AUTHENTICATED
U.S. GOVERNMENT
INFORMATION
GPO

PROTECTING OUR NATION'S CYBER SPACE: EDUCATIONAL AWARENESS FOR THE CYBER CITIZEN

HEARING

BEFORE THE

SUBCOMMITTEE ON TECHNOLOGY, INFORMATION POLICY, INTERGOVERNMENTAL RELATIONS AND THE CENSUS

OF THE

COMMITTEE ON GOVERNMENT REFORM

HOUSE OF REPRESENTATIVES

ONE HUNDRED EIGHTH CONGRESS

SECOND SESSION

APRIL 21, 2004

Serial No. 108–209

Printed for the use of the Committee on Government Reform

Available via the World Wide Web: http://www.gpo.gov/congress/house
http://www.house.gov/reform

U.S. GOVERNMENT PRINTING OFFICE

96–315 PDF WASHINGTON : 2004

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

COMMITTEE ON GOVERNMENT REFORM

TOM DAVIS, Virginia, *Chairman*

DAN BURTON, Indiana
CHRISTOPHER SHAYS, Connecticut
ILEANA ROS-LEHTINEN, Florida
JOHN M. MCHUGH, New York
JOHN L. MICA, Florida
MARK E. SOUDER, Indiana
STEVEN C. LATOURETTE, Ohio
DOUG OSE, California
RON LEWIS, Kentucky
JO ANN DAVIS, Virginia
TODD RUSSELL PLATTS, Pennsylvania
CHRIS CANNON, Utah
ADAM H. PUTNAM, Florida
EDWARD L. SCHROCK, Virginia
JOHN J. DUNCAN, JR., Tennessee
NATHAN DEAL, Georgia
CANDICE S. MILLER, Michigan
TIM MURPHY, Pennsylvania
MICHAEL R. TURNER, Ohio
JOHN R. CARTER, Texas
MARSHA BLACKBURN, Tennessee
PATRICK J. TIBERI, Ohio
KATHERINE HARRIS, Florida

HENRY A. WAXMAN, California
TOM LANTOS, California
MAJOR R. OWENS, New York
EDOLPHUS TOWNS, New York
PAUL E. KANJORSKI, Pennsylvania
CAROLYN B. MALONEY, New York
ELIJAH E. CUMMINGS, Maryland
DENNIS J. KUCINICH, Ohio
DANNY K. DAVIS, Illinois
JOHN F. TIERNEY, Massachusetts
WM. LACY CLAY, Missouri
DIANE E. WATSON, California
STEPHEN F. LYNCH, Massachusetts
CHRIS VAN HOLLEN, Maryland
LINDA T. SANCHEZ, California
C.A. "DUTCH" RUPPERSBERGER, Maryland
ELEANOR HOLMES NORTON, District of Columbia
JIM COOPER, Tennessee

BERNARD SANDERS, Vermont (Independent)

MELISSA WOJCIAK, *Staff Director*
DAVID MARIN, *Deputy Staff Director/Communications Director*
ROB BORDEN, *Parliamentarian*
TERESA AUSTIN, *Chief Clerk*
PHIL BARNETT, *Minority Chief of Staff/Chief Counsel*

SUBCOMMITTEE ON TECHNOLOGY, INFORMATION POLICY, INTERGOVERNMENTAL RELATIONS AND THE CENSUS

ADAM H. PUTNAM, Florida, *Chairman*

CANDICE S. MILLER, Michigan
DOUG OSE, California
TIM MURPHY, Pennsylvania
MICHAEL R. TURNER, Ohio

WM. LACY CLAY, Missouri
STEPHEN F. LYNCH, Massachusetts

EX OFFICIO

TOM DAVIS, Virginia

HENRY A. WAXMAN, California

BOB DIX, *Staff Director*
DAN DALY, *Professional Staff Member*
JULIANA FRENCH, *Clerk*
ADAM BORDES, *Minority Professional Staff Member*

CONTENTS

	Page
Hearing held on April 21, 2004	1
Statement of:	
Clinton, Larry, chief operating officer, Internet Security Alliance; Andrew Howell, vice president, Homeland Security, U.S. Chamber of Commerce; Rodney Petersen, security task force coordinator, EDUCAUSE; and Douglas Sabo, member, board of directors, National Cyber Security Alliance	58
Swindle, Orson, Commissioner, Federal Trade Commission; and Amit Yoran, Director, National Cyber Security Directorate, Department of Homeland Security	12
Letters, statements, etc., submitted for the record by:	
Clay, Hon. Wm. Lacy, a Representative in Congress from the State of Missouri, prepared statement of	10
Clinton, Larry, chief operating officer, Internet Security Alliance, prepared statement of	61
Howell, Andrew, vice president, Homeland Security, U.S. Chamber of Commerce, prepared statement of	69
Petersen, Rodney, security task force coordinator, EDUCAUSE, prepared statement of	84
Putnam, Hon. Adam H., a Representative in Congress from the State of Florida, prepared statement of	5
Sabo, Douglas, member, board of directors, National Cyber Security Alliance, prepared statement of	105
Swindle, Orson, Commissioner, Federal Trade Commission, prepared statement of	15
Yoran, Amit, Director, National Cyber Security Directorate, Department of Homeland Security, prepared statement of	36

PROTECTING OUR NATION'S CYBER SPACE: EDUCATIONAL AWARENESS FOR THE CYBER CITIZEN

WEDNESDAY, APRIL 21, 2004

HOUSE OF REPRESENTATIVES,
SUBCOMMITTEE ON TECHNOLOGY, INFORMATION POLICY,
INTERGOVERNMENTAL RELATIONS AND THE CENSUS,
COMMITTEE ON GOVERNMENT REFORM,
Washington, DC.

The subcommittee met, pursuant to notice, at 2 p.m., in room 2154, Rayburn House Office Building, Hon. Adam H. Putnam (chairman of the subcommittee) presiding.

Present: Representatives Putnam and Clay.

Staff present: Bob Dix, staff director; John Hambel, senior counsel; Dan Daly, professional staff member and deputy counsel; Juliana French, clerk; Suzanne Lightman, fellow; Earley Green, minority chief clerk; and Jean Gosa, minority assistant clerk.

Mr. PUTNAM. A quorum being present, this hearing of the Subcommittee on Technology, Information Policy, Intergovernmental Relations and the Census will come to order. Good afternoon and welcome to another important hearing on cyber security.

I want to welcome you all today to the hearing entitled "Protecting our Nation's Cyber Space: Educational Awareness for the Cyber Citizen." In the past few years, the growth in access and use of the Internet, the increase in high-speed connections that are always on, and the rapid development and deployment of new computing devices has resulted in an expanding global computing network. Although these advances have improved our quality of life, this global network is susceptible to viruses and worms that can circle the world in minutes, not to mention the potential of more malicious cyber attacks. While businesses, educational institutions, and home users enjoy the benefits of using the Internet, they are often not adequately informed about the potential dangers that their computer systems face if left vulnerable and unprotected. The good news is there are solutions and remedies to help mitigate the threats; the bad news is awareness of these solutions and the practice of safe Internet use is not far reaching. Attacks are evolving at a greater speed than preparation.

This hearing will provide an opportunity to learn about the efforts of the Federal Government, trade associations, corporations, and nonprofits to raise awareness about the importance of cyber security. Today I want to call on all stakeholders to take immediate action. All of us have a role and a responsibility to implement basic

cyber security hygiene in order to reduce the potential vulnerabilities that could contribute to a successful cyber attack.

As use of the Internet all over the world grows, so do the presence and ambitions of people with criminal and malicious intent. Hackers attempt to take over people's computers to create ways to send spam, steal information, and launch attacks undetected. Criminals try to trick unsuspecting cyber citizens to reveal personal information by impersonating respectable Web sites, a crime known as "phishing." Consumers on the Internet may be tricked into downloading spyware. These programs may be harmless, yet extremely annoying, such as delivering a continuous stream of pop-up ads. Or they may be malicious, extracting information such as passwords and personal information for criminal purposes.

There are existing and emerging protections against these threats. Cyber citizens can arm themselves with virus protection software to help stop any potential impact of worms and viruses. Use of firewalls can help prevent some forms of spyware. Of course, after the rapid spread and dramatic impact of worms and viruses this past year, I think we all know the importance of keeping our systems patched and up to date. Security notices are everywhere reminding us not to open e-mail from people we do not know, and not to download programs from unknown sources.

However, many Internet users, consumers, nonprofits, educational institutions, and businesses do not employ these well-known protections. They are either unaware of the risks, or unaware of the solutions, or both.

User awareness is only part of the problem. Many of the security problems that users face are rooted in products that were designed to deliver functionality, often without adequate regard to security. The manufacturers of both software and hardware products must accept some responsibility in this area and respond to the growing demands of the consuming public for improved quality and security. This subcommittee has already held hearings on the proliferation of worms and viruses and on the issue of software assurance. And I will continue to pursue those issues. But I am heartened by what I see as signs that the manufacturers are stepping up to the plate. I see an increased attention to security that seems to go beyond merely lip service. Manufacturers of all levels of notoriety are publicly confirming their commitment to providing consumers with products that are less "buggy" and more secure.

In an effort to dramatically improve information security throughout corporate America, I convened a group of 25 leaders from business organizations, as well as representatives from academic and institutional communities to form the Corporate Information Security Working Group. The intent was to produce a set of recommendations that could form the basis of an action plan for improving cyber security for businesses and enterprises of all sizes and sectors. The group divided into subgroups, one of which was the Awareness, Education, and Training Subgroup. This subgroup's mission was to identify, partner with and build on the good work of organizations that have or are developing campaigns to raise awareness on the importance of cyber security. Let me pause and acknowledge the tremendous work that Commissioner Swindle and the FTC have been pursuing for some time now. It is my view that

our collective efforts can make a difference. The Awareness, Education, and Training Subgroup reported recommendations for three categories of users—small businesses, large enterprises, and home users.

For small businesses, the group suggested creating and distributing a Small Business Guidebook for Cyber Security that explains cyber security risks in terms that are readily understood and that motivate small business owners to take action.

For large enterprises, the Awareness, Education, and Training Subgroup suggested enhancing distribution of existing documents for large enterprise managers. Many organizations, including the Institute for Internal Auditors, the Internet Security Alliance, and the Business Software Alliance, have done great work in this regard. The group believes these documents deserve greater distribution and will work with organizations representing large corporations to find the proper channels for broader dissemination. Furthermore, for large enterprises, the group suggested creating a guide for information security for C-level executives, such as CEOs, CFOs, and COOs. A user-friendly guide for C-level executives is necessary to raise the profile of the information security issue in terms senior executives can understand. To that end, the group is currently working with representatives of large business organizations to see how it might collaborate on and distribute such a guide.

Finally, the group suggested targeted efforts aimed at the mass market would help educate home users. The group is seeking to buildupon existing relationships and forging new partnerships between organizations, corporations, and the government to help educate the home user base on cyber security.

One of the other subgroups worked diligently on developing a set of best practices and guiding principles in information security that could apply from the most unsophisticated home user to the most sophisticated enterprise. Those efforts have produced incredible results, and provided a foundation for the Awareness, Education, and Training Subgroup to buildupon.

In addition to my Corporate Information Security Work Group, there are several other organizations, including both public and private entities, that are working to improve awareness and provide education to cyber citizens. This includes a broad base of constituent groups, including the education community. Today we will hear about awareness and education efforts in the K through 12 community, as well as in institutions of higher education. In addition to these awareness and education efforts, I am pleased to announce at this hearing two partnerships that the Department of Homeland Security is undertaking to train information security and assurance professionals through our Nation's colleges and universities. The Department will be partnering with NSA to enhance the Centers of Academic Excellence in Information Assurance Education Program to increase the number of information security professionals entering the work force. The Department will also be partnering with the National Science Foundation on a Scholarship for Service Program, which provides 2-year scholarships for training information assurance specialists who in turn make a commitment to work for a Federal civilian agency for 2 years. I look for-

ward to hearing more about these various initiatives in the testimony today.

I will note that I do have a concern. I worry that if we bombard our cyber citizens with too many messages from too many sources, they may become confused and take no action at all. If we are to begin a national, intensive campaign to educate individuals, and small and medium businesses on cyber security, we need to have a collaborative strategy that facilitates the delivery of a clear and common message about how folks can protect against the threat of a cyber attack. I look forward to hearing from today's witnesses that my concern is being addressed in a proactive and collaborative manner.

We must maintain the advantages that multiple channels give us for outreach and we must continue to recognize that one size does not fit all and that a required level of cyber security hygiene will vary depending on the profile of the user. Some basic steps are invariably common to most users and today we will identify steps being taken to convey that information. The more voices repeating the message, the more people are likely to hear it and pay attention. It would be difficult in my estimation and based on what I have learned to overstate the importance and timeliness of such an effort.

I look forward to the testimony of our witnesses and I thank them for their contribution to the cyber security of our Nation.

Today's hearing can be viewed live via Web cast by going to reform.house.gov and clicking on the link under live committee broadcast.

