible only at that specific moment, based on what was limited knowledge we, and the customers, had at the time.* Later, some choices might prove to deliver little value, while others were far more than worth their price. Still other, more devastating threats might remain threateningly at large.

This is a serious issue. Companies, particularly those with public shareholders, can't sit still and ignore the latest security technologies lest they find their systems seriously compromised. Security vendors have every incentive to reinforce that knowledge. They continuously can deliver new security widgets to counteract newly discovered threats. Some of these "solutions" invariably will be ineffectual or impractical. Are customers' threats addressed and risks reduced overall, at any increased rate? While there was and is no way to measure, the answer appears to be a resounding "No." We now see the world's most extensive, sophisticated IT operations, in corporations and governments worldwide, penetrated by China, Iran, organized crime and other top-tier adversaries.

Given the fundamental flaw in reactive approaches, a community began to emerge in around the year 2000 to create a *science* of experimental cyber–security. We saw a need to build environments that would:

- support experimentation and testing of hypotheses;
- enable creation of repeatable, science-based experiments that could be validated by others;
- generate research results that could be leveraged into broad, multi-component solutions in which components demonstrably support one another, making the whole greater than the sum of its parts.
- foster methodologies and tools to help guide experimenters toward this new, scientific cyber-security, and provide an open environment for researchers in industry, government and academia to build on one another's achievements.

Under funding from Dr. Douglas Maughan, then at DARPA, we performed a study, "Justification and Requirements for a National DDoS Defense Technology Evaluation Facility." The study provided the basis for defining key objectives for the DETER project. In 2003, with funding from NSF and DHS S&T, we initiated the DETER Project.

Looking forward, it is clear that cyber security R&D must be grounded in the same systematic approach to discovery and validation that is routine in other scientific and technological disciplines. To approach these challenging research problems, *we must create a paradigm shift in experimental cyber-security*. Only by enabling demonstrable, repeatable experimental results can we provide a sound basis for researchers to leverage prior work – and create new capabilities not yet imaginable. Tomorrow's researchers must be able to stand on the shoulders of today's researchers, not be consigned to re-treading the same ground.

Only by living in the future – enabling researchers to experiment with techniques and tools that do not yet exist and operate in environments only beginning to emerge – can highly capable, fluid new approaches take shape. The alternative is to remain caught on the new-widget treadmill, in which the nation must continually run faster to stay in same place, while invariably falling behind.

Living in the future also means enabling continuous R&D infrastructure gains. Our highly connected world is growing exponentially in scale and complexity. Critical national assets, and the threats to them, evolve in tandem as well. While there are now various cyber-security testbed experimentation facilities around the U.S., only a few are applicable to a wide range of experimentation and almost none are openly available. Still, their existence is a valuable step toward research into a cross-disciplinary range of cyber-security experimentation and testing methods and tools.

NSF, DHS S&T, DOE and DARPA all have invested in this evolution, spurring valuable advances such as federation of diverse scientific facilities. Researchers in disparate

locations now are able to work collaboratively, at the same time, to conduct experiments on a global scale.

But these advances are circumscribed and uneven. To match dramatic, ongoing change and complexity in the world at large, our cyber-defenders need parallel growth in R&D infrastructure capabilities. These initiatives must be expanded and coordinated to support a highly capable, shared national resource.

- **Recommendation #2:** ***Formulate a research strategy/agenda to develop open, broad, multi-organizational cyber-security experimentation and testing capabilities.***

The Cybersecurity Enhancement Act of 2013 includes provisions for addressing this recommendation in sec. 103, Cybersecurity Strategic Research and Development plan. Specifically, item 4 requires a plan to "maintain a national research infrastructure for creating, testing, and evaluating the next generation of secure networking and information technology systems."

2.3 Technology Transfer

The U.S. government and major corporations have poured hundreds of millions of dollars into security R&D for more than 20 years. Creditably, this spending is growing in scale and increasingly is strategically focused on critical infrastructure and homeland security. These investments hold the promise of delivering real-world value: putting practical security technologies in place to protect important assets. Of course, I recommend that funding agencies continue to grow their emphases in these crucial directions.

At the same time, however, troubling technology-transfer issues remain. As Members of this committee and its sub-committees, you may wonder: Why is technology transfer so difficult? Why does so much promising research not find its way into viable commercial products? Why do specific needs of specific government agencies and departments remain unaddressed?

In part, the answer lies in what I've already discussed: that security R&D has tended to be ad hoc, small-scale and lacking in the scientific methods of other disciplines – and thus in creation of a solid, accessible body of knowledge. But there also have been, and continue to be, structural problems with current tech transfer processes that can't be solved through hardening the science alone. Researchers and funders could achieve our wildest dreams for effective, cost-efficient, privacy-assuring cyber-security. Yet the results might have no impact unless the underlying structural issues are addressed and resolved.

These issues historically have included:

- *Insufficient awareness of the complexity of cyber-security tech transfer.* Tech transfer, while difficult in any field, seems particularly so in the constantly shifting world of cyber-security. At each stage from initial research idea, advanced prototype and early stage product to widespread adoption, the process can break due to internal factors or sudden shifts in attack methodologies, tools and strategies. Commercializing security technologies effectively accordingly has been, in some cases, largely a matter of chance.

- *A scatter-shot approach to R&D.* Over the last 40 years, governments and businesses around the globe have invested hundreds of millions of dollars in cyber-security R&D – but only loosely in coordination with one another. Research often was initiated based on a largely reactionary model driven by the hot security topic of the day.

- *Mismatch between market and threat environment.* Security vendors became very tactical in focus, looking at which innovations would fuel the next incremental security fix. They then upsold to existing customers and attempted to pull in new ones.

- *Assumptions of contained damage.* When a major cyber-attack occurred in the 1990s, businesses and governments were forced to reboot a few thousand systems. The scale and pervasiveness of computing technology has grown so dramatically that such an approach is now wholly unfeasible.

As a result of this largely ad hoc approach, some government and private investment has sparked revolutionary new products, companies and industries. Others have improved the operational security practices of IT departments around the world dramatically. Still others have resulted in research papers and prototypes, but not commercializable technologies. The net effect is that many potentially valuable security technologies never saw the light of day.

Fortunately, the situation is improving. Tech-transfer issues are being mitigated as researchers and funders set more realistic expectations and achievable goals. Businesses better understand that stellar approaches must be combined with sharp execution in operations, finance, sales and marketing. An enormous, interconnected world market also has forced research institutions and businesses to make more strategic choices in the technologies and approaches they pursue.

New approaches to tech transfer also are paying – often literally – dividends. For example, the Stevens Institute for Innovation at USC, funded by highly successful venture capitalist Mark Stevens and his wife, assists faculty and students with everything from nuts-and-bolts contracts and funding issues to instilling a culture of innovation university-wide. Its reliance on public-private partnerships, while not unique to USC, offers a uniquely effective means for engineers, physicians and other academic researchers to connect with the world at large.

In recent years, cyber-security R&D has been steered toward a model directed at homeland security and critical infrastructure. This strategic shift is fostering collaborations between universities and national labs, and is beginning to yield excellent work on smart energy grids, advanced persistent threats, next-generation Internet, and other security innovations that meet specified, high-priority needs. Much of this work is both strategic and long-term in nature, with the potential for fundamental transformation in protected assets or their protections.

Unfortunately, general enterprise security vendors have gone in the opposite direction. Most are now completely tactical, rather than strategic, in focus. As long as the cyber-security market was expanding dramatically, businesses could afford to pursue numerous, promising approaches. But market growth for these large-enterprise vendors largely has stalled despite the proliferation of technology. Large security vendors, like all players in mature markets, are chasing incremental growth in revenue and market share. They are dependent on creating small-scale innovations that will fuel the next incremental security fix. The vendor with the longest list of Band-Aids has the competitive edge.

At the same time, the majority of critical infrastructures are privately owned and operated in highly regulated industries, leaving them cost-constrained and lacking in capital for new technology. These industries also constitute narrow vertical markets that do not drive commercial product cycles. Such an approach is completely at odds with securing critical cyber infrastructure – and with strategic, long-term, transformational innovation.

In my view, it's imperative that we invent a new virtuous cycle in which government-funded work steers strategic cyber-security R&D. Clearly, the nation would be foolish to rely solely on incumbent vendors and system integrators to decide which innovations should be pushed forward and which consigned solely to professional journals. Public private partnerships and other innovative approaches surely can help re-define what the market is and how its vital players should be approached, For instance, the overall market may include not just large enterprise systems, but control systems for transportation, dedicated distribution like pipelines, and other businesses that deal in critical infrastructure. I don't know what this tech-transfer model ultimately will look like, but the current model flings open the door wide to cyber-***in***security.

There is, however, another structural issue: the businesses and government entities that are major security customers. Beginning in the 1990s, hydroelectric power plants, chemical manufacturers on major waterways, nuclear plants and other entities crucial to public safety began running control systems to monitor and manage their operations. Such systems theoretically separate their critical national assets from other systems connected to the Internet – and thus vulnerable to outside attack. Many control systems have known vulnerabilities, however, that are only partially addressed by commercial security products. While innovative security technologies exist to harden these systems, customers are slow to adopt them.

The reason: For decades, the security vendors on which these customers rely have offered assurances that current technology is "good enough." To admit otherwise might

require major, costly infrastructure changes for their customers. In highly regulated markets with limited capital, vendors are better served by continuing offer "good enough" and incremental low-cost Band-Aids.