[The prepared statement of Hon. Adam H. Putnam follows:]

TOM DAVIS, VIRGINIA
CHAIRMAN

DAN BURTON, INDIANA
CHRISTOPHER SHAYS, CONNECTICUT
ILEANA ROS-LEHTINEN, FLORIDA
JOHN M. McHUGH, NEW YORK
JOHN L. MICA, FLORIDA
MARK E. SOUDER, INDIANA
STEVEN C. LATOURETTE, OHIO
DOUG OSE, CALIFORNIA
RON LEWIS, KENTUCKY
JO ANN DAVIS, VIRGINIA
TODD RUSSELL PLATTS, PENNSYLVANIA
CHRIS CANNON, UTAH
ADAM H. PUTNAM, FLORIDA
EDWARD L. SCHROCK, VIRGINIA
JOHN J. DUNCAN, JR., TENNESSEE
NATHAN DEAL, GEORGIA
CANDICE MILLER, MICHIGAN
TIM MURPHY, PENNSYLVANIA
MICHAEL R. TURNER, OHIO
JOHN R. CARTER, TEXAS
MARSHA BLACKBURN, TENNESSEE
PATRICK J. TIBERI, OHIO
KATHERINE HARRIS, FLORIDA

ONE HUNDRED EIGHTH CONGRESS

Congress of the United States

House of Representatives

COMMITTEE ON GOVERNMENT REFORM

2157 RAYBURN HOUSE OFFICE BUILDING

WASHINGTON, DC 20515–6143

MAJORITY (202) 225–5074
FACSIMILE (202) 225–3974
MINORITY (202) 225–5051
TTY (202) 225–6852

www.house.gov/reform

HENRY A. WAXMAN, CALIFORNIA
RANKING MINORITY MEMBER

TOM LANTOS, CALIFORNIA
MAJOR R. OWENS, NEW YORK
EDOLPHUS TOWNS, NEW YORK
PAUL E. KANJORSKI, PENNSYLVANIA
CAROLYN B. MALONEY, NEW YORK
ELIJAH E. CUMMINGS, MARYLAND
DENNIS J. KUCINICH, OHIO
DANNY K. DAVIS, ILLINOIS
JOHN F. TIERNEY, MASSACHUSETTS
WM. LACY CLAY, MISSOURI
DIANE E. WATSON, CALIFORNIA
STEPHEN F. LYNCH, MASSACHUSETTS
CHRIS VAN HOLLEN, MARYLAND
LINDA T. SANCHEZ, CALIFORNIA
C.A. DUTCH RUPPERSBERGER, MARYLAND
ELEANOR HOLMES NORTON, DISTRICT OF COLUMBIA
JIM COOPER, TENNESSEE

BERNARD SANDERS, VERMONT, INDEPENDENT

"Protecting Our Nation's Cyber Space: Educational Awareness For the Cyber Citizen."

Wednesday, April 21, 2004
2:00 p.m.

Room 2154 Rayburn House Office Building

Opening Statement of Chairman Adam Putman (R-Fl)

I want to welcome you all today to this hearing on "Protecting Our Nation's Cyber Space: Educational Awareness for the Cyber Citizen." In the past few years, the growth in access and use of the Internet, the increase in high-speed connections that are always on, and the rapid development and deployment of new computing devices has resulted in an expanding global computing network. Although these advances have improved our quality of life, this global network is susceptible to viruses and worms that can circle the world in just minutes…not to mention the potential of more malicious cyber attacks. While businesses, educational institutions, and home users enjoy the benefits of using the Internet, they are not often adequately informed about the potential dangers that their computer systems face if left vulnerable and unprotected. The good news is there are solutions and remedies to help mitigate the threats; the bad news is awareness of these solutions and the practice of safe Internet use is not far reaching. Attacks are evolving at a greater speed than preparation. This hearing will provide an opportunity for us to learn about the efforts of the Federal government, trade associations, corporations, and non-profits to raise awareness about the importance of cyber security. Today I call on all stakeholders to take immediate action…all of us have a role and a responsibility…to implement basic cyber security hygiene in order to reduce the potential vulnerabilities that could contribute to a successful cyber attack.

As use of the Internet all over the world grows, so do the presence and ambitions of people with criminal and malicious intent. Hackers attempt to take over people's computers to create ways to send spam, steal information and launch attacks undetected.

Criminals try to trick unsuspecting cyber citizens to reveal personal information by impersonating respectable web sites, a crime known as "phishing." Consumers on the Internet may be tricked into downloading spyware. These programs may be harmless, yet extremely annoying, such as delivering a continuous stream of pop-up ads. Or they may be malicious, extracting information such as passwords and personal information for criminal purposes.

There are existing and emerging protections against these threats. Cyber citizens can arm themselves with virus protection software to help stop any potential impact of worms and viruses. Use of firewalls can help prevent some forms of spyware. Of course, after the rapid spread and dramatic impact of worms and viruses this past year, I think we all know the importance of keeping our systems patched and up to date. Security notices are everywhere reminding us not to open e-mail from people we don't know, and not to download programs from unknown sources.

However, many Internet users, consumers, non-profits, educational institutions and businesses, do not employ these well-known protections. They are either unaware of the risks, or unaware of the solutions, or both.

User awareness is only part of the problem though. Many of the security problems that users face are rooted in products that were designed to deliver functionality, often without adequate regard to security. The manufacturers of both software and hardware products must accept responsibility in this area, and respond to the growing demands of the consuming public for improved quality and security. This Subcommittee has already held hearings on the proliferation of worms and viruses and on the issue of software assurance. And I will continue to pursue those issues. However, I am heartened by what I see as signs that the manufacturers are stepping up to the plate. I see an increased attention to security that seems to go beyond merely lip service. Manufacturers of all levels of notoriety are publicly confirming their commitment to providing consumers with products that are less "buggy" and more secure.

In an effort to dramatically improve information security throughout corporate America, I convened a group of 25 leaders from business organizations, as well as representatives from academic and institutional communities, to form the Corporate Information Security Working Group. The intent was to produce a set of recommendations that could form the basis of an action plan for improving cyber security for businesses and enterprises of all sizes and sectors. The group divided into subgroups, one of which was the Awareness, Education, and Training Subgroup. This subgroup's mission was to identify, partner with and build on the good work of organizations that have or are developing campaigns that raise awareness on the importance of cyber security. Let me pause and acknowledge the tremendous work that Commissioner Swindle and the FTC have been pursuing for some time now. It is my view that our collective efforts CAN make a difference. The Awareness, Education, and Training Subgroup reported recommendations for three categories of users – small businesses, large enterprises, and home users.

For small businesses, the group suggested creating and distributing a Small Business Guidebook for Cyber Security that explains cyber security risks in terms that are readily understood and that motivates small business owners to take action.

For large enterprises, the Awareness, Education, and Training Subgroup suggested enhancing distribution of existing documents for large enterprise managers. Many organizations – including the Institute for Internal Auditors, the Internet Security Alliance, and the Business Software Alliance – have done good work in this regard. The group believes these documents deserve greater distribution, and will work with organizations representing large corporations to find the proper channels for broader dissemination. Furthermore for large enterprises, the group suggested creating a guide to information security for C-level executives, such as CEOs, CFOs, and COOs. A user-friendly guide for C-level executives is necessary to raise the profile of the information security issue in terms senior executives can understand. To that end, the group is currently working with representatives of large business organizations to see how it might collaborate on and distribute such a guide.

Finally, the group suggested targeted efforts aimed at the mass market would help to educate home users. The group is seeking to build upon existing relationships and to forge new partnerships between organizations, corporations, and the government that will help educate the home user base on cyber security.

One of the other Subgroups worked diligently on developing a set of best practices and guiding principles in information security that could apply from the most unsophisticated home user to the most sophisticated enterprise. Those efforts have produced incredible results, and provide a foundation for the Awareness, Education, and Training Subgroup to build upon.

In addition to my Corporate Information Security Working Group, there are several other organizations, including both public and private entities that are working to improve awareness and provide education to cyber citizens. This includes a broad base of constituent groups, including the education community. Today we will hear about awareness and education efforts in the K through 12 community, as well as in institutions of higher education. In addition to these awareness and education efforts, I am pleased to announce at this hearing two partnerships that the Department of Homeland Security is undertaking to train information security and assurance professionals through our Nation's colleges and universities. The Department will be partnering with NSA to enhance the Centers of Academic Excellence in Information Assurance Education Program to increase the number of information security professionals entering the work force. The Department will also be partnering with the National Science Foundation on its Scholarship for Service Program, which provides two-year scholarships for training information assurance specialists who in turn make a commitment to work for a Federal civilian agency for two years. I am looking forward to hearing more about these various initiatives in the testimony today.

I will note that I do have a concern. I worry that if we bombard our cyber citizens with too many messages from too many sources, they may become confused and take no action at all. If we are to begin a national, intensive campaign to educate individuals, and small and medium businesses on cyber security, I think we need to have a collaborative strategy that facilitates the delivery of a clear and common message about how folks can protect against the threat of a cyber attack. I look forward to hearing from today's witnesses that my concern is being addressed in a proactive and collaborative manner.

We must maintain the advantages that multiple channels give us for outreach and we must continue to recognize that one size does not fit all and that the required level of cyber security hygiene will vary depending on the profile of the user. Some basic steps are invariably common to most users and today we will identify steps being taken to convey that information. The more voices repeating the message, the more people are likely to hear it and pay attention. It would be difficult in my estimation and based on what I have learned to overstate the importance and timeliness of such an effort.

I look forward to the testimony from today's witnesses and I thank you for your contribution to the security of our Nation.

Mr. PUTNAM. I would like to welcome the gentleman from Missouri, our ranking member of the subcommittee, Mr. Clay, and recognize him for his opening remarks.

Mr. Clay.

Mr. CLAY. Thank you, Mr. Chairman, for holding today's hearing on ways we can improve our educational efforts in the realm of cyber security. I, too, share your concerns and I am hopeful that our witnesses can share with us different perspectives on effective methods for reaching our goals.

As our global economy becomes more dependent on the efficiencies associated with the information super-highway, we must become more aware of the risks and costs associated with such advanced technology. Although legislating appropriate standards in rapidly changing technologies is, at best, a reactive approach to policymaking, we may have few other viable options. The ominous threat of widespread and well-orchestrated cyber attack would have severe consequences in both real economic terms and consumer confidence. If efforts to legislate cyber security standards are to be effective, the prevention of such attacks through outreach, training, education, and awareness must be central to its mission.

Once again, I believe there are two central components that are integral to providing adequate computer security for the Federal Government. First, the management of our agencies' networks must become a top priority throughout the government. This approach should not only include adequate funding for computer security, but better stewardship of our critical assets and more frequent vulnerability assessments for our investments.

Second, the government must find a way to incorporate minimal software and hardware security standards into its annual $60 billion investment in information technology. We must harness the purchasing power of the Federal Government to demand more stringent computer security standards from vendors and contractors at every level of the procurement process.

I want to thank our chairman for his work on improving computer security standards through the Corporate Information Security Working Group. It is my hope that his collaborative efforts with the private sector can bring us closer to achieving what have been, to this point, elusive goals.

Mr. Chairman, this concludes my remarks, and I ask that they may be inserted into the record. Thank you.

[The prepared statement of Hon. Wm. Lacy Clay follows:]

STATEMENT OF THE HONORABLE WM. LACY CLAY
AT THE HEARING ON
Educational Awareness and Cyber Security

April 21, 2004

Thank you Mr. Chairman for holding today's hearing on ways we can improve our educational efforts in the realm of cyber security. I am hopeful that our witnesses can share with us different perspectives on effective methods to reach our goals.

As our nation and global economy becomes more dependent on the efficiencies associated with the information super-highway, we must become more aware of the risks and costs associated with such advanced technology. Although legislating appropriate standards in rapidly changing technologies is, at best, a reactive approach to policy making, we may have few other viable options. The ominous threat of a widespread and well-orchestrated cyber attack would have sever consequences in both real economic terms and consumer confidence.

If efforts to legislate cyber security standards are to be effective, the prevention of such attacks through outreach, training, education, and awareness must be central to its mission.

Once again, I believe there are two central components that are integral to providing adequate computer security for the federal government. First, the management of our agencies' networks must become a top priority throughout the

government. This approach should not only include adequate funding for computer security, but better stewardship of our critical assets and more frequent vulnerability assessments for our investments.

Second, the government must find a way to incorporate minimal software and hardware security standards into its annual $60 billion investment in information technology. We must harness the purchasing power of the federal government to demand more stringent computer security standards from vendors and contractors at every level of the procurement process.

I want to thank our Chairman for his work on improving computer security standards through the Corporate Information Security Working Group. It is my hope that his collaborative efforts with the private sector can bring us closer to achieving what have previously been elusive goals. Mr. Chairman, this concludes my remarks, and ask that they may be inserted into the record.

Mr. PUTNAM. Without objection, so ordered.

I will move directly into the oath. As is the custom with this committee, our witnesses are sworn in.

[Witnesses sworn.]

Mr. PUTNAM. Note for the record that both witnesses responded in the affirmative.

We will now move into the testimony. I would like to introduce our first witness, Orson Swindle. Mr. Swindle was sworn in as Commissioner for the Federal Trade Commission December 18, 1997. In December 2001, Commissioner Swindle was appointed as head of the U.S. delegation to the Organization for Economic Cooperation and Development Experts' Group to review the 1992 OECD guidelines for the security of information systems. He has a distinguished military career, and served in the Reagan administration from 1981 to 1989 directing financial assistance programs to economically distressed rural and municipal areas of the country. As Assistant Secretary of Commerce for Development, he managed the Department of Commerce's national economic development efforts, directing seven offices across the country. He was State Director of the Farmers Home Administration for the U.S. Department of Agriculture, financing rural housing, community infrastructure, businesses, and farming.

We welcome you to the subcommittee, and appreciate your work in this area. You are recognized for 5 minutes for your oral statement. Your written statements, for both witnesses, will be inserted into the record. You are recognized.

STATEMENTS OF ORSON SWINDLE, COMMISSIONER, FEDERAL TRADE COMMISSION; AND AMIT YORAN, DIRECTOR, NATIONAL CYBER SECURITY DIRECTORATE, DEPARTMENT OF HOMELAND SECURITY

Mr. SWINDLE. Mr. Chairman, Mr. Clay, and members of the subcommittee, I appreciate the opportunity to discuss the FTC's work on information security. The views expressed in the written statement represent the views of the Federal Trade Commission. My oral remarks and responses to questions, of course, are my own. This hearing is most timely and I applaud the chairman for his leadership on this very vital subject.

Today, maintaining the security of our information systems and networks is essential to every aspect of our lives. We are all directly or indirectly linked together by this infrastructure. We benefit enormously from these systems; however, there are vulnerabilities that threaten the security of and do major harm to stored information, the flow of information, and the continued viability of the systems themselves.

The FTC has sought to address these vulnerabilities through consumer and business education, stressing the fundamental importance of good security practices, plus law enforcement actions, and international cooperation. Safe computing practices by home computer users are especially important in our broadband world. Viruses, worms, and dial-up service attacks have left a trail of very costly destruction and, as the chairman mentioned, it could get worse. To help promote a culture of security, the FTC created an information security mascot, Dewie the e-Turtle, to educate busi-

nesses, consumers, and children about the importance of information security and the precautions they can take to protect personal information. The Dewie Web site has registered more than 600,000 visits since its deployment in August 2002. In addition the FTC had distributed a video news release seen by 1.5 million consumers; we have distributed 160,000 postcards featuring Dewie; and information security was the theme of National Consumer Protection Week in 2003.

Our Web site contains tips on how to stay safe on line as well as publications addressing issues related to spam, file sharing, high-speed Internet access, shopping on line, and identity theft. The growing problem of phishing is addressed. This is a high-tech scam that uses spam to deceive consumers into disclosing their credit card numbers, bank account information, Social Security numbers, passwords, and other sensitive personal information. This information and our Web sites are available to Members of Congress for constituent services. Despite our efforts, only about three dozen Members of the Congress have their Web sites linked to the FTC Web site. I think we can all do better than this.

The Internet has made us a global community and international collaboration is important to ensuring information security. The FTC has played a leading role within the OECD in revising and implementing its security guidelines, urging a widely publicized OECD Web site, and aggressively urging member countries to immediately implement the principles of information security. We are encouraging our global partners to share their experiences with the international community, including the APEC, the United Nations, and the TransAtlantic Business and Consumer Dialogues.

The FTC, the Department of Homeland Security, and such organizations as the newly formed National Cyber Security Partnership of trade associations, which includes the Chamber of Commerce, ITAA, TechNet, and BSA, are working individually and together to enhance consumer and business education. The National Cyber Security Summit met in December 2003 to implement the National Strategy to Secure Cyber Space and formed five task forces, including one devoted to comprehensive awareness. I am pleased that Dan Caprio of my staff participated as co-chairman of the awareness task force. That task force issued a report recommending a number of very concrete proposals to increase consumer awareness, including a comprehensive cyber awareness campaign to reach consumers through a 3-year national advertising campaign; a partnership with ISPs to educate home users about cyber security issues; and distribution of a cyber security tool kit through Stay Safe On Line.

The FTC remains committed to expanding our public-private partnership and leveraging relationships with consumer groups, industry, trade associations, other government agencies, and educators to raise consumer awareness. The Commission has used its law enforcement authority to address information security issues using our authority under Section 5 of the Federal Trade Commission Act. To date, the Commission's security cases have been based on deception. In four separate settlements with companies that collected personal information from consumers, including a settlement with Tower Records which was announced today, we have alleged

that the companies made explicit or implicit promises to take appropriate steps to protect consumers' information. In fact, we found their security measures to be inadequate. We alleged that Tower made specific promises to protect personal information provided by consumers on its Web site, yet failed to take reasonable and appropriate steps to detect and prevent against well-known vulnerabilities. The lesson: When you are making changes, do not forget to ensure that your security safeguards are in place.

Through these information security enforcement actions, the Commission has come to recognize several principles that govern any information security program. First, a company's security procedures must be appropriate for the kind of information it collects and maintains. Second, not all breaches of information security are violations of the Federal Trade Commission law. Third, there can be law violations without a known breach in security. And fourth, good security is an ongoing process of assessing and addressing risk and vulnerabilities.

The critical reality in our information-based economy is that we all have a role to play in protecting cyber space. Creating a culture of security is a journey, it is not a destination, and leadership will be essential. Thank you for this opportunity to appear here today, and I look forward to answering your questions.

[The prepared statement of Mr. Swindle follows:]

PREPARED STATEMENT OF THE
FEDERAL TRADE COMMISSION

before the

SUBCOMMITTEE ON TECHNOLOGY, INFORMATION POLICY, INTERGOVERNMENTAL RELATIONS, AND THE CENSUS

COMMITTEE ON GOVERNMENT REFORM

U.S. HOUSE OF REPRESENTATIVES

on

PROTECTING OUR NATION'S CYBERSPACE

April 21, 2004

I. Introduction

Mr. Chairman, and members of the subcommittee, I am Commissioner Orson Swindle.[1] I appreciate the opportunity to appear before you today to discuss the Commission's role in protecting information security and its importance to both consumers and businesses.

Today, maintaining the security of our computer-driven information systems is essential to every aspect of our lives. A secure information infrastructure is required for the operation of everything from our traffic lights to our credit and financial systems, including our nuclear and electrical power supplies and our emergency medical service. We are all, therefore, directly or indirectly linked together by this infrastructure. Consumers rely on and use computers at work and at home; increasingly, more consumers are making purchases over the Internet and paying bills and banking online.

These interconnected information systems provide enormous benefits to consumers, businesses, and government alike. At the same time, however, these systems can create serious vulnerabilities that threaten the security of the information stored and maintained in these systems as well as the continued viability of the systems themselves. Every day, security breaches cause real and tangible harms to businesses, other institutions, and consumers.[2] These breaches and the harm they do shake consumer confidence in the companies and systems to which they have entrusted their personal information.

II. The Federal Trade Commission's Role

The Federal Trade Commission has a broad mandate to protect consumers and the Commission's approach to information security is similar to the approaches taken in our other consumer protection efforts. As such, the Commission has sought to address concerns about the security of our nation's computer systems through a combined approach that stresses the education of businesses, consumers, and government agencies about the fundamental importance of good security practices; law enforcement actions; and international cooperation. In the information security matters, our enforcement tools derive from Section 5 of the FTC Act,[3] which prohibits unfair or deception acts or practices, and the Commission's Gramm-Leach-Bliley Safeguards Rule ("Safeguards Rule" or "Rule").[4] Our educational efforts include business education to promote compliance with the law, consumer and business education to help promote a "Culture of Security," public workshops to highlight emerging issues, and outreach to political leaders. In addition, in our increasingly global economy, international collaboration is fundamental to ensuring the security of consumers' information.

A. Section 5

The basic consumer protection statute enforced by the Commission is Section 5 of the FTC Act, which provides that "unfair or deceptive acts or practices in or affecting commerce are declared unlawful."[5] The statute defines "unfair" practices as those that "cause[] or [are] likely to cause substantial injury to consumers which is not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition."[6] To date, the Commission's security cases have been based on deception,[7] which the Commission and the courts have defined as a material representation or omission that is likely to mislead consumers acting reasonably under

the circumstances.[8]

The companies that have been subject to enforcement actions have made explicit or implicit promises that they would take appropriate steps to protect sensitive information obtained from consumers. Their security measures, however, proved to be inadequate; their promises, therefore, deceptive.

Through the information security enforcement actions, the Commission has come to recognize several principles that govern any information security program.

1. Security procedures should be appropriate under the circumstances

First, a company's security procedures must be appropriate for the kind of information it collects and maintains. Different levels of sensitivity may dictate different types of security measures. It is highly problematic when a company inadvertently releases sensitive personal information due to inadequate security procedures.

The Commission's first information security case, Eli Lilly,[9] involved an alleged inadvertent disclosure of sensitive information despite the company's promises to maintain the security of that information. Specifically, Lilly put consumers' e-mail addresses in the "To" line of the e-mail that was sent to Prozac users who subscribed to a service on Lilly's website, essentially disclosing the identities of all of the Prozac user-subscribers.

Given the sensitivity of the information involved, this disclosure was a serious breach. Nevertheless, the Commission recognized that there is no such thing as "perfect" security and that breaches can occur even when a company has taken all reasonable precautions. Therefore, the Commission construed statements in Lilly's privacy policy as a promise to take steps "appropriate under the circumstances" to protect personal information. Similarly, the complaint alleged that the

breach resulted from Lilly's "failure to maintain or implement internal measures appropriate under the circumstances to protect sensitive consumer information."[10] The focus was on the reasonableness of the company's efforts.

According to the complaint in the Lilly matter, the company failed, among other things, to provide appropriate training and oversight for the employee who sent the e-mail and to implement appropriate checks on the process of using sensitive customer data. The order contains strong relief that should provide significant protections for consumers, as well as "instructions" to companies. First, it prohibits the misrepresentations about the use of, and protection for, personal information. Second, it requires Lilly to implement a comprehensive information security program similar to the program required under the FTC's Gramm-Leach-Bliley Safeguards Rule, which is discussed below. Finally, to provide additional assurances that the information security program complies with the consent order, every year the company must have its program reviewed by a qualified person to ensure compliance.

2. Not All Security Breaches Are Violations of FTC Law

The second principle that arises from the Commission's enforcement in the information security area is that not all breaches of information security are violations of FTC law – the Commission is not simply saying "gotcha" for security breaches. Although a breach may indicate a problem with a company's security, breaches can happen, as noted above, even when a company has taken every reasonable precaution. In such instances, the breach will not violate the laws that the FTC enforces. Instead, the Commission recognizes that security is an ongoing process of using reasonable and appropriate measures in light of the circumstances.

When breaches occur, our staff reviews available information to determine whether the

incident warrants further examination. If it does, the staff gathers information to enable us to assess the reasonableness of the company's procedures in light of the circumstances surrounding the breach. This allows the Commission to determine whether the breach resulted from the failure to have procedures in place that are reasonable in light of the sensitivity of the information. In many instances, we have concluded that FTC action is not warranted. When we find a failure to implement reasonable procedures, however, we act.

3. Law Violations Without a Known Breach of Security

The Commission's case against Microsoft[11] illustrates a third principle – that there can be law violations without a known breach of security. Because appropriate information security practices are necessary to protect consumers' privacy, companies cannot simply wait for a breach to occur before they take action. Particularly when explicit promises are made, companies have a legal obligation to take reasonable steps to guard against reasonably anticipated vulnerabilities.

Like Eli Lilly, Microsoft promised consumers that it would keep their information secure. Unlike Lilly, there was no specific security breach that triggered action by the Commission.[12] The Commission's complaint alleged that there were significant security problems that, left uncorrected, could jeopardize the privacy of millions of consumers. In particular, the complaint alleged that Microsoft did not employ "sufficient measures reasonable and appropriate under the circumstances to maintain and protect the privacy and confidentiality of personal information obtained through Passport and Passport Wallet."[13] The complaint further alleged that Microsoft failed to have systems in place to prevent unauthorized access; detect unauthorized access; monitor for potential vulnerabilities; and record and retain systems information sufficient to perform security audits and investigations. Again, sensitive information was at issue – financial information including credit

card numbers.

Like the Commission's order against Eli Lilly, the Microsoft order prohibits any misrepresentations about the use of, and protection for, personal information and requires Microsoft to implement a comprehensive information security program. In addition, Microsoft must have an independent professional certify, every two years, that the company's information security program meets or exceeds the standards in the order and is operating effectively.

4. Good Security is an Ongoing Process of Assessing Risks and Vulnerabilities

The Commission's third case, against Guess, Inc.,[14] highlighted a fourth principle – that good security is an ongoing process of assessing and addressing risks and vulnerabilities. The risks companies and consumers confront change over time. Hackers and thieves will adapt to whatever measures are in place, and new technologies likely will have new vulnerabilities waiting to be discovered. As a result, companies need to assess the risks they face on an ongoing basis and make adjustments to reduce these risks.

The Guess case highlighted this crucial aspect of information security in the context of web-based applications and the databases associated with them. Databases frequently house sensitive data such as credit card numbers, and Web-based applications are often the "front door" to these databases. It is critical that online companies take reasonable steps to secure these aspects of their systems, especially when they have made promises about the security they provide for consumer information.