As a result, the new virtuous cycle also must build sharply heightened threat awareness into customers' mindsets. Businesses and government entities must understand the magnitude of threats, the dire risks of miscalculation – to health and safety, citizen and consumer trust, and public and private finances – and that the disruption of the technology status quo may be more than worth the benefits. Customers must demand the level and pace of transformative technology that Americans deserve. Again, I don't presume to know how this should be done, only that it is as vital a mandate as advancing cyber-security defenses themselves.

In sum, the research challenges I described initially are compounded by significant tech transfer challenges. These challenges are surmountable if we:

- Continue steering security R&D firmly toward national strategic goals.
- Use public-private partnerships and other approaches to define or redefine markets and opportunities not served by incumbent security vendors.
- Find ways to engage customers in their own protection, both for the benefit of organizations and of the Americans they serve.

- **Recommendation #3:** ***Develop new models of technology transfer operation, funding, partnership and cultural change within organizations.***

The Cybersecurity Enhancement Act of 2013 includes provisions for addressing this recommendation in sec. 103, Cybersecurity Strategic Research and Development plan. Specifically, item 3 calls for programs that, "... foster the rapid transfer of research and development results into new cybersecurity technologies and applications for the timely benefit of society and the national interest..."

2.4 Educating the Next Generation of Cyber-Security Researchers and Professionals

Beginning to change the asymmetric dynamics of cyber-space requires astute, knowledgeable researchers, educators, operators, users and citizens. But we as a nation are nowhere near that goal. Rapid growth and spread of information technology, dramatically increased system complexity, and the multi-dimensional interdependence of these systems have left us woefully unprepared on many fronts.

The current dearth of cyber-professionals has sparked significant new federal training and education programs aimed at addressing this need. Among these initiatives: the National Initiative for Cyber Security Education (NICE), the Scholarship for Service program, the National Centers of Academic Excellence in Information Assurance Education, and the Centers of Academic Excellence in Research.

While these initiatives are beginning to increase the pipeline of cyber-professionals, their scale, pace and depth so far are nowhere near sufficient to address America's critical

needs in the public or private sectors. The challenge now is to help government agencies, contractors and critical infrastructure providers locate and access program suited for their organizations' needs.

Just last week (on February 21, 2013), the U.S. Department of Homeland Security (DHS) launched the National Initiative for Cybersecurity Careers and Studies (NICCS), an online resource for cyber-security career, education, and training information. NICCS will help expand, inform, monitor, certify and promote training programs. The process of creating, cataloging and monitoring training programs is a positive step toward meeting the nation's pressing cyber-security needs.

To fundamentally change the cyber-threat dynamic, however, we need deep intellectual resources as well. These are represented by the brightest, best trained, most curious and most ambitious researchers and educators. We accordingly need to be prepared to make significant investments in higher education. I applaud the efforts of the NSF and other federal research agencies to create and fund cyber-security research and education grants. These fundamental research endeavors are the essential catalyst for research breakthroughs. Only by educating the next generation of researchers and educators today can we build the intellectual resources vital to solving tomorrow's problems.

USC actively is engaged in several new initiatives to advance cyber-education. The USC Viterbi School of Engineering offers classes in computer security, and recruits and funds graduate students who are exposed to leading-edge cyber security research. In addition, the University will begin offering a Master of Cyber Security degree. This novel degree, which will integrate strong engineering and computing theory with applied science, will educate students to help solve real-world information security challenges.

While classroom study and early exposure to research provide foundational cyber-security education, effective training also demands direct, hands-on involvement. Teaching cyber security is challenging. How do you demonstrate system weaknesses, inspire students to create constructive new solutions to vulnerabilities, and provide an environment in which they realistically can explore threat scenarios? We believe that undergraduates with direct cyber-security experience are most likely to be eager to – and capable of – earning master's degrees. Similarly, graduate students who engage in science-based experimental research are most likely to develop the passion to pursue demanding doctoral and post-doctoral studies, and to obtain the academic positions that will enable them to continue developing our nation's cyber-warriors. None of these advances would be possible without federal government investment in fundamental cyber-security research.

The DETER Project at ISI offers precisely the hands-on security education, to a wide range of colleges and universities, that is essential for strengthening our intellectual resources. Teaching cyber-security is a core component of DETER's two-fold mission: to develop research into capable new cyber-security methods and technologies, and to operate DeterLab, our shared facility for cyber-security experimentation, testing and education. Through the DETER Project, educators can tap into DeterLab, providing

students with the vivid, realistic experience that can spark imagination and ignite passion for research.

DeterLab also fills a significant gap in security instruction by providing educators worldwide with substantive, thoroughly vetted facilities and materials. These security lab exercises complement existing, more abstract courses, enabling students to see and feel the phenomena they learn in classrooms. Instructors and students conduct lab exercises using DeterLab's dedicated hardware, networks and customized Web-based interface.

We need to develop a new generation of cyber-security researchers who are brought up in the world of R&D performed in realistic settings, and we need to provide the resources necessary for realistic, scientific testing and experimentation. We need to develop the research community to be part of the invention of new models of R&D and tech transfer. We cannot hope to begin to change the dynamics of the asymmetric cyber space if we don't have knowledgeable researchers, educators, I.T. operators, users and citizens.

- **Recommendation #4** – ***Increase educational programs in cyber-security research and development, with an emphasis on doctoral degrees.***

The Cybersecurity Enhancement Act of 2013 includes provisions for addressing this recommendation in sec. 106, Federal Cyber Scholarship For Service
18 Program; sec. 107, Cybersecurity Workforce Assessment; and sec. 108, Cybersecurity University-Industry Task Force.

3. Summary

Cyber security is now a constant, serious and accelerating challenge in every facet of American society. We have become completely dependent on cyber capabilities and, as a result, highly vulnerable to wide-ranging threats. Where these once were largely annoying hacker probes and network intrusions, we now face organized crime and state-sponsored cyber-terrorism. Despite many years of research, we are still on the losing side of an asymmetric battle. These dynamics must be changed to protect US government information, corporate trade secrets, and public health and safety, among other vital concerns. We can no longer treat cyber security as an engineering discipline, we must embrace multiple disciplines bringing economists, sociologists, anthropologists and the other sciences to the table to create holistic research agendas.

Increase the breadth and scope of cyber-security R&D, and create opportunities for multi-disciplinary research.

Corporations and government entities often define security as the absence of visible insecurity. Cyber-security R&D often has been small-scale and ad hoc, and has struggled to prove its worth. Research must be grounded in the same systematic approach to discovery and validation that is routine in other scientific and technological disciplines.

New approaches to research and development must be energized – and new findings must be based in hard experimental science – to support crucial cyber-security discovery, validation and ongoing analysis. Only by enabling demonstrable, repeatable experimental results can we provide a sound basis for researchers to leverage prior work – and create new capabilities not yet imaginable.

Formulate a research strategy/agenda to develop open, broad, multi-organizational cyber-security experimentation and testing capabilities.

Technology transfer is particularly difficult in the constantly shifting world of cyber-security. At each stage from initial research idea, advanced prototype, early stage product and widespread adoption, the process can break due to internal factors or sudden shifts in attack methodologies, tools and strategies. The net effect is that many potentially valuable security technologies never see the light of day. Commercializing security technologies in some cases has been largely a matter of chance.

Develop new models of technology transfer operation, funding, partnership and cultural change within organizations.

The U.S. needs deep intellectual resources to change the cyber-threat dynamic fundamentally. In addition to creating, cataloging and monitoring training programs, we need to be prepared to make significant investments in higher education. I applaud the efforts of the National Science Foundation and other federal research agencies to create and fund cyber-security research and education grants. These fundamental research endeavors are the essential catalyst for research breakthroughs. Only by educating the next generation of researchers and educators today can we build the intellectual resources vital to solving tomorrow's problems.

Increase educational programs in cyber-security research and development, with an emphasis on doctoral degrees.

Taken together, these four recommendations form the basis for a multi-pronged, sustainable national program to address cyber R&D challenges – and to pursue the most promising approaches to a new order for research, development and innovation partnerships.

Chairman MASSIE. Thank you, Ms. Benzel.

I thank all the witnesses for their testimony today. Reminding Members that Committee rules limit questioning to five minutes, the Chair will at this point open the round of questions. And I now recognize myself for five minutes.

Mr. Barrett, as a representative of private industry, it was good to hear you acknowledge that it is PayPal's responsibility to ensure security for PayPal's customers. But you alluded to some gaps in the research that exists and that there might be a role for the Federal Government to fund research in these gaps. Can you motivate the need for federal funding in this area and then also talk about what some of those gaps are?

Mr. BARRETT. Yes, I alluded to this problem a little bit in my oral testimony. Essentially, we have a problem at the moment which is we actually don't know how bad the problem is. We—it sounds perverse to say it that way, but essentially, there are hugely disparate estimates that you see flying around in various publications of the scale of the problem. Everybody agrees it is getting worse, but I have three rhetorical questions that I would like to ask and they are significant ones. And actually, at the moment, I defy anybody to answer them.

So again, I am purely talking about cybercrime, not cyber terrorism or cyber warfare. So I work for a commercial enterprise so we have a narrow worldview.