In Guess, the Commission alleged that the company broke such a promise concerning sensitive information collected through its website, www.guess.com. According to the Commission's complaint, by conducting a "web-based application" attack on the Guess website, an

attacker gained access to a database containing 191,000 credit card numbers. This particular type of attack was well known in the industry and appeared on a variety of lists of known vulnerabilities. The complaint alleged that, despite specific claims that it provided security for the information collected from consumers through its website, Guess did not: employ commonly known, relatively low-cost methods to block web-application attacks; adopt policies and procedures to identify these and other vulnerabilities; or test its website and databases for known application vulnerabilities, which would have disclosed that the website and associated databases were at risk of attack. Essentially, the Commission alleged that the company had no system in place to test for known application vulnerabilities or to detect or to block attacks once they occurred.

In addition, the complaint alleged that Guess misrepresented that the personal information it obtained from consumers through www.guess.com was stored in an unreadable, encrypted format at all times; but, in fact, after launching the attack, the attacker could read the personal information, including credit card numbers, stored on www.guess.com in clear, unencrypted text.

As in its prior security cases, the Commission's emphasis in Guess was on reasonableness. When the information is sensitive, the vulnerabilities well known, and the fixes inexpensive and relatively easy to implement, it is unreasonable simply to ignore the problem. As in the prior orders, the Commission's order against Guess prohibits the misrepresentations, requires Guess to implement a comprehensive information security program, and, like Microsoft, requires an independent audit every two years.

B. GLB Safeguards Rule

In addition to our enforcement authority under Section 5 of the FTC Act, the Commission also has responsibility for enforcing its Gramm-Leach-Bliley Safeguards Rule, which requires

financial institutions under the FTC's jurisdiction to develop and implement appropriate physical, technical, and procedural safeguards to protect customer information.[15] The Safeguards Rule is an important enforcement and guidance tool to ensure greater security for consumers' sensitive financial information. It requires a wide variety of financial institutions to implement comprehensive protections for customer information - many of them for the first time. If fully implemented by companies, as required, the Rule could go a long way to reduce risks to this information, including identity theft.

The Safeguards Rule requires financial institutions to develop a written information security plan that describes their program to protect customer information. Due to the wide variety of entities covered, the Rule requires a plan that accounts for each entity's particular circumstances - its size and complexity, the nature and scope of its activities, and the sensitivity of the customer information it handles.

As part of its plan, each financial institution must: (1) designate one or more employees to coordinate the safeguards; (2) identify and assess the risks to customer information in each relevant area of the company's operation, and evaluate the effectiveness of the current safeguards for controlling these risks; (3) design and implement a safeguards program, and regularly monitor and test it; (4) hire appropriate service providers and contract with them to implement safeguards; and (5) evaluate and adjust the program in light of relevant circumstances, including changes in the firm's business arrangements or operations, or the results of testing and monitoring of safeguards. The Safeguards Rule requires businesses to consider all areas of their operation, but identifies three areas that are particularly important to information security: employee management and training; information systems; and management of system failures.

Prior to the Rule's effective date, the Commission issued guidance to businesses covered by the Safeguards Rule to help them understand the Rule's requirements.[16] Commission staff also met, and continues to meet, with a variety of trade associations and companies to alert them to the Rule's requirements and to gain a better understanding of how the Rule is affecting particular industry segments. Since the Rule's effective date, the Commission has continued these efforts and has also conducted investigations of compliance by covered entities.

C. Education and workshops

In addition to our law enforcement efforts and conducting outreach under the Commission's Safeguards Rule, the Commission has engaged in a broad outreach campaign to educate businesses and consumers about the importance of information security and the precautions they can take to protect or minimize risks to personal information. These efforts have included creation of an information security "mascot," Dewie the e-Turtle, who hosts a portion of the FTC website devoted to educating businesses and consumers about security,[17] publication of business guidance regarding common vulnerabilities in computer systems[18] and responding to information compromises,[19] speeches by Commissioners and staff about the importance of this issue, and outreach to the international community. Many offices in the Commission, including the Commission's Bureau of Consumer Protection, the Office of Public Affairs, and the Office of Congressional Relations, have participated in this effort to educate consumers and businesses.

The Commission's information security website[20] has registered more than 600,000 visits since its deployment in August 2002, making it one of the most popular FTC web pages. The site has been made available in CD-ROM and exists in PDF format. The site itself is frequently updated

with new information for consumers on cybersecurity issues. Further, the Commission's Office of Consumer and Business Education has produced a video news release, which has been seen by an estimated 1.5 million consumers; distributed 160,000 postcards featuring Dewie and his information security message to approximately 400 college campuses nationwide; and coordinated the 2003 National Consumer Protection Week with a consortium of public- and private-sector organizations around the theme of information security. The Commission's Office of Congressional Relations has also conducted outreach through constituent service representatives in each of the 535 House and Senate member offices by providing "Safe Computing" CDs to encourage incorporation of safe computing information into mailings, newsletter articles, and other communication channels. More than 40 members now host links to FTC online resources, with many devoting entire sections of their websites to consumer protection, including identity theft and information security. In the past two years, the FTC staff have partiticpated in more than 20 town-hall meetings about consumer protection and information security issues. The agency also has participated in consumer education events on Capitol Hill, including joining the Congressional Internet Caucus Advisory Committee on a series of workshops related to information security.

The Commission also uses opportunities that arise in non-security cases (brought under both deception and unfairness theories) to educate the public about security issues. For example, when the Commission filed a case challenging a scam that bombarded consumers' computers with repeated Windows Messenger Service pop-up ads,[21] we also issued a consumer alert providing instructions on how to disable the Windows Messenger Service in order to avoid other pop-up spam. The alert[22] also discusses the use of firewalls to block hackers from accessing consumers' computers.

The Commission has also issued a number of alerts to consumers about "phishing."[23]

Phishing is a high-tech scam that uses spam to deceive consumers into disclosing their credit card numbers, bank account information, Social Security numbers, passwords, and other sensitive personal information. These spam messages often pretend to be from businesses with whom the potential victims deal - for example, their Internet service provider, online payment service, or bank. The fraudsters tell recipients that they need to "update" or "validate" their billing information to keep their accounts active, and then direct them to a "look-alike" Web site of the legitimate business, further tricking consumers into thinking they are responding to a bona fide request. Unknowingly, consumers submit their financial information - not to the businesses - but to the scammers, who use it to order goods and services and obtain credit.

Finally, the Commission continues, and will continue, to host workshops on information security issues when appropriate. Last summer, the Commission hosted two workshops focusing on the role technology plays in protecting personal information.[24] The first workshop focused on the technologies available to consumers to protect themselves. Panelists generally agreed that to succeed in the marketplace, these technologies must be easy to use and must be built into the basic hardware and software consumers purchase.

The second workshop focused on the technologies available to businesses. We learned that businesses, like consumers, need technology that is easy to use and compatible with their other systems. Unfortunately, we also heard that too many technologies are sold before undergoing adequate testing and quality control, frustrating progress in this area.

The Commission also held a workshop in 2003 on unsolicited commercial e-mail ("spam") which was instructive about the security risks that spam poses. We learned that, in addition to other

problems, spam can also serve as a vehicle for malicious and damaging code.

Further, just this week, the Commission hosted a workshop to explore issues associated with "spyware" – software that is loaded on personal computers without users' consent.[25] Among the issues discussed were the privacy and security concerns raised by such software programs and the steps that consumers can take to protect themselves. The workshop consisted of six panels. The first three panels dealt with defining and understanding spyware, security risks, and potential privacy risks with such software. The last three panels addressed possible responses from a variety of constituencies. For example, one panel moderated by Commissioner Mozelle Thompson examined efforts by industry to develop responses to the problems associated with spyware. Other panels dealt with potential technological and governmental responses to the issue.

D. International Efforts

In addition to our cases and domestic efforts, the Commission has taken an active international role in promoting cybersecurity. We recognize that American society and societies around the world need to think about security in a new way. The Internet and associated technology have literally made us a global community. We are joining with our neighbors in the global community in this enormous effort to educate and establish a culture of security.

During the summer of 2002, the Organization for Economic Cooperation and Development ("OECD") issued a set of voluntary principles for establishing a culture of security – principles that can assist us all in minimizing vulnerabilities. Commissioner Swindle has had the opportunity to work with this organization and to head the U.S. Delegation to the Experts Group on the post-September 11 review of existing OECD Security Guidelines and to the Working Party on

Information Security and Privacy.

The OECD principles are contained in a document entitled "Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security."[26] The nine principles are an excellent, common-sense starting point for formulating a workable approach to security. They address awareness, accountability, and action. They also reflect the principles that guide the FTC in its analysis of security-related cases, recognizing that security architecture and procedures should be appropriate for the kind of information collected and maintained and that good security is an ongoing process of assessing and addressing risks and vulnerabilities. These principles can be incorporated at all levels of use among consumers, government policy makers, and industry. The OECD Guidelines already have been the model for more sector-specific guidance by industry groups and associations.

Through the efforts discussed above, the FTC has played a leading role in implementing the OECD Security Guidelines. The FTC also participated in the October 2003 OECD Global Forum on Information Systems and Networks in Oslo, Norway, which began the actual implementation process. In addition, the OECD has launched a website, www.oecd.org/sti/cultureofsecurity, dedicated to the global dissemination of information about the OECD Security Guidelines, and the FTC has played a prominent role in the development and promotion of the site.

Besides the OECD, the Commission also is involved in information privacy and cybersecurity work undertaken by the Asian Pacific Economic Cooperation ("APEC") forum. APEC's Council of Ministers endorsed the OECD Security Guidelines in 2002. Promoting information system and network security is one of its chief priorities. The APEC Electronic

Commerce Steering Group ("ECSG") promotes awareness and responsibility for cybersecurity among small and medium-sized businesses that interact with consumers. Commission staff participated in APEC workshop and business education efforts this past year and is actively engaged in this work for the foreseeable future.

Along with the OECD and APEC, in December 2002, the United Nations General Assembly unanimously adopted a resolution calling for the creation of a global culture of cybersecurity. Other UN groups, international organizations, and bilateral groups with whom the Commission has dialogues, including the TransAtlantic Business and Consumer Dialogues, the Global Business Dialogue on Electronic Commerce, and bilateral governmental partners in Asia and in the EU also are working on cybersecurity initiatives.

Finally, in January of this year, the FTC partnered with 36 agencies from 26 countries around the world to launch "Operation Secure Your Server," an international effort to reduce the flow of unsolicited commercial e-mail by urging organizations to close "open relays" and "open proxies."[27] As part of the initiative, the participating agencies identified tens of thousands of owners or operators of potentially open relay or open proxy servers around the world. The agencies sent letters urging these owners or operators to protect themselves from becoming unwitting sources of spam and providing guidance on inexpensive steps to take to secure their servers.[28]

E. Partnerships

The FTC, the Department of Homeland Security (DHS), and such organizations as the National Cyber Security Partnership and the National Cyber Security Alliance Stay Safe Online program, are all working to enhance consumer and business education.[29] The National Cyber

Security Partnership created five task forces to examine home user awareness, corporate governance, cyber security early warning, software development, technical standards, and common criteria. Last month, the awareness task force issued a report recommending a number of concrete proposals to increase consumer awareness. The recommendations included: a comprehensive cyber security awareness campaign to reach consumers through a three-year national advertising campaign based on the Stay Safe Online "Top 10" cybersecurity tips; a partnership with the United States Internet Service Providers Association (USISPA) to educate home users about cyber security issues; and distribution of a Cyber Security Tool Kit to provide home users with easy-to-follow instructions on implementing the "Top 10" cyber tips.

Notwithstanding these efforts, developing a "Culture of Security" is a daunting challenge. The FTC, DHS, the Departments of Commerce, Justice, and State, and other government agencies have a role to play, but the government cannot do this alone, nor should it try. The Commission is working with consumer groups, business, trade associations, and educators to instill this new way of thinking. We are encouraging our global partners to do the same and to share what is learned.

III. Conclusion

The Commission, through law enforcement and consumer and business education, is committed to reducing the harm that occurs through information security breaches. Maintaining good security practices is a critical step in preventing these breaches and the resulting harms, which can range from major nuisance to major destruction. It is important to recognize one critical aspect of the global information-based economy: we are all in this together – government, private industry, and consumers -- and we must all take appropriate steps to create a culture of security.

ENDNOTES

1. The views expressed in this statement represent the views of the Commission. My oral presentation and responses to questions are my own and do not necessarily represent the views of the Commission or any other Commissioner.

2. For example, our recently released Identity Theft Report, available at http://www.ftc.gov/os/2003/09/synovatereport.pdf, showed that over 27 million individuals have been victims of identity theft, which may have occurred either offline or online, in the last five years, including almost 10 million individuals in the last year alone. The survey also showed that the average loss to businesses was $4800 per victim. Although various laws limit consumers' liability for identity theft, their average loss was still $500 – and much higher in certain circumstances.

3. 15 U.S.C. § 45.

4. 16 C.F.R. Part 314, available online at http://www.ftc.gov/os/2002/05/67fr36585.pdf.

5. 15 U.S.C. § 45 (a) (1).

6. 15 U.S.C. § 45(n).

7. Where appropriate, the Commission has also alleged unfairness in its Internet cases. *See FTC v. Zachary Keith Hill*, Civ. No. H 03-5537 (filed S.D. Tex. December 3, 2003), http://www.ftc.gov/opa/2004/03/phishinghilljoint.htm; *FTC v. C.J.*, Civ. No. 03-CV-5275-GHK (RZX) (filed C.D. Cal. July 24, 2003), http://www.ftc.gov/os/2003/07/phishingcomp.pdf.

8. Letter from FTC to Hon. John D. Dingell, Chairman, Subcommittee on Oversight and Investigations (Oct. 14, 1983), *reprinted* in appendix to *Cliffdale Associates, Inc.*, 103 F.T.C. 110, 174 (1984) (setting forth the commission's Deception Policy Statement.).

9. The Commission's final decision and order against Eli Lilly is available at www.ftc.gov/os/2002/05/elililldo.htm. The complaint is available at www.ftc.gov/os/2002/05/elililldcmp.htm.

10. *Eli Lilly Complaint*, paragraph 7.

11. The Commission's final decision and order against Microsoft is available at http://www.ftc.gov/os/2002/12/microsoftdecision.pdf. The complaint is available at http://www.ftc.gov/os/2002/12/microsoftcomplaint.pdf.

12. The Commission initiated its investigation of Microsoft's Passport services following a complaint from a coalition of consumer groups led by the Electronic Privacy Information Center.

13. *Microsoft Complaint*, paragraph 7.

14. The Commission's final decision and order against Guess, Inc. is available at http://www.ftc.gov/os/2003/06/guessagree.htm. The complaint is available at http://www.ftc.gov/os/2003/06/guesscmp.htm.

15. 16 C.F.R. Part 314, available online at http://www.ftc.gov/os/2002/05/67fr36585.pdf.

16. Financial Institutions and Customer Data: *Complying with the Safeguards Rule,* available at http://www.ftc.gove/bcp/conline/pubs/buspubs/safeguards.htm.

17. *See* http://www.ftc.gov/bcp/conline/edcams/infosecurity/index.html.

18. *See* http://www.ftc.gov/bcp/conline/pubs/buspubs/security.htm.

19. *See* http://www.ftc.gov/bcp/conline/pubs/buspubs/idtbizkit.htm.

20. *See* http://www.ftc.gov/infosecurity.

21. *See FTC v. D Squared Solutions*, Civ. No. AMD 03 CV3108 (filed N.D. Md. Nov. 6, 2003). Pleadings are available at http://www.ftc.gov/os/caselist/0323223.htm.

22. The alert can be found at http://www.ftc.gov/bcp/conline/pubs/alerts/popalrt.html.

23. *See*, e.g., http://www.ftc.gov/bcp/conline/pubs/alerts/phishregsalrt.htm. The Commission has also brought enforcement actions challenging unfair and deceptive practices in connection with "phishing." *See* cases cited *supra* note 7.

24. Additional information about the workshops are available at http://www.ftc.gov/bcp/workshops/technology/indes.html.

25. *See* http://www.ftc.gov/bcp/workshops/spyware/index.htm.

26. *See* http://www.oecd.org/dataoecd/16/22/15582260.pdf.

27. *See* http://www.ftc.gov/secureyourserver.

28. A sample letter is available at http://www.ftc.gov/bcp/conline/edcams/spam/secureyourserver/letter_english.htm.

29. The National Cyber Security Partnership is an industry-led group of interested security experts from the public and private sectors and trade associations, including the U.S. Chamber of Commerce, the Information Technology Association of America, TechNet, and the Business Software Alliance. The partnership was created as part of the December 2003 National Cyber Security Summit held in Santa Clara, California.

Mr. PUTNAM. Thank you very much Commissioner.

Our next witness is Amit Yoran. Mr. Yoran is the Director of the National Cyber Security Division of the Department of Homeland Security. The National Cyber Security Division provides for 24–7 functions, including conducting cyber space analysis, issuing alerts and warnings, improving information sharing, responding to major incidents, and aiding in national level recovery efforts. Most recently Mr. Yoran served as the vice president of worldwide managed security services at the Symantec Corp., overseeing 24–7 security operation centers delivering security services to hundreds of companies in over 40 countries around the world. Prior to working at Symantec, Mr. Yoran founded RipTech, an information security company. He also served as an officer in the U.S. military as the vulnerability assessment program director for the U.S. Department of Defense's computer emergency response team, and supported security efforts for the Office of the Assistant Secretary of Defense.

We welcome you to the subcommittee. You are recognized for 5 minutes.

Mr. YORAN. Good afternoon, Chairman Putnam and distinguished members of the subcommittee. My name is Amit Yoran, and I am Director of the National Cyber Security Division within the Office of Infrastructure Protection of the Homeland Security's Information Analysis and Infrastructure Protection Directorate. I am pleased to appear before you today to discuss our initiatives addressing educational awareness for the cyber citizen. We view cyber awareness as a critical component within our mandate to improve cyber security. We have implemented measures to reach as many people as quickly as possible. Education and training are also critical elements of our strategic initiatives to improve the long term cyber security posture of our Nation. Education of our cyber community on the rules of the road is fundamental for enhancing citizen safety in the cyber world.

The National Cyber Security Division was created to serve as the national focal point for public and private sectors to address cyber security issues. NCSD is charged with coordinating the implementation of the National Strategy to Secure Cyber Space. The Department works closely with our partners in the Federal Government, at the State and local level, as well as with the private sector and academia on a variety of programs and initiatives to protect our information infrastructure.

On January 28th of this year, the Department of Homeland Security unveiled the National Cyber Alert System, delivering targeted, timely, and actionable information to Americans to secure their computer systems. We have already issued several alerts and a periodic series of best practices and how-to guidance pieces. We strive to make the information provided understandable to all computer users, both the highly technical and those like my wife, who, despite her advanced degrees and profession, need this information presented in plain English. I am pleased to report that Americans are exhibiting a keen interest in the alert system. And on the day of the National Cyber Alert System launch we had over 1 million hits to the US-CERT Web site. Today, more than 250,000 direct subscribers are receiving National Cyber Alerts to enhance their cyber security. For your reference and for your constituents, I urge

you to visit www.us-cert.gov and to encourage you to include a link to US-CERT on your congressional Web page and recommend your constituents sign up for the National Cyber Alert System to help them improve their cyber vigilance and protect our Nation.

We have engaged in many media interactions to provide a voice of reason in our efforts to improve awareness among the cyber citizenry and also reach as many Americans as possible in the plain language they can easily understand and act upon. The Department of Homeland Security is the sponsor of the National Cyber Security Alliance and the Stay Safe On Line, a public-private effort created to educate home users and small businesses on cyber security best practices. Each time we turn our clocks ahead and back to account for Daylight Savings Time we encourage Americans to review and improve their cyber readiness. I challenge each Member of Congress to sponsor a cyber security awareness event in your district on October 31, the next National Cyber Security Day. Although Cyber Security Day is not yet broadly recognized, our continued and joint efforts will ensure their future success and effectiveness.

In addition to awareness, other key aspects of our strategy are focused on training and education. Homeland Security is actively engaged with our intergovernmental partners and is also reaching out to academic institutions to establish cooperative relationships. I again cite the two recent accomplishments which you previously mentioned in this regard.

We have signed on to partner with the National Security Agency to expand the NSA Center for Academic Excellence in Information Assurance Education Program to a broader National Centers of Academic Excellence initiative. The program was established by the NSA in 1998 to promote higher education in information assurance. Universities designated as centers are eligible for scholarships and grants through both the Federal and Department of Defense Information Assurance Scholarship programs. The new, increased scope will accelerate and expand the current program to attain national prominence, attract participation from other universities, resulting in an increased number of cyber security professionals for our Nation.

Second, Homeland Security has partnered with the National Science Foundation on the Scholarship for Service program. This initiative promotes university level information assurance education and places program graduates into the Federal work force. The Department of Homeland Security has already hired graduates and we are excited about the capability of these graduates and the quality of the work force this program is producing.

In addition to these accomplishments, we have identified other strategic education programs. We are working with the Department of Education, EDUCAUSE, and others to develop cyber security programs for the K through 12 curriculum in our public schools. It is imperative that we educate and raise America's youth in a culture which fosters prudent cyber security practices and ethics. Our goal is to ensure that all computer users understand the rules of the road for cyber security and are empowered to stay safe on line.

Thank you for opportunity to testify before you today. I would be pleased to answer any questions that you have at this time.

[The prepared statement of Mr. Yoran follows:]

Statement by
Amit Yoran
Director, National Cyber Security Division, Office of Infrastructure Protection
U.S. Department of Homeland Security

Before the Subcommittee on Technology
Committee on Government Reform
U.S. House of Representatives
April 21, 2004

Good morning, Chairman Putnam and distinguished Members of the Subcommittee. My name is Amit Yoran, and I am Director of the National Cyber Security Division the Office of Infrastructure Protection in the Department of Homeland Security's (DHS) Information Analysis and Infrastructure Protection Directorate. I am pleased to appear before you today to discuss DHS' initiatives addressing educational awareness for the cyber citizen focused on protecting our nation's cyberspace. We view awareness as a critical component to our mandate for increasing cyber security and have implemented programs to reach as many people as quickly and effectively as possible. Education and training are critical elements of our strategic initiatives that seek to improve our cyber security posture over the long term and for increasing safety in the cyber world.

Introduction

February 23rd marked the one-year anniversary of the Department of Homeland Security. In his remarks commemorating that day, Secretary Ridge stressed that one of the Department's goals is to strengthen our information sharing capability with respect to securing the nation's critical infrastructure over the next year. We in the Information Analysis and Infrastructure Protection Directorate (IAIP) take that mandate to heart in our collective efforts and activities to protect the Nation. Established by the Homeland Security Act, the IAIP Directorate is the focal point for the Nation to protect our critical infrastructures from attack or disruption. We have made significant strides toward this objective under the leadership of Under Secretary Frank Libutti.

The IAIP Directorate includes the Office of Information Analysis, the primary threat information intelligence gathering and analysis capability of DHS, and the Office of Infrastructure Protection. In today's highly technical and digital world, we recognize that attacks against the nation may manifest themselves in both physical and cyber forms. The interconnected and interdependent nature of our critical infrastructure makes our physical and cyber assets impossible to separate, and it would be irresponsible to address them in isolation. The placement of these two offices within the Directorate underscores this linkage and enables us to work together to share intelligence and other information and coordinate our efforts to mitigate our nation's vulnerabilities. This is why IAIP takes a holistic view of critical infrastructure vulnerabilities and works to protect the nation

from all threats by ensuring the integration of physical and cyber security approaches in the Directorate's Office of Infrastructure Protection.

In support of the broader IAIP mission, the National Cyber Security Division (NCSD) was created in June 2003 to serve as a national focal point for the public and private sectors to address cyber security issues. NCSD is charged with coordinating the implementation of the *National Strategy to Secure Cyberspace* released by the President in February 2003.

Under that mandate, DHS works closely with our partners in the federal government, the private sector, and academia on a variety of programs and initiatives to protect our critical infrastructure. We recognize that the challenge is vast and complex, that threats are multi-faceted and global in nature, and that our strengths – and our vulnerabilities – lie in our interdependencies. Further, we acknowledge that the environment changes rapidly and that information sharing and coordination are crucial to improving our overall national and economic security. Cognizant of these realities, DHS' cyber security initiatives and efforts are designed to address each of the priorities set forth in the *National Strategy to Secure Cyberspace* ("the Strategy"):

Priority I:	A National Cyberspace Security Response System
Priority II:	A National Cyberspace Security Threat and Vulnerability Reduction Program
Priority III:	A National Cyberspace Security Awareness and Training Program
Priority IV:	Securing Government's Cyberspace
Priority V:	National Security and International Cyberspace Security Cooperation

Cyberspace Security Awareness and Training: A National Priority

The Strategy recognizes that in addition to vulnerabilities in existing information technology systems, a lack of familiarity, knowledge, and understanding of the issues contribute to the challenge we face in securing our information infrastructure and networks. In its Priority III: A National Cyberspace Security Awareness and Training Program, the Strategy lays out a mandate to address this challenge that calls upon the U.S. Government to promote a comprehensive national awareness program to empower all Americans – businesses, the general workforce, and the general population – to secure their own parts of cyberspace. Just as we all have an obligation to learn about driving safety rules on the highway for our own personal protection, as well as for the protection of others; we have an equal responsibility to protect ourselves and our Nation by learning about cyber security.

DHS has integrated all of the priorities of the Strategy into our cyber security programs. In addition, we are working closely with other federal agencies, academic institutions, and the private sector toward these objectives.

Awareness

The Strategy clearly identifies the users and stakeholders in cyber security in Priority III as home users and small business, large enterprises, institutes of higher education, the private sectors that own and operate the vast majority of the Nation's cyberspace, and state and local governments. We are reaching out to, and partnering with, each of these groups in addition to other groups within the Federal Government.