So the questions are these: how much money is lost to cybercrime on an annual basis in the United States alone? And I am not talking about how much money people like me spend on running a defensive team. I am actually talking about dollars that our customers—and therefore we—lose. So that is question one.

Question two is where does it go? Is it all going back into the United States or is it going overseas? And what are the distributions of country? Now, various people in my industry have various hypotheses about where it is going, and certainly, my team has all sorts of interesting hypotheses. But fundamentally, it is unsupported by large-scale data.

And then finally, do those countries actually have good programs themselves to manage cybersecurity, and do they in fact prosecute cyber criminals? Do they even recognize cybercrime violations as being violations of law or are they just oh, well? It is kind of the equivalent of doing some antisocial act and there are no consequences.

We have no answers to those questions today and they are really important ones that I think are at the heart of what the Federal Government could do to help understand the problem better.

Chairman MASSIE. Thank you.

My next question is for Ms. Benzel.

In this bill we are contemplating expanding funding at universities which are typically open universities where sharing is encouraged. And you mentioned the DeterLab at your institution, which is funded by DHS and DOD I think. Can you tell us or give us some level of comfort that we wouldn't be funding efforts that could then be used by our adversaries? Thank you.

Ms. BENZEL. Being part of a major university and having a deep faith in the need for education, we do run an open facility. It is

funded, as I said, by Department of Homeland Security. And so the DeterLab is a national—and yes—it is an international resource that is available for anyone to be able to use. Obviously, we vet our users. Our approach within the DETER system is to be looking at defenses. And defenses need to be something that can be openly developed. Looking at security by obscurity is sure to get us into trouble.

Now, having said that, I am being a deep believer in being able to educate our next generation and to do publications, et cetera, there are opportunities to do research in other environments which might be more closed and might be providing some classified support for. But we advocate an openness in educating the next generation. Thank you.

Chairman MASSIE. Thank you very much. DeterLab makes a lot more sense than DeterLab.

Ms. BENZEL. We do try and deter the attackers as we say. Thank you.

Chairman MASSIE. Okay. I now recognize Ranking Member Ms. Wilson for five minutes.

Ms. WILSON. Thank you, Mr. Chairman. Mr. Chairman, as outlined in my opening statement, a few of the agencies within our Committee's jurisdiction have indicated that sequestration could impact their cybersecurity research and development portfolios. I would like to place two letters in the record, one from NSF and one from DHS, detailing those potential impacts.

To all, in his testimony, Dr. Chang recommends that the legislation raise the trajectory of cybersecurity research and development spending from its historical levels because it would create long-term benefits in our effort to improve the Nation's cybersecurity posture. As you are all likely aware, sequestration is set to take effect on Friday. Sequestration will cut federal R&D budgets by 8.2 percent, and agencies like NSF and DHS have indicated that research in cybersecurity may be affected.

How would the security posture of the United States be impacted if sequestration were to take effect and cybersecurity research and development was significantly cut? Dr. Chang?

Dr. CHANG. In the 2010 CSIS report, we reported a number of about 2/10 of one percent of the federal R&D budget was spent on cybersecurity. And I looked recently. That number is just a little bit larger now. If you think about the priorities that the Nation is now placing on cybersecurity, the fact that it is something less than one percent seems to be a small number. It is not for me to determine what the priorities are but that just strikes me as a sort of a low number.

I guess I am suggesting that it needs to be a long-term prospect. I mentioned this analogy with planting trees. I am suggesting that we need to plant a few trees to place some bets on some research issues that are going to build over time. Research certainly won't guarantee answers, but as I mentioned as related to infectious diseases, we need to understand causes. We need to understand solutions. We need to understand countermeasures. We know how to do it. We have done it before. We have gone after large public programs before. And my suggestion is research is required to make

some long-term bets and begin changing the vector on what the defensive posture looks like.

Ms. WILSON. Ms. Benzel?

Ms. BENZEL. Yes, I think that we have begun to see some progress in the funding, of course, at a very small level as Dr. Chang says in being strategic about our cybersecurity R&D. If we are to slow that down as a result of funding cuts with sequestration, then we have set ourselves back. We are already on the losing end of an asymmetric battle. And giving our adversaries another year to gain a leg up while we fight our own internal budget is only going to make the situation much worse.

You know, as it is with funding cycles with places like the National Science Foundation it takes close to a year from the time I, as a researcher, have an idea, submit that idea, and get a contract. And so again introducing another delay as a result of the budget battles is only going to set us back. And in particular, a point in time when these agencies have become much more strategic, better coordinated, and better focused in their research. We have researchers in the pipeline. We have projects that are happening today, and we can't afford to stop them, slow them down, or lessen and weaken their effects while the adversaries are on a dramatic increase as we have seen recently.

The change that we see in the adversarial landscape in the last year is ten times what we saw in the ten years before. And so any gap in funding is going to be extremely detrimental. Thank you.

Ms. WILSON. Thank you, Mr. Chair.

Chairman MASSIE. On the gentlelady's request to include two letters in the record?

Ms. WILSON. I have them.

Chairman MASSIE. Without objection, so ordered.

[The information appears in Appendix II]

Chairman MASSIE. I now recognize Chairman Bucshon for five minutes.

Mr. BUCSHON. Thank you, Mr. Chairman.

And there has been some emphasis on the importance of social science research and cybersecurity, among other areas, partly because so much security has to do with human behavior. And the Cybersecurity Enhancement Act supports this type of work in Section 104 of the legislation.

The question is—I will direct this to Mr. Barrett first—is—let me say a couple of things that have been funded recently—$1.2 million to pay seniors to play video games, $764,825 to study how college students use mobile devices for social networking. So with these type of things being funded, how should we prioritize social science research conducted by the National Science Foundation to ensure that such work is focused on critical national needs such as cybersecurity?

Mr. BARRETT. I am not sure whether it is necessarily proper for me to have an opinion on how Congress should prioritize the work of the National Science Foundation, but I do think there are key research gaps, and certainly, in a number of areas in part about cybersecurity education, which is woefully lacking across the spectrum from young kids up through college-level curricula and various different levels. As Dr. Chang alluded earlier, we don't frankly

have enough information security professionals in the field. There is essentially a major skills shortage there. There was basically zero unemployment in my field throughout the recession. And that in its own right is saying something.

Very clearly, there is a lot of work that can be done in understanding behavior around how people interact with computers from a security perspective. And that certainly is a topic worthy of research. Because if you don't understand how people use the computers, especially for security tasks, then it is very hard to see what you can do with them. But I should——

Mr. BUCSHON. Yes, thank you very much. And again, the Cybersecurity Enhancement Act supports this type of work.

Dr. Chang, do you have anything to add?

Dr. CHANG. I do. Thank you. I mention in my written testimony that cybersecurity is a wicked problem, wicked not meaning evil but wicked being resilient to solution. A characteristic of the wicked problem is that what you believe is a solution may actually make things worse. As it relates to that kind of the human component, I am reminded of a concept known as risk homeostasis, and that is basically the idea that people have sort of a risk level that they generally operate at, and if they believe that something is now more safe, they will actually act riskier.

There are some classic experiments showing that when taxi drivers are given better safety on their taxicabs, let us say antilock brakes, you would think that the incidents of accidents would actually go down because the cars are safer, you can steer better and stuff at high speeds. It turns out that the level of accidents might actually go up a little bit because the taxi driver started thinking they were safe and started driving faster and causing more accidents.

Same thing might be happening in cybersecurity such that you are actually making—you are telling the user that they are actually now more safe. When they think now I am more safe, and now I am going to start doing riskier things. And so it is just a sort of very complex thing where you have the best intention that a solution is making something better but it actually makes it worse.

Mr. BUCSHON. Thank you. And this will be directed at Ms. Benzel. I am a parent. I have kids. And I know how my kids almost shut down one of my computers, essentially a black screen. I had to get a computer guy to come out and get it back, and there were literally hundreds of viruses and Trojans and everything else. So I mean I am amazed at what children can do on a computer. And however, there are threats that are directed at all of us through children. Does the current parental control technology adequately protect minors against this type of threat if used properly or are there areas of research and developmental efforts to address this?

Ms. BENZEL. Yes, I would have to say I am not a particular expert in the current set of parental control technology that is out there. I believe that looking at how we model the human behavior and understanding, as Dr. Chang said, the relationship between the way people use their computers. And I am just as concerned about our children as we are to the seniors or the uneducated users. And so I believe that we do need to advance that technology,

but I would have to get back to you on the state-of-the-art in the current parental technology.

Mr. BUCSHON. Thank you. I yield back.

Chairman MASSIE. Thank you. I now recognize Mr. Lipinski for five minutes.

Mr. LIPINSKI. Thank you, Mr. Chairman.

As many people here know, I am a—used to be—maybe I still am—a political scientist, and I know that there is—I have seen plenty of bad social science research in my time. But I think it is important—and I am not trying to start a fight here on this but I know that the—I pay attention—I look to see what is going on and what is being said about some of the supposedly bad research that is being funded. And my understanding is—was the $1.2 million videogame claim was given a pants-on-fire by PolitiFact because it was helping to study how to keep seniors sharp and keep their cognitive skills up as they are getting older.

But that said, I mean there is some bad research but we need to be doing good research. Obviously, there are—as all of you have pointed out—social science research and how people interact is key because it is one of the weakest links that we have right now in cybersecurity.