DHS recognized that in order to meet many of the mandates in the Strategy and other objectives addressing greater national cyber security, we needed to create an operational mechanism for building a cyber security readiness and response system. As such, through an initial partnership with the CERT Coordination Center (CERT/CC) at Carnegie Mellon University, we created the U.S. Computer Emergency Readiness Team, or US-CERT. Through the partnership, US-CERT is able to leverage, rather than duplicate, existing capabilities and accelerate national cyber security efforts. US-CERT provides a national coordination center that links public and private response capabilities to facilitate information sharing across all infrastructure sectors and to help protect and maintain the continuity of our Nation's cyber infrastructure. The overarching approach to this task is to facilitate and implement systemic global and domestic coordination of deterrence from, preparation for, defense against, response to, and recovery from, cyber incidents and attacks across the United States, as well as the cyber consequences of physical attacks. To this end, US-CERT is building a cyber watch and warning capability, launching the US-CERT Partnership Program to build situational awareness and cooperation, and coordinating with U.S. Government agencies and the private sector to deter, prevent, respond to and recover from cyber – and physical – attacks. Through its Internet portal, US-CERT is a crucial component of – and a distribution tool for – our cyber security awareness activities.

On January 28, 2004, the Department of Homeland Security, through US-CERT, unveiled the National Cyber Alert System, an operational system developed to deliver targeted, timely and actionable information to Americans to secure their computer systems. As the U.S. Government, we have a fundamental duty to warn the public of imminent threats and to provide protective measures when we can, or least provide the information necessary for the public to protect their systems. Furthermore, it is also important to inform the public about the true nature of a given incident, what the facts are, and what steps they can and should take to address the problem. The offerings of the National Cyber Alert System provide that kind of information, and we have already issued several alerts and the initial products in a periodic series of "best practices" and "how-to" guidance messages. We strive to make sure the information provided is understandable to all computer users, technical and non-technical, and reflects the broad usage of the Internet in today's society. I am pleased to report that Americans are exhibiting a keen interest in the alert system. On day one of the National Cyber Alert System launch we had more than one million hits to the US-CERT website. Today, more than 250,000 direct subscribers are receiving National Cyber Alerts to enhance their cyber security. As we increase our outreach, the National Cyber Alert System is

investigating other vehicles to distribute information to as many Americans as possible. For your reference and for your constituents, I urge you to visit www.us-cert.gov to subscribe to a number of our information services to facilitate protecting your computer systems. We encourage you to include a link to US-CERT on your Committee web page to notify your constituents of the National Cyber Alert System and empower them to sign up to the system to improve their cyber vigilance.

DHS is keenly aware of the power of the media as an education and awareness vehicle. We launched an outreach program concurrent with the launch of the National Cyber Alert System. In nine days, we generated almost one thousand media placements across national newspapers, trade publications, web sites, as well as television and radio broadcast media. Feature coverage on CNN, Fox News, NBC News, National Public Radio, and in *The Wall Street Journal, The Washington Post, Newsweek,* and *The New York Times* generated millions of impressions, increasing American's cyber security awareness and driving citizens to visit the US-CERT website to subscribe to the National Cyber Alert System.

DHS is also a sponsor of the National Cyber Security Alliance (NCSA) and *StaySafeOnline*, a public-private organization created to educate home users and small businesses on cyber security best practices. Other NCSA sponsors include: The Federal Trade Commission, AT&T, America Online, Computer Associates, ITAA, Network Associates, and Symantec. DHS is providing matching funds to expand the NCSA end-user outreach campaign, which will include a Fall 2004 Public Service Announcement to increase awareness among Americans about key cyber security issues. We look forward to working actively with the NCSA to increase the profile and impact of its semi-annual National Cyber Security Day initiative. Coincident with the days that we reset our clocks in the spring and fall, the National Cyber Security Day program encourages Americans to review and improve their cyber readiness. We will utilize the National Cyber Security Days as a focal point to heighten our awareness efforts. We encourage each of you to take advantage of this program to hold a cyber security event in your respective districts in conjunction with the next National Cyber Security Day – October 31. In addition, we are working with NCSA on a series of other educational and awareness programs, including collaborative initiatives with Internet Service Providers and developing cyber security educational tool kits. We will be pleased to make these resources available to you for use in your districts.

The Federal Trade Commission (FTC) has also been very active in building awareness with home users and small businesses, and I am pleased that Commissioner Swindle is here to share the FTC's initiatives with you. As referenced earlier, the FTC plays a significant role in NCSA. The Commissioner has been a leading force in the FTC's information security campaign, and we work closely with his team.

It is estimated that 85 percent of America's critical infrastructure is owned and operated by private companies, and technology developed by industry continues to fuel the growth and evolution of the Internet. In December 2003, the National Cyber Security Division co-hosted the first National Cyber Security Summit in Santa Clara, California, with the Information Technology Association of America, TechNet, the Business Software Alliance, and the U.S. Chamber of Commerce. This event was designed to energize the public and private sectors to implement the *National Strategy to Secure Cyberspace*. The Summit allowed the Department of Homeland Security to work side-by-side with leaders from industry to address the key cyber security issues facing the Nation. Five industry task forces were established to focus specifically in the areas of:

- Increasing awareness
- Cyber security early warning
- Best practices for information security corporate governance
- Technical standards and common criteria
- Security across the software development lifecycle

Perhaps most importantly, the Summit served as a call to action. It represented a logical transition point from developing a national strategy to energizing the public-private partnership to implement concrete, measurable actions to improve the security of America's cyber systems. Over the past few weeks, the industry task forces have put forward sets of recommendations in each of these key areas for both the public and private sector. DHS is reviewing these recommendations, as well as those put forth by other industry and government groups. We are excited that the industry is showing such initiative.

DHS is establishing the US-CERT Partnership Program as our primary mechanism for responding to these various recommendations. As previously indicated, collaboration between the public and private sectors is crucial to achieving greater cyber security, as both have specific and important roles to play. We are developing the components of the US-CERT Partnership Program based on recommendations of the task forces, the National Infrastructure Advisory Council (NIAC), the National Security Telecommunications Advisory Committee (NSTAC), your own committee's working groups, and other similar groups. The goal of the partnership is to facilitate and leverage stakeholder collaboration to drive measurable progress in addressing key cyber security issues and mitigating our cyber vulnerabilities. DHS is moving with great urgency to put this partnership into place. We are working closely with the private and public sectors to implement an effective program.

Under the auspices of the US-CERT Partnership Program, DHS will work jointly with software developers, academic institutions, researchers, and communities of interest including the Information Sharing and Analysis Centers (ISACs) in each of the critical infrastructure sectors outlined in Homeland Security Presidential Directive 7 (HSPD 7) as well as with our federal, state, local, and international government counterparts. Our goal is to participate in, coordinate, and help refine current activities and define

future programs that will improve our national cyber security. We are already working closely with many of these organizations, such as the Multi-State ISAC and the National Association of State Chief Information Officers (NASCIO), to shape the program and to understand hurdles in our path forward.

Training and Education

In addition to awareness, I would highlight another key aspect of the Strategy's Priority III: training and education. The Strategy specifically calls for efforts to foster adequate training and education programs to support the Nation's cyber security needs and increase the efficiency of existing federal cyber security training programs.

DHS is collaborating with our intergovernmental partners to leverage and build upon their ongoing training and education programs, and we are also reaching out to academic institutions to establish cooperative arrangements. I would like to highlight two recent accomplishments in this regard.

First, I am pleased to announce that DHS has just signed on to partner with the NSA to expand its program from an NSA-specific focus to a broader national program. To reflect the expanded scope, the program is renamed, the new *National* Centers of Academic Excellence in Information Assurance Education Program.

The traditional Centers of Academic Excellence in Information Assurance Education (CAEIAE) Program was established by the NSA in 1998 to promote higher education in information assurance, and as such, increase the number of information security professionals with this critical expertise. NSA grants the CAEIAE designation following a rigorous review of university applications against published criteria based on training standards established by the National Security Telecommunications and Information Systems Security Committee, an intergovernmental organization that sets policy for the security of national security systems. The criteria measure the depth and maturity of established programs in the field of information assurance. Since its inception, the program has been highly successful, designating 50 universities in 26 states.[1] Universities designated as Centers are eligible to apply for scholarships and grants through both the Federal and Department of Defense Information Assurance Scholarship Programs.

The new, increased scope will accelerate and expand the current program, help attain national prominence, and attract participation from other universities. The net result is that America will be furnished with a growing number of cyber security professionals. Government at all levels; corporations, small businesses, and the general public all benefit from educating a strong force of highly educated information assurance professionals.

Second, I am pleased to announce that DHS has partnered with the National Science Foundation on the Scholarship for Service program. This initiative promotes

[1] See Appendix for list of CAEIAE-designated universities.

university level information assurance education and efficiently places program graduates into the federal workforce.

NSF established the Scholarship for Service Program in 2001 to train a corps of information assurance (IA) specialists and place them in federal agencies for the protection of the U.S. Government's information infrastructure. The program provides two-year scholarships to graduate and upper-level undergraduate students and, in return, those students are required to make a commitment to work for a federal civilian agency for two years. NSF projects that 81 students will graduate in May 2004, and our goal is to graduate 300 students into the program annually. The qualifications of the program graduates are outstanding. DHS, as well as US-CERT, have already hired several graduates. We are excited about the capabilities this program is producing.

In addition to these accomplishments, we have identified other strategic education programs. We are working with the Department of Education to develop cyber security programs for the K-12 curriculum in our public schools. These children are our future, and they are working on computers at a very young age. It is important to educate and raise them in a secure cyber culture from the beginning.

Conclusion

DHS views building awareness as a key, immediate, and daily objective for addressing our national cyber security. We have operationalized that function through US-CERT, the National Cyber Alert System, and our partnerships with industry, academia, and others. In addition, we know we have an obligation to address cyber security in more strategic way for the long term, and we are targeting our education and training programs to work to ensure that we have a cadre of trained security professionals to carry on that task as technology continues to evolve and change our lives over time. We have made some important strides in both these operational and strategic efforts, and we are committed to improving and expanding on them going forward.

In closing, I would add one important additional strategic systemic consideration – we need to change the DNA of technology offerings to make it easier for people to understand and deploy cyber security. While I commend the technology solution provider community for its major steps forward in auto-updating and auto-configuration management, and the like, there is much work ahead. The technology community at large needs to redouble our collective efforts to produce secure code that is easier to maintain and manage. The US-CERT Partnership Program brings together solution providers, critical infrastructure operations, educational institutions, and end-user advocacy groups to tackle these systemic issues. Our goal is to ensure that all computer users understand the rules of the road for cyber security and are empowered to stay safe online.

Thank you for the opportunity to testify before you today. I would be pleased to answer any questions you have at this time.

APPENDIX

Centers of Academic Excellence in Information Assurance Education (CAEIAE)

Alabama

Auburn University

California

Naval Postgraduate School

Stanford University

University of California at Davis

Florida

Florida State University

Georgia

Georgia Institute of Technology

Idaho

Idaho State University

University of Idaho

Illinois

University of Illinois at Urbana-Champaign

Indiana

Purdue University

Iowa

Iowa State University

Maryland

Capital College

Johns Hopkins University

Towson University

University of Maryland, Baltimore County

University of Maryland, University College

Massachusetts

Northeastern University

University of Massachusetts, Amherst

Michigan

Walsh College

Mississippi

Mississippi State University

Nebraska

University of Nebraska at Omaha

New Jersey

New Jersey Institute of Technology

Stevens Institute of Technology

New Mexico

New Mexico Tech

New York

Pace University

Polytechnic

State University of New York, Buffalo

State University of New York, Stony Brook

Syracuse University

U.S. Military Academy, West Point

North Carolina

North Carolina State University

University of North Carolina, Charlotte

Ohio

Air Force Institute of Technology

Oklahoma

University of Tulsa

Oregon

Portland State University

Pennsylvania

Carnegie Mellon University

Drexel University

East Stroudsburg University

Indiana University of Pennsylvania

Pennsylvania State University

University of Pennsylvania

Texas

Texas A&M University

University of Dallas

University of Texas, San Antonio

Vermont

Norwich University

Virginia

George Mason University

James Madison University

University of Virginia

Washington, D.C.

George Washington University

Information Resources Management College

West Virginia

West Virginia University

Mr. PUTNAM. Thank you, Mr. Yoran. I appreciate your being here today. You have had an interesting week. I would like to give you the opportunity to elaborate on the Cyber Alert that you have issued and if you would give some comment to this subcommittee on the nature of the vulnerability and the status of efforts to remedy that vulnerability on the Internet routers.

Mr. YORAN. Thank you, Chairman Putnam. The creation of the National Cyber Alert System allows us to reach out directly to a large number of operators in cyber space with information targeted to them on how they can best protect their systems or the systems which they are responsible for. In a number of recent cases, vulnerabilities have been brought to our attention which would cause specific routers to malfunction and become inoperable and not pass the traffic which they were intended to pass. This vulnerability is not information which is actionable to most home users, but certainly through our targeted delivery mechanism we can reach out to the cyber security community and provide this information to them. The detail and accuracy of the information allow the Department of Homeland Security and the Federal Government to work closely and cooperatively with the private sector. In an alert we issued late last night, we worked closely with Cisco, who proved to be a valuable partner to the Department of Homeland Security and the Nation in being very forthright about a vulnerability which was brought to their attention in their close working relationship with the US-CERT and the Department of Homeland Security, and, perhaps most importantly, with their customers, to assure that Internet backbone services and routers were adequately protected in an expeditious fashion.

Mr. PUTNAM. Why was it the British Government who revealed the vulnerability and not the Department of Homeland Security in our own country?