I wanted to ask about technology transfer. Ms. Benzel had mentioned barrier technology transfer in your testimony. I have a great deal of interest in this, particularly in areas like cybersecurity. It is vital that we translate as much federal research as possible to new products and new companies that we can help keep our cyber infrastructure secure, and also it has the added benefit of creating new jobs so long as we can also address the workforce and education issues that our witnesses have raised.

But I just want to ask the panel, what steps can Federal Government take the best partner with industry in encouraging technology transfer in the cybersecurity sector? Ms. Benzel?

Ms. BENZEL. Yes, thank you very much for your question. It is an important area.

So we do need Federal Government to help us fill the gap between the university research and industry. And I think I can speak somewhat authoritatively to that having spent much time in a university, as well as being a Vice President of Research at McAfee. We have all heard about the Valley of Death.

So we really do have some models that are broken between expecting that industry can just pick up and take research prototypes that have been developed in a university kind of setting. So we need strategic funding which pushes us in a particular direction with an awareness. The DHS S&T program run by Dr. Doug Maughan has introduced new efforts to work with VCs to its signet organization to be able to get venture capitalists and to have the researchers be aware of technology transfer from the day that they write their proposals.

The National Science Foundation had introduced its Transition to Practice. I am arguing that we need a lot more of these sorts of things where we have very early-on awareness of where we want to go. And as a researcher, we want to do the fundamental basic research, and that is absolutely necessary. But as researchers, we also want to see our work have an impact. And we need help in

working with the different types of organizations. And that is where we call for, as the bill currently does, industry partnerships with venture capitalists, with different kinds of technology organizations. There is really nothing currently in that middle to help fill the gap between the research dollars and the product dollars. And I have to say, unfortunately, it is not realistic to believe that industry can simply pick up and do it. Industry is focused on its near-term market, next quarter features, and are totally market-driven and sales driven, particularly in today's economy. And so we need some bridging dollars which should come from combinations of university, public/private partnerships, and federal funding in that new area.

Thank you very much.

Mr. LIPINSKI. Dr. Chang, do you want to add something?

Dr. CHANG. Sure. I will just support what Terry mentioned.

There is this model I like to use: technology transfer is a contact sport. So it is not uncommon for the private sector to establish sort of I guess what you might call lab-lets or sort of mini-labs with the university. And the folks in the private sector would work sort of shoulder-to-shoulder with the folks at the university such that when an innovation is developed, it isn't sort of tossed over the cubicle wall and you would like for the private sector company to incorporate it. But rather, they are generated together.

To the extent that this kind of notion, of kind of, working hand-in-hand between the government, between the private sector and academia would be representative of this notion of let us develop the technologies together. Technology transfer is a contact sport. Let us have them work together. I think that is a useful concept here.

Mr. LIPINSKI. Thank you.

A quick question. Mr. Barrett mentioned NSTIC. I just want to know when will we be able to do—instead of having passwords, have a thumbprint that we use to identify ourselves?

Chairman MASSIE. Very quickly, please.

Mr. BARRETT. Yes, we are actually working on that. That is the FIDO Alliance work that I mentioned at the beginning, which is trying to develop open standards to actually make those kind of technologies become much more widely used. And I think you will actually see products deployed in the market before the end of the year that do exactly that.

Chairman MASSIE. Thank you.

I now recognize Mr. Hultgren.

Mr. HULTGREN. Thank you, Chairman. Thank you all for being here. I appreciate it very much.

This would be first addressed to all of you. My understanding is this growing mass of data that is available online certainly has implications for cybersecurity. In some ways, I know the data can be analyzed to help identify potential cyber threats, but I also know in another way the data provides bad actors with additional opportunities to exploit that data.

I wonder can you discuss how the emerging big data phenomenon poses both challenges and opportunities for cybersecurity research and development, and also just any recommendations you

might have for policymakers to address this phenomenon in a beneficial way and not a harmful way?

Dr. CHANG. Sure. I guess I will kind of mention the notion of dual use. So many of the cyber technologies are so-called dual use. So my company, 21CT, Inc., basically has capabilities to analyze big data to sort of find suspicious behaviors in an attempt to improve the defensive posture of somebody's network. At the same time, an adversary could use similar technologies to sort of target folks similarly to look for vulnerabilities and so forth.

So it is always kind of a really important kind of balancing act and kind of risk assessment proposition such that you will always know that the technologies that could be used for defense could potentially be flipped over. So it is important to kind of understand both sides, understand the technologies deep enough and then make sure you sort of come to the right balance point.

Ms. BENZEL. Well, as a researcher I find big data to be very exciting. From the research point of view and networking and network cybersecurity, we have always been lacking in data. And so again, DHS has its PREDICT program and some of the researchers in my organization have done some really groundbreaking work at analyzing the data, mapping the Internet, the first Internet census to give us information both about the known spaces and the dark spaces.

Clearly, in all of our research, there are two sides to it and we need to be very understanding about how things could be used against us.

I say the other point to also bring in to this discussion about big data are issues with privacy. And so as citizens, we need to understand how the data is being used, stored, and moved about in transit.

Mr. HULTGREN. Mr. Barrett, before you answer, I would love to hear your thoughts on this as well, but I have one other additional question I would like to ask you so if maybe you can respond to both. We already talked a little bit about authentication—online authentication and the challenges there. I understand many European governments issue voluntary electronic identification cards combining two unique identifiers to serve as a type of online passport. But for various reasons, I believe the United States is unlikely to endorse any sort of government-sanctioned identification mechanism. I understand businesses have been working for years on providing different online identity schemes to consumers and that the Administration's National Strategy for Trusted Identities in Cyberspace, or NSTIC, intend to use that work to find common standards for online identities.

I wondered in your view should the government be involved at all in this process? If so, is NIST the appropriate agency to coordinate the effort? How do we ensure privacy? And what prevents this effort from eventually resulting in regulations that inhibit innovation?

Mr. BARRETT. So we have been enthusiastic supporters of the NSTIC initiative ever since it was first proposed. Simply because, as Congresswoman Lofgren said when she introduced me, a decade ago I chaired the Liberty Alliance, which is an open standards organization in the identity management space. It has actually prov-

en quite difficult to develop really large-scale identity ecosystems on the Internet.

We show a lot of promise for users, and so tying that back to the question about breaches in big data, the silver lining in the cloud of all of the data that has been published in last few years essentially as a byproduct of criminal activities is that we now actually understand how consumers in large-scale use passwords in particular. And the answer is a depressingly large number of them, something like 2/3 of them, use the same password absolutely everywhere they go on the Internet, with a net effect that their security of every single account they possess is now the security of that least secure place they visited.

And so having an ecosystem that is built around consumers managing their own identity online and allowing the Federal Government to help kind of just appropriately nudge that but not place too constricting a role is very important. And that is actually why a guy on my team was the first Co-Chair of the Identity Ecosystem Steering Group so—

Mr. HULTGREN. My time is expired. Thank you all very much. Thank you, Mr. Chairman.

Chairman MASSIE. Thank you.

I now recognize Mr. Bera.

Mr. BERA. Thank you, Mr. Chairman.

As an academic physician who comes out of a research background, I truly appreciate the analogy with healthcare and what we do in medicine and the importance of doing research in our academic and research universities. The fact that we do a lot of experiments, that we look for solutions and we fail a lot, but we are constantly feeding that back into the system. And then we have that major breakthrough. Where we fall down in the academic centers—and Ms. Benzel touched on it—is we don't know how to then take those ideas to market.

You touched on the issue of technology transfer and how important that is. I am a firm believer that we would not be able to do the research that we do without the Federal Government's funding of our academic centers. But we do need to do a better job with technology transfer.

What would your suggestion be as a best practice model of taking idea to market given that you have worked on both sides of this?

Ms. BENZEL. Well, thank you very much. You know, I agree with Dr. Chang. It is a contact sport. We can't do the wait-until-the-end-and-throw-it-over. And so I think the best practice model is early engagement. Engage early and often. So they say encouraging the fundamental research funding organizations to call out for tech transfer from day one from the time you write your proposal and come up with your idea, opportunities for communications and meetings with a variety of industry partners, opportunities to understand the needs that are out there and to work with different kinds of funding models both with things such as venture capital organizations who might be willing to take some of the risk in early technology and also on the university side.

So at the University of Southern California we have the Stevens Institute that works with our researchers early on. So early and often. Thank you.

Mr. BERA. Absolutely.

Now, also as a former Associate Dean out of University of California Medical School, we focus a lot on the workforce issue recruiting the best and the brightest and then retaining those individuals. You know, on the issue of cybersecurity, on the issue of making sure we have the computer science professionals, we don't have enough engineers in this country and we are not graduating enough engineering students or programmers. In other sectors of IT we are certainly trying to get that workforce from abroad. But on the issue of cybersecurity, we need a homegrown workforce because this—these are issues that are critical to national security.

Dr. Chang, you touched on this a bit. What are some models that we can use to continue to recruit and retain the best and the brightest to go into areas of information technology and then go into both the service sector working for the Federal Government, working for our Department of Defense and Department of Homeland Security? Because they can make 10 times as much going off into the private sector but we need some of the best and the brightest working to protect our country.