Mr. YORAN. I will not comment on the logic behind the British Government releasing this vulnerability on their specific timeline. Given the availability of that information, it was important for the Department of Homeland Security, working with Cisco and key Internet service providers, to put out and make as broadly available as possible some technical information with an appropriate level of detail so that folks knew how best to protect themselves. I am happy to report that while this is a significant vulnerability, those warnings were rapidly heeded by much of the backbone community and the likelihood of significant Internet disruption as a result of this vulnerability has been minimized.

Mr. PUTNAM. My understanding is, and correct me if I am wrong, that the potential for this vulnerability has been known for some time; it was not known that anyone could exploit it. Is that the case? And if so, how long has your office been aware of the existence of this potential vulnerability? And the followup would be, are there others that until now people have thought were not exploitable that we should be addressing and that people should be aware of?

Mr. YORAN. Chairman Putnam, I would welcome the opportunity to brief you in a smaller forum, a more confidential venue on some of the pre-public announcement activities and coordination on what

information was released and which communities we worked with to best serve the public interest and protect the Nation.

In terms of specific exploit code, in terms of specific vulnerabilities which were known about and have recently had exploit code developed, there have been a series of vulnerabilities discovered over the past 24 hours. In fact, two alerts have been issued on very similar topics over the past 24 hours. One of those alerts, the one dealing with the border gateway protocol, the more commonly adopted best practices approach to router management would significantly mitigate the risk and exposure an organization would experience, again highlighting the need for best practices and best practice guidance such as your working group produced and is available from NIST and from many of the vendors.

For the second of the recent vulnerabilities discovered, it is in fact a new vulnerability discovered in a specific vendor's implementation of the Simple Network Management Protocol.

Mr. PUTNAM. I think that Mr. Clay and I both would appreciate the opportunity to discuss other issues in the appropriate forum and setting. But for the purposes of this hearing, let me just ask, is security enhanced by a fundamental shift from the Internet to IP–6?

Mr. YORAN. Mr. Chairman, there are some very promising characteristics of IP version 6 which have security enhancing capability which have significant impact on how the Nation or the infrastructures might defend against some of the threats we face today. Many attack techniques which deal with exhaustive searching of Internet addresses, looking for vulnerabilities are much less practical in an IP v. 6-type of environment. Through a number of efforts within the Department of Homeland Security's Science and Technology Directorate, we are investing in a better understanding of IP v. 6's effect on Internet security. The Department of Commerce has a very active effort in understanding the implications of IP v. 6 and the adoption of IP v. 6 from a security perspective. It is important, however, to also recognize that many of the vulnerabilities which exist and many of the attack techniques which exist are not going to go away with the increased adoption of this new protocol.

Mr. PUTNAM. Thank you. I appreciate that very much. We will return to the theme of the day.

Commissioner Swindle, the evidence clearly indicates that computer users of all levels of sophistication are potential victims of worms and viruses and denial of service attacks. Who are the target audiences of the efforts by the FTC and, in Mr. Yoran's case, the cyber security division to address improvements in cyber security? I assume that the cyber turtle is not speaking to large enterprises. But in general, as you prioritize your audience, who is at the top of the list?

Mr. SWINDLE. Mr. Chairman, the cyber turtle is actually a very sophisticated creature. He is handsome and he is affable and he was modeled after me, so let us be careful how we talk about him. [Laughter.]

Mr. PUTNAM. Mr. Clay and I would like to meet him. Can we call him as a witness? [Laughter.]

Mr. SWINDLE. The FTC has traditionally been involved with consumer protection matters and consumer education is a large aspect of how we go about doing our business, both from the antitrust side as well as the consumer protection side. It is all to enhance consumer welfare. We have a tremendous amount of experience in consumer education and our efforts with Dewie the e-Turtle have been addressed primarily to consumers and small businesses. However, in the process of finding better ways to communicate with consumers, we deal with industry associations and large businesses on a constant basis and have established some rather good relationships with these companies, seeking a better understanding of the problems, seeking their advice on how they market to their customers, and we learn together from each other's experiences. So, it is a rather comprehensive approach to educating the consumer.

The target primarily is the broad base. If you can imagine a triangle of people concerned with computer and information systems security, the broad base of the triangle would be 250 million consumers here in the United States, and then we can multiply by all the people in the world who are also involved in this. Then we get up to higher levels of corporate involvement, lower levels of small business involvement, but yet the base is broad and the triangle narrows as you go higher. So our focus is on the broad base consumers, and we work closely with industry, small businesses, and associations to try to convey our message.

Mr. PUTNAM. Thank you. We look forward to Dewie joining the great pantheon of other public servant characters like Woodsie the Owl, Smokey the Bear, and McGruff the Crime Dog.

Mr. SWINDLE. That was the motivation behind my asking three bright young people, I said "I want a Smokey the Bear to be our spokesperson." and they came up with Dewie. And it has been fairly successful.

Mr. PUTNAM. Well, good.

Mr. SWINDLE. At the Federal Trade Commission, while we have the potential and expertise to do a lot of consumer education, we are a relatively small agency. We've got Dewie launched, and we are hoping that industry will pick it up and expand it. And it has expanded. We have Dewie appearing in schools and on television and with industries, and we have many industries and associations of industries linked to our Web site in which you will see the presence of Dewie on each one of those, as well as the OECD, for that matter, in the international world. They are still trying to figure him out over in Germany, but they will get there.

Mr. PUTNAM. Thank you, Commissioner. At this time, I would like to yield to Mr. Clay for his first round of questions.

Mr. Clay.

Mr. CLAY. Thank you, Mr. Chairman. I appreciate it.

Mr. Yoran, welcome to the committee. Can you describe for me the procedures that are in place to work with the private sector in circumstances that DHS advisories or warnings are necessary? For example, did the Department of Homeland Security collaborate effectively with Microsoft and the anti-virus companies during the recent wave of cyber attacks?

Mr. YORAN. Thank you, Congressman Clay. The Department of Homeland Security, through the efforts of the U.S. Computer

Emergency Readiness Team, have several venues and interaction points with which we are working with many entities in both the public and private sector. In many cases, before issuing a specific alert, in cases such as the recent Cisco alert which was published, in cases like recent viruses alerts and vulnerabilities in specific vendor operating systems such as MicroSoft, we have worked with and collaborated with those companies to assure that the information which we are providing is, in fact, technically accurate and that we are adequately providing enough information in an actionable fashion so that the public can work with the vendors providing those specific software packages on how they can best protect themselves. Further, our collaboration with the private sector extends beyond the vendor community and into the critical infrastructure owner-operator community, working closely with numerous ISACs, numerous industry associations, other information sharing organizations, and cyber security professionals and experts in the private sector to help them best assess the impact of these vulnerabilities on their specific industries.

Mr. CLAY. An extensive network of consulting going on there.

Mr. YORAN. Yes, sir. There exists an extensive network and numerous interaction points which we are continually refining and expanding upon in a series of public-private partnerships.

Mr. CLAY. Thank you. In creating the Homeland Security Department, Congress moved the Federal Computer Response Team from GSA to Homeland Security. Has this move contributed in a positive manner in the ways in which DHS now responds to cyber attacks? Did anyone leave the agency rather than move, as we saw with some other agencies?

Mr. YORAN. Well, sir, I could not provide details at this point as to whether anyone moved or not. I can certainly assure you that a number of highly qualified experts came into the Department of Homeland Security with the transition of the Fed-CERT capability and that Fed-CERT is very active in helping the Federal Government understand, address, and respond to vulnerabilities and malicious activities as they are discovered and as they occur. Earlier this morning, in fact, the Fed-CERT, Larry Hale, who is the Assistant Director of the US-CERT and the Director of Fed-CERT, conducted a conference call with OMB, under the leadership of Karen Evans, and the entire CIO council, we had representation there from the US-CERT, we had representation from Cisco, to help provide specific detail on the recent vulnerabilities, as, again, an illustration of how that Fed-CERT capability has translated into rapid capability for the Department of Homeland Security in addressing cyber security threats. We additionally conducted coordination activity with the chief information security officers of the Federal Government over the past 24 hours with respect to this specific vulnerability.

Mr. CLAY. OK. Thank you for that response.

Mr. Swindle, from a business perspective, do you view the software security industry as competitive and cutting-edge, or are there limited participants that may impact the availability of products or the cost of these products? How do you view the industry as far as from a business perspective?

Mr. SWINDLE. If I understand the question correctly, Mr. Clay, there is no doubt in my mind that we have very competitive companies out there attempting to come up with better and better and more acceptable, I mean that from the standpoint of consumer acceptability, products. As Chairman Putnam mentioned earlier, we have gone through this evolutionary process of getting into this world of cyber space and companies raced out, competitively, I might add, to try to acquire customer base, they had bells and whistles galore. Not many people were thinking too much about security or privacy for that matter, which has been a major concern of the Federal Trade Commission over the past few years. I think today, certainly on the privacy matter, these competitive companies are paying attention to it, and now I think they are focusing on security, and we are seeing better and better products from a security standpoint.

I think we will eventually see an evolution, and I think this is driven by the capacity of technology to accommodate it. I mean, everybody sort of knows what we want to do, getting the technology that will do it economically is another question. We are seeing us progress to a point where more and more computers, especially home computers, the personal devices that the masses of people use, will have baked into them more and more security and privacy attributes that will hopefully take some of the necessary action away from the user and make it automatic. I guess probably the best analogy I have found throughout this whole discussion has been the automobile. I can remember and I guess, I am looking around the room here, I may be the only one in here that can remember the way automobiles were back in the early 1950's. There were an awful lot of things we had to do then that we do not even know exist today. So I think we will see this industry progress that way. We have tremendous private sector companies trying to do good work, and they are working very hard at it.

Mr. CLAY. I thank you for that response. One other question. From your perspective, are there additional measures that the Federal Government ought to pursue to strengthen security measures taken by those in private industry? And are there economic-based computer security hygiene standards or other mechanisms in the marketplace?

Mr. SWINDLE. I think the answer to that question is multifaceted. It is going to take all of us working on it. It is going to take legislative pressure, it is going to take regulatory pressure, it is going to take competition pressure. As I said, we all got out front providing bells and whistles and nobody thought about security. Now, the company that gets ahead of its competition is one that is providing good security. So I think all these forces together are going to play a role. I think the chairman's program with the private sector and the initiatives he has taken are good. He has sort of waived the flag of regulation or some new law, and it is just amazing how that inspires people to get moving.

Mr. CLAY. To get together, right.

Mr. SWINDLE. And I do the same thing. I say either you do it—it is like the old Fram oil filter commercial where the guy holds it up and says either you buy one of these now or I will see you over here, and there is a smoldering engine over here. So, legislation

alone will not solve this problem. It is moving too fast. By the time the Congress enacts legislation, that problem has come and gone and we have a new one. I just do not think legislation alone is a solution. But I do think we progress if we are all pushing each other, challenging each other, and we continue this dialog in search of the right answer—because we all have a stake in this. We all have a selfish interest in getting it right because we are going to pay the price either as a home user whose computer which costs $700 got a virus and destroyed it, he has an interest in it, as well as Microsoft and AOL and all these other big guys, and the Federal Government. So we all have to work on this and push.

Mr. CLAY. Thank you for your response, Mr. Swindle.

Mr. SWINDLE. Yes, sir.

Mr. PUTNAM. Thank you, Mr. Clay. Before I get back into some more questions, I would like to introduce Matthew Jaunce, from Laughton-Childs Middle School in Lakeland, FL, who has a class assignment of shadowing a member of the community, hopefully a productive member of the community, unfortunately, he chose to shadow a Congressman. But Matthew, wave your hand, and welcome to Washington.

[Applause.]

Mr. PUTNAM. Commissioner Swindle, is there an estimate on the amount of economic impact or harm that has been done through phishing, phishing with a P?

Mr. SWINDLE. P-H.

Mr. PUTNAM. Phishing with a P-H.

Mr. SWINDLE. I struggle with that also. I do not know, Mr. Chairman, if we have an accurate quantitative assessment of how much of a problem it is. But we know that identity theft is very large. I think we did a survey here recently, I think it was last September, in which it is estimated, if I remember correctly something on the order of 27 million people over the past 5 years have had some unfortunate engagement with identity theft. As you certainly know, and as I mentioned earlier, phishing is a process whereby people are tricked into giving vital information such as their names and their Social Security numbers. Those two items alone can lead to an awful lot of mischief on the part of bad guys because they can use those two pieces of information to get credit cards, and by the time you catch them, your credit report has been done such damage it will take you years to get over it. These are serious problems and phishing is expanding.

There are lots of different things that could help curtail it. But I still contend the one thing that will help most is individual responsibility. And for people to be responsible and protect themselves they have to know what is happening. And that is a part of our consumer education program, to let people know the kinds of bad things that go on. We are seeing good signs. There is a commercial running on at least cable networks, because that is about all I get a chance to look at, advertising, if I remember correctly, a shredder. It shows a guy rummaging through a trash can, and he finds some stuff, puts it in his pocket, and the owner of the trash can drives up. It is late in the evening, and the guy who is rummaging through the trash can says, "Hi, Tom" or something to that effect, as if he knew this guy, and the guy has a puzzled look

on his face. So much of this information does come from trash cans and mishandled information, carelessly handled information.

So the problem of phishing, I cannot give you quantitative numbers on it, but I can assure you it is growing. The damage caused by bits and pieces of personal information falling into the wrong hands either by people losing it, which tends to be the dominant way, or somebody stealing it through the technology of computers is major. Very large.