Dr. CHANG. I was recently in a meeting with some folks in Austin where we talked about a very sort of broad approach that would incorporate trying to recruit students of many ages in many disciplines. There is a program that has recently started in New Jersey. It is referred to as Cybersecurity Centers, and they basically have these kind of initial competitions that begin attracting people from all walks of life, maybe former military. There are 16 roles, just a whole group of folks. And then depending on how they do in that initial competition—and it is a fun competition. It sort of capitalizes on people's interest in just competing and sort of a person-on-person competition. And then depending on how you do with that, the people who are more skillful sort of move on.

But it is this notion of can we come up with ideas that attract many, many people, and then if they have a particular propensity to kind of move forward, then you can kind of winnow them down. I mentioned that there was this need for extremely technical deeply elite people. But you have to have a broad funnel to kind of bring them in and then a way to successfully kind of pull out the people who operate the highest levels.

Mr. BERA. Wonderful. So playing off of what you just mentioned, I would ask our Committee to look at returning veterans, men and women who have already shown their patriotism to this country, already understand the service to our Country and the immediate need to protect ourselves and looking for strategic ways to get those folks engaged through our modern GI Bill and so forth to get these skills.

I yield back.

Chairman MASSIE. Thank you.

I recognize Mr. Schweikert.

Mr. SCHWEIKERT. Thank you, Mr. Chairman.

Mr. Barrett, first off, you have a bunch of PayPal folks in Scottsdale, don't you? Yes, it is—when I am in–district, I seem to start every morning having coffee with them. We all attend the same Starbucks. As a company, you have been trying to roll out a number of different products, you know, cell phone billfolds or some of

those types of mechanics. When we are talking about cybersecurity, how much is the threat on this site slowing down your adoption and introduction of new products?

Mr. BARRETT. That is a really interesting question. It is hard to measure. There is certainly good evidence that consumers have been worried about security aspects of Internet solutions ever since the beginning of the Internet. And there is certainly some evidence that they care in the same way about mobile solutions, for example, and that they want to see that they are appropriately protected in those areas.

The difficulty, of course, is in saying how much does the apparent lack of those features really impact their adoption? And so, for example, if you see a—one solution that has a lot of barriers to it, in terms of it is hard to use and has a lot of security features; but on the other hand, you have another very similar product that was much easier to use because it didn't have all these apparent security things that you have to do. Whether or not the consumers actually believe that, the one with the more security features is actually safer. And that ties back to the initial research we were talking about a little while ago.

Mr. SCHWEIKERT. Well, Mr. Barrett, some of that is the adoption side. I am interested on your engineering side. Is it a suppressing effect to the design, you know, studio you would have on the introduction of new technologies?

Mr. BARRETT. If I am understanding the question correctly, it would depend on how much overhead we impose on the engineering teams in terms of how much we try to partition them and so forth. So, if we were working on confidential projects, then clearly we will partition those off as well as, yes, we do impose a number of security overheads as we develop those applications. But it is a—it has lots of tentacles in terms of——

Mr. SCHWEIKERT. It is just having a fixation on expansion, economic growth, and new technology. I have always wondered how much of a suppressing effect I have over here.

Mr. Chairman, Ms.—is it Benzel?

Do you agree with Mr. Barrett's earlier comments that we—it is hard to have a quality census of how many bad actors, bad events, bad things that are actually going on in the cyber marketplace?

Ms. BENZEL. Well, most absolutely. I thought his questions were very astute and exactly right on. So——

Mr. SCHWEIKERT. So as a Member of Congress, where would you send me if I really wanted to get from your academic, sort of, view of the world as much data saying, look, here is what the best census we have of banking attacks and this type of attacks? Or where would you go?

Ms. BENZEL. I think that is a very hard question. I mean, clearly, some of our intelligence agencies on the dark side have a good census of some of the levels of attacks that are happening, particularly in nation-state and against nation targets. The different industries tend to keep those things pretty closely held. Now, some of the work that has been done in the past to set up the Information-Sharing and Analysis Centers, the ISACs, are places where that knowledge is known but held close to the chest.

Mr. SCHWEIKERT. Okay. And so right now, you are not sure there is a good collection of the census, shall we say?

Ms. BENZEL. Oh, I don't believe so.

Mr. SCHWEIKERT. Okay. Mr. Chairman, Dr. Chang—and sorry, I am down to just a few, but you actually started to touch on something that I would love to have an extended discussion with you. And that is, how do we finance ourselves right now? Right now, we are sort of in a classic academic sort of model of finance, primary research. And hopefully, there is something that comes out of it.

But what you were describing a little while ago in your experience sounds more like almost the X-prize-type mechanic of bringing people together, whether it be a garage engineer or an academic. And the person that produces something great gets to move forward. Do you think it is time we also start to wedge and design some other ways to finance innovation here?

Dr. CHANG. I will answer that in—maybe in kind of in connection with the question you asked to Mr. Barrett. Basically, security today is not where it needs to be, and fundamentally, somebody is going to have to pay to move security up. It will be the government because they have to prosecute more criminals. It will be software companies because they have to make software more secure. It will be people because people are bearing losses.

So overall I would love to have a longer conversation.

Mr. SCHWEIKERT. Mr. Chairman, thank you for your patience. Sorry.

Chairman MASSIE. Thank you. If Dr. Chang would like to respond in writing for the record, that would be fine.

I now recognize Ms. Esty. Oh, I am sorry. Mr. Peters. Sorry.

Mr. PETERS. Thank you, Mr. Chairman.

And I appreciate the chance to be here today. This is an important industry in my district as well in San Diego, both because we are developing a lot of the software and also because the Navy has a lot of—or the military has a lot of interest in the field.

And Dr. Chang, I am glad you are a UCSD grad, too. I appreciate that.

My question is sort of, you know, we know that—I think it was yesterday that the Global Information Security Workforce Study from Booz Allen Hamilton said that 56 percent of cybersecurity professionals feel that security organizations are short-staffed and that the cybersecurity field is projected to grow 11 percent annually over the next five years. And so there is—I think it is widely understood that there is a gap in the workforce. But what I am sort of interested in is what are the—what is the field of cybersecurity from an academic sense? You described it as an interdisciplinary exercise. We know it is not just computer science or software. But if you were trying to certify someone in cybersecurity, kind of—do you have a sense—maybe you can help me understand what it is that that person would need to know. And that is for anyone.

Dr. CHANG. Sure. I can start. So there are the traditional disciplines that you learn in computer science about programming, about algorithms, about discrete math and so forth. You would add some elements to that in order to focus more specifically in cybersecurity. And so you would add more about networking, perhaps more about analysis. There is this interesting conversation

happening at universities now where they talk about—that there is a classic computer science major and that maybe there ought to be a cybersecurity major as well.

So there are many things in common but it is different enough such that it is worth an interesting dialogue about the extent that there is the creation of a specific major in cybersecurity.

Mr. PETERS. Well, I guess I think it would be helpful for us because the intent of the legislation before us is to kind of secure our future in that. But if we don't know kind of what we are educating—if you don't understand—if you don't have a sense or a consensus about what it is we are seeking to educate people in, we are going to—I think we face some of the concerns that we are not going to be or that the money is going to be bleeding, or we are not going to be effective?

So if it is anthropology or if it is law in addition to these technical things, is there a way to land that plane?

Ms. BENZEL. So first off, I think you need to make a distinction between education and training. So many of the training organizations and CISSP certifications, that is one level of something that is about operations and being able to run things.

And then there is the education challenge in terms of creating new researchers and new educators and Ph.D.'s. I think that we are just as a community—as Dr. Chang said—beginning to put forth master's curriculums in cybersecurity. USC is just about to introduce one starting next fall. And really, there are different fields. So cybersecurity is not one narrow field. So there are cybersecurity researchers in defenses, in active security, in mathematical analysis, in networking. And so even in a master's degree, there will be specializations in these different areas drawing from primarily a computer science curriculum but also some engineering, some systems kind of work, networking, and then bringing in an understanding of human behavior.

Mr. PETERS. I guess there is going to be some sense we are going to have to keep adjusting as we go.

Ms. BENZEL. That is right. There is not one answer that fits all.

Mr. PETERS. Mr. Barrett, maybe quickly, you might touch on the first of your rhetorical questions which is how much money are we losing? Do you have a sense of how we go about answering that question?

Mr. BARRETT. I believe the answer is we need to put in place more detailed reporting frameworks in order to actually ascertain the scope of the problem. Because the estimates range all over the place, I mean as low as a few billion up into the trillion range. My own personal view is it is probably in the tens of billions of range. But that would be hard to——

Mr. PETERS. That would be something that would be done by industry presumably. Is that right?

Mr. BARRETT. I believe so, yes.

Mr. PETERS. Okay.

Mr. BARRETT. It certainly could be done. A reporting framework could be developed, but at the moment, what we have is entirely voluntary and it models how much money is lost with how much the company spends on defenses, and those two numbers are quite different as well. And how much do you turn away?

Mr. PETERS. Again, I very much appreciate your being here.

Thank you, Mr. Chairman.

Chairman MASSIE. Thank you.

I want to recognize Ms. Esty—Etsy.

Ms. ESTY. Esty, not the crafting website. Although I would be much wealthier if it were mine.

Thank you very much, Mr. Chairman.

For Dr. Chang and Ms. Benzel, both of you had talked about the need to create a science of cybersecurity. And if you can elaborate a little bit on that, what are the metrics we would need? If we don't know right now if a company is more secure than it was a month ago, where do we even start with this? What sort of research do we need? What sort of metrics do we need to develop so that we even know what we are talking about?

Dr. CHANG. Well, that is one of the key issues. We actually don't have the right language, the right set of metrics to even begin to understand this notion of whether my—the computer this year is more secure than it was last year, if this computer is more secure than somebody else's.

There is kind of this idea of understanding the limits of what is possible. So that is what a science allows you to do. Can I understand how secure something can be? We sort of don't know, kind of what is possible, you know, what are kind of the control bounds. Cybersecurity is an adversarial science. And like anything adversarial, we will probably never completely eliminate it. But if we can establish some sort of control bars that basically say we are going to make it harder for an adversary to kind of get through and maybe the difficulty that their—you know, if we make it too hard for them to get through, then, they will quit trying. But it is this motion of kind of setting some control bars and trying to keep it within that. We certainly won't eliminate crime.

Ms. BENZEL. So we advocate being able to do experimental science. So in many other sciences we have workbenches and labs and we can go in and we can also repeat our peers' experiments and be able to understand what they are. Unfortunately, in computer science and in—particularly in cybersecurity, the experiments are very ad hoc. And so it might work once or it might work in my lab or in my example.

This is one of the challenges also in technology transfer. It may have worked in some researcher's lab under some conditions, but I don't know that it is really going to work. So what we really advocate is that we need an experimental science where we can create hypotheses, we can do an experiment, see the results, modify some parameters, rerun the experiment. And my colleagues similarly have an opportunity to do that just as they would in any of the hard sciences.

Ms. ESTY. Are there any of the federal agencies that are actually doing work on this notion of the metrics that we would even use to measure?

Dr. CHANG. I am aware of some work that has started at NIST, and I would tell you I haven't looked at the work in more detail. I probably need to. But I am recalling from some years ago, oh, maybe 2009 or 2010 within the Computer Security Division at NIST, they started up a program in metrics. It is something I

would need to look at further. But I believe there is some activity happening.

Ms. BENZEL. Metrics is a very difficult area in security and has plagued us for a long time. I would say that DARPA has started some work there and some very fundamental research. The National Science Foundation and DHS S&T always include metrics as a research topic in their calls.

Ms. ESTY. And one final question. As I know some colleagues and friends of my son who is a junior in college, if you could elaborate a little bit more on this adversarial science notion because I think it is different—it strikes me as different than a lot of times what attracts people to science and a sense of the purity and how you go about thinking about recruiting young people designing programs—if they need to have this back-and-forth adversarial approach.

Dr. CHANG. I would have to do some more thinking about this, but the models of the human immune system strike me as a reasonable model. So basically, the human immune system is fighting off adversaries of all kinds. And it is just sort of amazing how versatile and how flexible the human immune system is. The human immune system—by the way, about one percent of human cells are leukocytes, are actually defensive. So when you think about the body is basically allocating about one percent of its cells to defense, that is a pretty substantial number. If you look at the number of lines of computer code, I doubt one percent is dedicated to defense.

The other model that seems to make sense to me in terms of the science is in the field of actually agriculture. So agriculture also has pests, and the pests try to eat the crops. And you can either make the crops more resilient or you kill the pests. I mean that is another sort of adversarial model that seems to be relevant.

Chairman MASSIE. Thank you. I want to thank Chairman McCaul for his initiative with this bill and his persistence in reintroducing it and especially his patience today.

And I recognize him now for five minutes.

Mr. MCCAUL. I thank the Chairman.

And Dr. Chang, let me say thank you for your service on the CSIS Commission and to the Nation and to the University of Texas in Austin.

And Ms. Benzel, I agree with you our adversaries are moving forward, moving ahead. They are attacking our federal agencies every day. In support—and building a record in support of this legislation, I see this bill doing several things, applying NIST standards to the Federal Government. It provides—it bolsters research and development in this area, a private-sector university federal task force, education and awareness piece and procurement standards within the Federal Government.

And I would like to go through each of you and if you could tell me how you believe—if you do—that this legislation will advance the cause for enhancing cybersecurity for this Nation. Mr. Barrett?

Mr. BARRETT. I would give a very brief answer which is maybe not quite so brief.

In general, philosophically, we think that cybersecurity, as Dr. Chang said, is a wicked problem. And as such, there is probably

no single bill that could be passed that will, on its own, materially change the trend line. But on the other hand, the sort of lack of a grand unification theory shouldn't stop us from doing good work. And this bill would definitely appear to be falling into that place where it does no harm and it also does good work in the specific areas it has chosen.

Mr. MCCAUL. That is a very good point. I think—I served on the Speaker's Cybersecurity Task Force, and our first action was to do no harm by legislation. So I appreciate you saying that.

Dr. Chang?

Dr. CHANG. Thank you.

So in advance of reading the bill if I could have picked two things that are critical to improving the Nation's cybersecurity posture it would be research and development and workforce development. And so this legislation to me is just right on target relative to addressing the top two problems. I guess I would add, as I mentioned in my spoken testimony, the notion that we need to be patient about this. You know, I guess it would be great if we could sort of plant a forest and all the trees turn into something that resulted in wonderful research. But we—I see this legislation as important in that it is at least planting a few trees. It allows us to plant some—a few things that will grow into the future.

I would sure hate to be sitting here ten years from now, 20 years from now still saying that we actually don't understand causes. We don't understand solutions. We don't understand countermeasures. And this legislation I believe begins planting a few trees. Thank you.

Mr. MCCAUL. And thanks for making the point about the cyber workforce in the Federal Government. I think that is very, very important as well.

Ms. Benzel?

Ms. BENZEL. Yes, thank you for the opportunity and thank you for your perseverance in this area.

I agree with my colleagues. There is no one answer. It is a very difficult field. But I was quite—very impressed to see this particular bill in two areas that I would call out. And one is the technology transfer recognition of the difficulty of that problem. And I have worked in a number of different public-private partnerships over the years. I was part of the PCAST Committee back in the early 2000s. I see that the opportunity here to do some real planning around university kinds of partnerships and bringing the universities into it so it is a three—tri-part aspect is very exciting in the bill.

The other one is in the science of cybersecurity and understanding that there is a need for research and development kinds of testbeds and experimentation. That is called out in the bill for experimental science.

So I think technology transfer and experimental cybersecurity have a chance to be fundamentally changing. And of course the education and training are important, too.

Mr. MCCAUL. Well, let me thank the witnesses for your expertise and for appearing here today.

Mr. Chairman, thank you for allowing me to participate in this hearing even though I don't sit on the Subcommittee. And I look

forward to the markup and hopefully overwhelmingly passage of the bill and signed into law by the President. Thank you. I yield back.

Chairman MASSIE. Thank you, Chairman McCaul.

In closing this joint hearing, I would like to recognize Chairman Bucshon for a moment to say a few words.

Mr. BUCSHON. Thank you, Mr. Chairman.

I just want to remind everyone about a few facts. Overall spending in the Federal Government has gone up 17 percent since 2008. This year, we are on track to spend $3.6 trillion with a tax collection of $2.7 trillion, which, by the way, is the highest amount in history that is being projected. We have 16.5 trillion in national debt, over 1 trillion in annual deficits for the past five years running. Recently reported, 110 billion in inappropriate payments the government made just last year across a multitude of federal programs and the current sequester is 85 billion.

I agree that spending cuts need to be more targeted. That is why the House has passed two bills over the last year that would target these cuts more appropriately. So I think that we are very well aware of research and development dollars that need to be there, not only on cybersecurity but other issues. And we will work towards this—a resolution that will help with that situation. Thank you. I yield back.

Chairman MASSIE. Thank you.

I want to thank the witnesses for traveling here today and for their valuable testimony and to the Members for their questions.

Members of the Committee may have additional questions for you and we will ask you to respond to those questions in writing. The record will remain open for two weeks for additional comments and written questions for Members.

The witnesses are excused and this hearing is adjourned.

[Whereupon, at 11:33 a.m., the Subcommittees were adjourned.]

Appendix I

Answers to Post-Hearing Questions

ANSWERS TO POST-HEARING QUESTIONS

Responses by Mr. Michael Barrett

QUESTIONS FOR THE RECORD
THE HONORABLE LARRY BUCSHON (R-IN)
U.S. House Committee on Science, Space, and Technology

Cybersecurity Research and Development: Challenges and Solutions

Tuesday, February 26, 2013

1. I understand the severity of our cybersecurity problem and the possibilities of failing to mitigate an attack; however, I cannot help but feel like this problem is like constantly trying to find a needle in a haystack, and that both the federal government and companies will continually spend without any measure of whether we have done "enough" or how safe our investments make us. Is there any way past this perpetual bottomless pit?

Chairman Bucschon, I appreciate your thoughtful question. You are correct in the fact that it is difficult and sometimes costly, for both the public and private sector, to constantly plug all of the security gaps in our cyber infrastructure and Internet and mobile systems. This topic is in fact one that professionals in the information security domain spend much time discussing. As by definition, it is not possible to be completely "safe" in any walk of life – crossing the street is a dangerous undertaking, but yet we all do it without much hesitation - instead, we aim to simply understand and manage our risks into a zone that we consider acceptable. As such, the questions then become about how much risk is acceptable, how much it will take to bring risks into an acceptable zone, and how quickly that can be accomplished.

As I stated in my testimony before the committee, there are approaches that policymakers could take to address some of the concerns that you reference. For instance, if the federal government invested some funds into research on the greatest cyber risks, not only on cyber terrorism, but also on cybercriminal activities, this could help the public and private sector better target their resources to protect their infrastructure. In addition, it could help law enforcement agencies better understand the current cyber risks and what actions they need to take to deter and, if needed, bring to justice cyber criminals and terrorists.

In addition, we believe that there are measures that the private sector could take to help safeguard their own investments without federal assistance and resources. As I stated in my written testimony, there are certain outdated statutes, like the Electronic Communication Privacy Act, that inhibit private companies from sharing information with each other about potential cyber threats. We believe that if private companies were empowered to work together to mitigate these cyber risks, it would cut down on the amount of money that is lost to cyber-criminal activities.

Again, I appreciate your thoughtful question. If we can ever be of assistance to you and your staff on this very important issue, please do not hesitate to reach out.

Responses by Dr. Frederick R. Chang

QUESTIONS FOR THE RECORD
THE HONORABLE LARRY BUCSHON (R-IN)
U.S. House Committee on Science, Space, and Technology

Cybersecurity Research and Development: Challenges and Solutions

Tuesday, February 26, 2013

1. I understand the severity of our cybersecurity problem and the possibilities of failing to mitigate an attack; however, I cannot help but feel like this problem is like constantly trying to find a needle in a haystack, and that both the federal government and companies will continually spend without any measure of whether we have done "enough" or how safe our investments make us. Is there any way past this perpetual bottomless pit?

Thank you for this question. I think that at least part of the answer lies in the development of robust cybersecurity metrics, and these really don't exist today. How secure is my computer right now? Is it more secure that it was a year ago? How about my company's computer network – is it more secure than it was a year ago? If I doubled my corporate spending in cybersecurity, have I doubled the security of my corporate cybersecurity infrastructure? I can't improve what I can't measure. To the extent that the federal government can help lead the way toward the development of a comprehensive, robust, and rigorous set of cybersecurity metrics, that would be of tremendous value, in my opinion. Perfect cybersecurity is not attainable – we've known this for some time now. So in some sense, it comes down to a risk assessment decision. Can I make it more difficult for an adversary to compromise my network than they have resources or time to do so? If I demand cybersecurity improvement targets (again assuming the existence of a robust set of metrics) such that week after week, month after month, year after year, I'm seeing improvements, then I'm increasing the level of effort and resources needed on the part of the adversary and I'm moving the advantage continually in my direction and away from my adversary.

QUESTIONS FOR THE RECORD
THE HONORABLE EDDIE BERNICE JOHNSON (D-TX)
U.S. House Committee on Science, Space, and Technology

Cybersecurity Research and Development: Challenges and Solutions

Tuesday, February 26, 2013

1. In your testimony, you mention that education and training is vital for all individuals—from users to professionals. Could you please address the role the federal government should play in closing the cybersecurity skills gap? What can or should be done by federal agencies to improve cybersecurity education at the K-12 level, undergraduate level, and graduate level?

Thank you for this question. At the K-12 level I tend to favor approaches that generally get more kids interested in the STEM – science, technology, engineering and math – areas. There are so many activities that compete for kids attention, that to the extent the federal government can create a motivation and focus such that more kids pursue STEM subjects, then I think that would be a win. Some of those individuals will pursue an interest in cybersecurity and that would be terrific. Others may pursue an interest in physics, chemistry, biology or the social sciences, and in my opinion that would be also be a win for the nation. Perhaps at some later time, these particular individuals would develop an interest in cybersecurity. There are many examples of great contributions to cybersecurity from people trained in a different area of science/engineering. I know that there are many outstanding ideas that have been offered as to how to increase interest in the STEM topics in the K-12 years, so I won't repeat them here.

At the post-secondary level, scholarships like the NSF Scholarship for Service (SFS) and the Department of Defense Information Assurance Scholarship Program (IASP) are invaluable tools for bringing talented college students into the field of cybersecurity. While I was at the University of Texas at San Antonio, I had the opportunity to work closely with several students who were holders of these scholarships. I could see first-hand the sort of difference these scholarships made to these students. I believe that by increasing the number and variety of scholarships like this could be a very useful way to help increase the number of well-qualified cybersecurity professionals. While at the University of Texas at Austin some years ago, I had the opportunity to serve as the faculty advisor for the UT-Austin team that competed in the first annual Texas Collegiate Cyber Defense Competition. These sorts of competitions give students a wonderful perspective on the field – one that they cannot get in the classroom. Competitions like this have grown in popularity over the years and to the extent that the federal government can play a role in their continued growth and popularity, I believe that would be an important contributor to increasing the number of trained professionals in the field.

Responses by Ms. Terry Benzel

QUESTIONS FOR THE RECORD
THE HONORABLE LARRY BUCSHON (R-IN)
U.S. House Committee on Science, Space, and Technology

Cybersecurity Research and Development: Challenges and Solutions

Tuesday, February 26, 2013

1. I understand the severity of our cybersecurity problem and the possibilities of failing to mitigate an attack; however, I cannot help but feel like this problem is like constantly trying to find a needle in a haystack, and that both the federal government and companies will continually spend without any measure of whether we have done "enough" or how safe our investments make us. Is there any way past this perpetual bottomless pit?

That's an excellent question, starting with the recognition that we lack useful metrics for assessing the practical benefits of deploying some new security technology, or of expanding the use of existing security technology. That's all too true. And to point out two ways that we can change that, let me explain two reasons for the current lack of metrics.

One factor is that it's only been in the last decade or less that we've realized a fundamental difference in objective between government use of cyber-security technology, and the kind of commercial use that drives the efforts of security vendors to bring new products to market. In the commercial sector, the fundamental benefit of security technology is liability management. Commercial organizations have obligations to their shareholders to protect corporate assets; and they have regulatory obligations to protect regulated assets such as personal data. There is no hard-and-fast measurement of "enough" but there is specific guidance: corporations must demonstrate that they have taken reasonable, usual, and customary measures to exercise due care in meeting those obligations. At any given point in time, once enough spending and enough efforts have been taken to implement best practices in security, there is little or no incremental value in additional spending. Corporate assets will still be at some risk, but if business operations are impacted by a future security event, the company can still demonstrate that they did all that they reasonably could to do prevent and prepare. Regulatory sanctions may still apply, but the company can still demonstrate due care, and avoid penalties being doubled or tripled for negligence.

In short, there is a practical metric for commercial spending on security, and it's not fundamentally based on effective protection so much as customary protection. That motivates the enterprise security vendors to continually expand their offerings with new technologies, to attract early adopters to use it, and then use the early adopters' example to expand the definition of usual and customary measures. While the early adopters may have chosen to use the new technology because of beliefs of effectiveness in their particular environment, later adopters are less concerned with proving effectiveness, and more concerned about demonstrating compliance. That's why enterprise security spending is at a fairly steady state of continuing to pay for new security technologies.

But in the last decade or less, we've come to understand that in some government sectors, as well as private-sector operators of critical infrastructure, effectiveness is actually important. And unfortunately, it is very often the case that a new security technology becomes available for commercial use, without any real demonstration of effectiveness in a realistic environment. Both the commercial and research parts of my career, I've seen many innovations work well in a limited test setting, but not work as intended in large scale complex real world networks and systems. And it's no surprise! They were never tested in such settings. In a very real sense, the early commercial adopters are the first real testers. And even if effectiveness is actually demonstrated in some of a new security product's vendors' customers, there is no guarantee that it will work the same for others.

That why I believe so strongly in the value of cyber-security experimentation and testing of security innovations. I've seen first hand a new breed of researchers who are now able to repeatably test innovations, scientifically measure their effectiveness in a variety of conditions, and have the data needed to tune their innovations to operate better in more large and complex settings. That means the anew technology can come to market along with specific tests to measure how effective it is. Commercial organizations may adopt it in order to keep up with the expanding definition of due care, but in the critical infrastructure sector, potential adopters can make much more informed decisions, and actually measure effectiveness using metrics that come with the new technology.

The second factor is easier to explain given the first. The path to commercial adoption has often been through large security vendors who primarily want to acquire new technology in order to add a new tool to the toolset that they offer customers. In the last decade, we've seen a number of innovations in defending against increasing subtle malicious software attacks. The vendors have taken some of them to market primarily to be able to get those early adopters, expand the definition of due care, and up-sell the rest of their existing customer base to buy the latest additions to the toolset.

As a result, much research was in specific silos of existing security problems, to come up with incremental improvements. And with good reason -- the "market" for security R&D was the commercial vendors who wanted incremental improvements.

Again, in just the last few years, R&D funders have made successful effort in directing researchers away from existing silos, and toward new problems or known hard problems, as well as problems that are specific to critical infrastructure, and emerging technology for critical infrastructure, for example, the emerging smart grid. There may not be a large and quantifiable market for the incumbent security vendors to spend on acquiring smart grid technology, for some years to come. But the funding organizations have been directing researchers to those problems anyway, and directing them to use scientific facilities -- the testbeds, ranges, and community labs -- to prove the effectiveness of their innovations in settings that are realistic to the environment that they are targeted to, even if those environments seems like niche markets today. It's research that has to be done to be able to secure our critical infrastructure as it evolves, rather than waiting for new assets and

new attacks on them, before even starting the R&D to protect them -- which is essentially what happened with the early days of the commercial internet.

However, I'm sympathetic to the concern over continued spending. What I've said here is that on the R&D side, the continued spending has recently been moving towards targeted critical needs and scientifically demonstrated effectiveness in meeting those needs. But the R&D spending will have to continue, because the technology that we need to protect is also evolving. But I think that we've begun a re-orientation so that more of that R&D funding is well-spent in terms of national interests. That's why I believe in the importance of experimentation and test as well as needed research in measurement, metrics, assessment and infrastructure for research and development.

QUESTIONS FOR THE RECORD
THE HONORABLE EDDIE BERNICE JOHNSON (D-TX)
U.S. House Committee on Science, Space, and Technology

Cybersecurity Research and Development: Challenges and Solutions

Tuesday, February 26, 2013

1. In your testimony, you mention that education and training is vital for all individuals—from users to professionals. Could you please address the role the federal government should play in closing the cybersecurity skills gap? What can or should be done by federal agencies to improve cybersecurity education at the K-12 level, undergraduate level, and graduate level?

There is no question that we are facing a serious shortage for security professionals. To obtain a greater yield of defenders out of our STEM education, we have to make cyber security more attractive to the learners at a younger age. The ability to provide grad students with a realistic test environment to run real malware and conduct scientific security work is great, but we need to something similar in spirit for undergrads and high school students. Packaged courseware is good for moving down into undergrad teaching as tech students make choices about what career to pursue. But more than courseware, we need to develop techniques for engaging learners on their own terms, at the age where their interest in the cyber world is beginning, rather than waiting until college or grad school. That may take the form of science competitions, or youth oriented cyber competitions, capture the flag games, or even computer and mobile gaming targeted at building cyber skills. There are a number of organizations initiating these types of efforts.

However, in order to realize a significant paradigm change we need to explore new programs and with nation wide scope and impact. Current federal funding for STEM are an important first step and should be encouraged and expanded. Not only is there a need for federal programs in traditional education venues, it is important to provide education, training and cyber awareness in public programs.

At the K – 12 programs federal funding can begin by providing education and training of teachers, development grants for technology, and innovative reach back from university programs into K-12 institutions. Similar programs can advance educational opportunities; while at the graduate level increasing funding for basic research in cyber security provides increased funding for graduate students and new curriculum development.

Finally, it is important that steps be taken to specifically target women and underrepresented minorities in cyber security at all levels. The field of cyber security lacks diversity. There are far fewer women and underrepresented minorities in cyber field than in many comparable computer and engineering fields.

Appendix II

Additional Material for the Record

DEPARTMENT OF HOMELAND SECURITY LETTER SUBMITTED BY
REPRESENTATIVE FREDERICA S. WILSON

Secretary

U.S. Department of Homeland Security
Washington, DC 20528

Homeland Security

January 31, 2013

The Honorable Barbara A. Mikulski
Chairwoman, Committee on Appropriations
United States Senate
Washington, DC 20510-6025

Dear Chairwoman Mikulski:

Thank you for your letter regarding the potential impacts of the March 1st sequestration. I share your deep concerns about the effects this unprecedented budget reduction to Fiscal Year (FY) 2013 funding will have on the Department of Homeland Security (DHS), its missions, and our Nation's security and economy.

Reductions mandated by sequestration would undermine the significant progress the Department has made over the past ten years and would negatively affect our ability to carry out our vital missions. Sequestration would roll back border security, increase wait times at our Nation's land ports of entry and airports, affect aviation and maritime safety and security, leave critical infrastructure vulnerable to attacks, hamper disaster response time and our Surge Force capabilities, and significantly scale back cyber security infrastructure protections that have been developed in recent years. In addition, sequestration would necessitate furloughs of up to 14 days for a significant portion of our frontline law enforcement personnel, and could potentially result in reductions in force at the Department. The following provides specific examples of the potential impacts of Sequestration on the Department:

- U.S. Customs and Border Protection (CBP) would not be able to maintain current staffing levels of Border Patrol Agents and CBP Officers as mandated by Congress. Funding and staffing reductions will increase wait times at airports, affect security between land ports of entry, affect CBP's ability to collect revenue owed to the Federal Government, and slow screening and entry programs for those traveling into the United States.

- U.S. Immigration and Customs Enforcement (ICE) would not be able to sustain current detention and removal operations or maintain the 34,000 detention beds mandated by Congress. This would significantly roll back progress that resulted in record-high removals of illegal criminal aliens this past year, and would reduce ICE Homeland Security Investigations' activities, including human smuggling, counter-proliferation, and commercial trade fraud investigations.

- The Transportation Security Administration would reduce its frontline workforce, which would substantially increase passenger wait times at airport security checkpoints.

- The U.S. Coast Guard (USCG) would have to curtail air and surface operations by nearly twenty-five percent, adversely affecting maritime safety and security across nearly all missions areas. A reduction of this magnitude will substantially reduce drug interdiction, migrant interdiction, fisheries law enforcement, aids to navigation, and other law enforcement operations as well as the safe flow of commerce along U.S. waterways.

- Furloughs and reductions in overtime would adversely affect the availability of the U.S. Secret Service workforce, and hinder ongoing criminal investigations.

- Reductions in funding for operations, maintenance and analytical contracts supporting the National Cybersecurity Protection System (NCPS) would impact our ability to detect and analyze emerging cyber threats and protect civilian federal computer networks.

- The Federal Emergency Management Agency's Disaster Relief Fund would be reduced by over a billion dollars, with an impact on survivors recovering from future severe weather events, and affecting the economic recoveries of local economies in those regions. State and local homeland security grants funding would also be reduced, potentially leading to layoffs of emergency personnel and first responders.

- The Science and Technology Directorate would have to stop ongoing research and development including: countermeasures for bio-threats, improvements to aviation security and cyber security technologies, and projects that support first responders.

- The Department would be unable to move forward with necessary management integration efforts such as modernizing critical financial systems. This would hinder the Department's ability to provide accurate and timely financial reporting, facilitate clean audit opinions, address systems security issues and remediate financial control and financial system weaknesses.

Hurricane Sandy, recent threats surrounding aviation and the continued threat of homegrown terrorism demonstrate how we must remain vigilant and prepared. Threats from terrorism and response and recovery efforts associated with natural disasters will not diminish because of budget cuts to DHS. Even in this current fiscal climate, we do not have the luxury of making significant reductions to our capabilities without placing our Nation at risk. Rather, we must continue to prepare for, respond to, and recover from evolving threats and disasters – and we require sufficient resources to sustain and adapt our capabilities accordingly. We simply cannot absorb the additional reduction posed by Sequestration without significantly negatively affecting frontline operations and our Nation's previous investments in the homeland security enterprise.

The Department appreciates the strong support it has received from Congress over the past 10 years. As we approach March 1, I urge Congress to act to prevent Sequestration and ensure that DHS can continue to meet evolving threats and maintain the security of our Nation and citizens. Should you have any questions or concerns at any time, please do not hesitate to contact me at (202) 282-8203.

Yours very truly,

Janet Napolitano

NATIONAL SCIENCE FOUNDATION LETTER SUBMITTED BY
REPRESENTATIVE FREDERICA S. WILSON

NATIONAL SCIENCE FOUNDATION
4201 WILSON BOULEVARD
ARLINGTON, VIRGINIA 22230
February 4, 2013



OFFICE OF THE
DIRECTOR

The Honorable Barbara Mikulski
Committee on Appropriations
United States Senate
Washington, DC 20510

Dear Chairwoman Mikulski:

This letter is in reply to your request for information regarding the impact of a possible sequester on the National Science Foundation's (NSF) operations and activities.

At NSF, the central focus of our planning efforts will be predicated on the following set of core principles:

- First and foremost, protect commitments to NSF's core mission and maintain existing awards
- Protect the NSF workforce
- Protect STEM human capital development

By adhering to these principles and the government-wide guidance provided in OMB memorandum M-13-03, "Planning for Uncertainty with Respect to Fiscal Year 2013 Budgetary Resources," the Foundation will best accommodate the possible sequestration reductions in ways that minimize the impact on our mission, both short- and long-term.

We do know, however, that the required levels of cuts to our programmatic investments would cause a reduction of nearly 1,000 research grants, impacting nearly 12,000 people supported by NSF, including professors, K-12 teachers, graduate students, undergraduates, K-12 students, and technicians.

Vital investments in basic research, leading edge technology, and STEM education would be jeopardized. Impacted areas could include:

- NSF-wide emphasis on sustainability, including vital investments in clean energy research;
- Major investments critical to job creation and competitiveness, such as advanced manufacturing and innovation;
- Advances in cybersecurity aimed at protecting the Nation's critical information technology;
- Pathbreaking efforts to improve pre-college and undergraduate education, including new investments to transform undergraduate science courses.

Major Research Equipment and Facilities Construction funding at $160 million or less in FY 2013 will result in the termination of approximately $35 million in contracts and agreements to industry for work in progress on major facilities for environmental and oceanographic research. This would directly lead to layoffs of dozens of direct scientific and technical staff, with larger impacts at supplier companies. In addition, out year costs of these projects would increase by tens of millions because of delays in the construction schedule.

Thank you for the opportunity to provide you with this look at possible impacts of a sequester on the Foundation. Please let me know if you have any additional questions, and as always, thank you for your strong support of the Foundation.

Sincerely,

Subra Suresh
Director