Mr. PUTNAM. As a corollary to that, has any action been taken to prevent the deliberate construction of Web sites that prey on people's misspellings and particularly target children, a common misspelling of Britney Spears would lead you into a pornographic site, or, the most common one, whitehouse.com instead of whitehouse.gov. I know that is not exactly a cyber security issue, but since we are talking about protecting the home user, that certainly is an important piece. Has anything been done on that where they deliberately construct a Web site to lure children into these sites?

Mr. SWINDLE. We have had a couple of cases which go back a couple of years. One we refer to as "Fat Finger Dialing," or something of that nature. But we have taken some action against people who do these kinds of things. Again, it is a large world out there. I do not recall many complaints of recent times about that because I frankly think people are sort of savvy to this and pick up on it. But it is certainly out there, and it is another pitfall that people can fall prey to.

Mr. PUTNAM. Sure. Mr. Yoran, what has been the impact of current and recent legislative initiatives such as Graham-Leach-Bliley, HIPPA, and Sarbanes-Oxley on improving information security, not just for the regulated sectors but throughout corporate America?

Mr. YORAN. Chairman Putnam, some of the corollary effects of both existing legislation and some of the proposed legislation is an increased visibility of cyber security issues, an increased awareness in the private sector of their responsibilities, and an increased focus on execution of cyber security practices in the private sector.

I will also add, given the opportunity, to some of the comments Commissioner Swindle made earlier in terms of cyber crime. I certainly commend the Department of Justice's focus in the protection of children and going after child pornography, and also commend various efforts in the private sector to help curtail this type of activity, specifically America OnLine and other organizations which are providing an infrastructure and a much safer environment for America's youth in terms of their cyber security and their exposure to some of these threats.

Mr. PUTNAM. What steps has your division taken to motivate the private sector to report intrusion incidents, and how is that information protected so as not to produce a competitive disadvantage for those people who are doing the right thing and coming forward with that information?

Mr. YORAN. There are a number of initiatives underway to help encourage collaboration with the private sector, one component of which is the reporting of incidents. Certainly, in our technical alerts and in delivering technical information and assistance, guidance to the private sector is one form of activity underway which

encourages and has resulted already in the private sector's willingness to discuss cyber security issues with the Department of Homeland Security and we are confident that will continue. Additionally, sharing the increased practices around information sharing not only within the public sector, but from the public sector to the private sector have encouraged increased collaboration with the private sector. Again, I will cite two recent interactions with Cisco as the US-CERT and Cisco's willingness to be very forthright with us and use us as one mechanism for their outreach to their customers and the set of people who may be affected by recent vulnerability discoveries.

Mr. PUTNAM. Commissioner Swindle, do you believe that some of the recent legislation like HIPPA, and Graham-Leach-Bliley, and Sarbanes-Oxley have aided in improving information security throughout corporate America?

Mr. SWINDLE. In a word, yes. I think again back to that pressure, and I think it has brought a greater awareness among corporate America, and the consumers, and vendors, and clients and customers that this is serious business. And while some of it may be an enormous burden, as oftentimes legislation tends to be, we have to keep working to minimize those burdens while at the same time, where it is possible through legislation, put in place measures that will improve the circumstances.

I think getting corporate America's leadership focused on this, getting boards of directors focused on this, on why it is important, and the bottom line is why it is important for most of those people, that will help us create this culture of security that I mentioned. I do not know of a better way that we can solve this problem or at least minimize this problem. I do not know that we will ever solve the problem because technology is moving too much, but when concerns about information security and privacy of customers and clients and the information that pertains to them becomes part of a corporate culture, it will be the way we do things as opposed to something we have to do. I think in this new world in which we are living, knowing that is what we should be responsible for doing, that this is what we ought to do for the benefit of the corporation ought to be a part of that company's culture. It is the establishing through audit and other means of how the company does business and certifying the ethics, the morality, if you will, the proper procedures that they use for their corporation.

I think that is just a part of the new world that we live in. And more and more corporate leadership is realizing this and they will adopt it because I think they represent responsible companies that want to do well. I think they are going to have to do these kinds of things to do well. I would hope they would do it of their own initiative as opposed to having to have a law that says you have to do this. This is common sense. It is the right thing to do.

Mr. PUTNAM. What is the role of the ISP community in serving as a communications channel to computer users about computer security hygiene and cyber ethics?

Mr. SWINDLE. I think they have a large responsibility in this and, as I mentioned I think in my oral testimony, a part of the recent task force on comprehensive awareness, one of the features of it, initiatives of it would be to have the ISPs engage in a lot of con-

sumer education. The ISPs have two big problems. One is all this stuff flooding in on top of it which is consuming its resources, causing it great expense. And on the other side of that, the ISPs push, and e-mail comes to mind right away because that is what most consumers are engaged in and that is where an awful lot of this mischief goes on, the nuisances go right out to consumers. The ISPs I think have made remarkable progress, certainly the major ones, and I am sure some of the smaller ones have done so also, over the past couple of years in providing their subscribers with great tools. I use one of the major ISPs, and I was beating them up rather severely a couple of years ago and now with their system I rarely see any spam. I can go see the spam if I want to, but I do not have to engage it at all. They are doing good work. They are providing the tools.

What I think the biggest challenge is is getting the point across to consumers, users, home users, this wide base, the necessity that they do certain things. It is sort of like changing the oil in your car. We can build the finest car in the world, but if you do not change the oil in it, it will not be the finest very long because it is going to have problems. I think we need to make this idea of information security as much a part of our mindset as changing the oil in the car, making sure the brake pads are in good shape, or, even more simply, looking to the left and right when you cross the street. There is a role, as we have both said, for everyone to play here. I just think we have to convey that message to everyone that they have to play this role.

Mr. PUTNAM. Mr. Yoran, the role of the ISP community?

Mr. YORAN. Thank you, Chairman Putnam. Similar to Commissioner Swindle's comments, I believe we need a common responsibility framework, certainly looking at and pointing to responsibilities and action which ISPs can take up, and many of them are taking up, is one venue for progress. But, similarly, the consumers and the users of technology need to adapt better practices. They need to place greater emphasis on their cyber security and cyber security preparedness. The produce vendors and the software community need to adopt better software development practices and take up the responsibility to do that, to make cyber security more understandable. If you were not thrown off by all the technical jargon required to explain some of the vulnerabilities of the past 24 hours, you are in a small minority. Cyber security is too complex in today's environment.

There is a clear role for educators to improve cyber security awareness, ethics, and make more available cyber security courses and information so that we can better train a cadre of cyber security professionals. And there is a significant role for industry to play in their information sharing and analysis centers and in the operator community to address with a unified front cyber security challenges facing their industries.

Mr. PUTNAM. Commissioner, what is the role of the law enforcement community here? Are they doing an adequate job in prosecuting hackers and people who are using spam and using spyware and using phishing techniques illegally to defraud people, and are they doing an adequate job of educating the public about the penalties for engaging in that type of conduct?

Mr. SWINDLE. I will answer the last question first, whether they are doing a great enough job of educating the public as to the penalties they might suffer. I think we are hampered in this business of technology by the inability sometimes to find the bad guys. Certainly, we at the Federal Trade Commission have pressed cases over the past several years in which large corporations have been called to task for some of their negligence and carelessness in how they protect information, and they pay prices in a civil sense, not a criminal sense. They are put under order to not do this again. In several cases that I mentioned in my written testimony, a couple of the companies have at least a 20 year love affair to endure with the Federal Trade Commission because they have to do audits and report to us.

As far as the criminals go, I know the spam issue is something that everybody is familiar with. Finding the perpetrators of spam is a very difficult process. We are doing a number of investigations in the Federal Trade Commission, and we are going to have some results. But oftentimes, as we have said previously in testimony, when we get to the end of the trail and find the bad guys, there is nothing for us really to get other than put him out of business. And for every one of those you put out of business, there is another one that pops up.

I think we do a pretty darn good job of law enforcement under the laws that we have. I would not advocate for more laws other than what has been passed here in the Can Spam Act. We are looking at the requirements of that act trying to figure out how we successfully employ the requirements of it. We are getting lots of input from industry, from consumer groups, from privacy advocates, from all sorts of people, to help us formulate the best possible way we can enforce the law.

Part of our education effort is to work with law enforcement agencies. In the past year or so, we visited I think it is at least 10 cities speaking to law enforcement personnel telling them about identity theft, because it is singularly, if I remember correctly, the largest complaint we get, trying to help them help consumers and victims. And, we put out a lot of education materials to try to help consumers who have been victims to work their way out of some of the problems that are created.

So, there is a large effort going on. Unfortunately, it is a target rich environment, and it is difficult to get to everyone.

Mr. PUTNAM. Thank you very much. Commissioner, I know you have another engagement that you need to attend to. Before we conclude, if you would give us the top three things that the home user should do to make their systems more secure.

Mr. SWINDLE. Think. Always think. You know, as I mentioned, the ISPs in the last couple of years I think have done a good job and what they have given you is a good spam blocker, they have provided prompted updates of virus protections and firewall protections. If the average consumer, home user would employ a virus program, employ a firewall, keep those up to date, use a spam blocker to narrow down how much garbage comes in your computer, and be careful about how you open e-mail and things of this nature, you could avoid a lot of grief because a lot of these really bad acts come through, believe it or not, the simple feat of sending

an e-mail. It can do a lot of destruction. And employing these simple steps is not a difficult thing to do.

Again, it is back to making everybody aware. And we would solicit the help of industry, as we are doing, and we would certainly ask that Congress call on us. We will make materials available. I would like to see, as sort of a goal for all of us, see every Member of Congress have a link to the Federal Trade Commissionsite as well as the sites that I think you mentioned earlier that industry has identified. There is so much good information out there about how to be safer. And that is what we have to achieve—safe computing. And I thank you very much for this opportunity.

Mr. PUTNAM. Thank you very much, Commissioner.

Mr. Yoran, top three things home users can do to make their systems more secure?

Mr. YORAN. I would agree that the top one is think. Many of the mistakes which are made could be easily avoided by folks taking a moment to reflect before opening attachments from folks they have not received e-mail from or from which they are not expecting e-mail. I would encourage folks to subscribe to the National Cyber Alert System to receive tips and information on how they can protect themselves from online scams, phishing, and a wide variety of activities. And to also learn more through participation in many of the Stay Safe On Line initiatives. Certainly, if turtles can be teenage mutant ninja and martial arts experts, they can help America better protect our cyber citizens.

Mr. PUTNAM. Thank you very much. I thank the entire first panel. And with that, I will dismiss panel I and we will go into recess momentarily as we set up for panel II.

The subcommittee is in recess.

[Recess.]

Mr. PUTNAM. The subcommittee will convene.

I would like to ask the second panel to rise and raise your right hand for the administration of the oath.

[Witnesses sworn.]

Mr. PUTNAM. Note for the record that all the witnesses responded in the affirmative and have their official souvenir photo of being sworn in.

We will move directly to the testimony. Our first witness is Larry Clinton. Mr. Clinton is currently the deputy executive director and chief of staff of the Internet Security Alliance, a collaboration between the CERT/cc at Carnegie Mellon University and one of the Nation's largest trade groups, the 1,200 member company Electronic Industries Alliance. This past year Mr. Clinton has served as the private sector coordinator of the Corporate Information Security Working Group on Market Incentives for Improved Cyber Security. Prior to coming to ISAlliance last year, Mr. Clinton was with U.S. Telecom Association for 12 years including the last 6 as vice president.

We welcome you to the subcommittee. You are recognized for 5 minutes.

STATEMENTS OF LARRY CLINTON, CHIEF OPERATING OFFICER, INTERNET SECURITY ALLIANCE; ANDREW HOWELL, VICE PRESIDENT, HOMELAND SECURITY, U.S. CHAMBER OF COMMERCE; RODNEY PETERSEN, SECURITY TASK FORCE COORDINATOR, EDUCAUSE; AND DOUGLAS SABO, MEMBER, BOARD OF DIRECTORS, NATIONAL CYBER SECURITY ALLIANCE

Mr. CLINTON. "I am very busy. Do I really need to read this?" That, Mr. Chairman, is the first line of the "Common Sense Guide to Cyber Security for Small Businesses" which the Internet Security Alliance released on its Web site earlier this month.

We decided to begin our publication in this unusual way because during the market research we did preparing the document we learned a critical fact. That is, that education is far more than simply raising awareness or disseminating information. Education, resulting in behavior change, requires motivation.

The Internet Security Alliance is a collaboration between the CERT/cc at Carnegie Mellon University and the Electronic Industries Alliance. We are an international organization with membership on four continents and a wide variety of economic sectors, including banking, insurance, entertainment, traditional manufacturing, as well as telecommunications, security, and consumer food products. The ISAlliance runs an intensive information sharing program with the CERT/cc and we have taken this information and from it produced a series of best practice guides which are provided free of charge on our Web site.

In December of last year, the ISAlliance was asked by the National Cyber Security Summit to produce a best practices document, this time targeted to small business users. Small businesses are particularly vulnerable to cyber attack. One out of every three small businesses was affected by the MyDoom virus, fully twice the number of larger businesses. Obviously, larger organizations have more to lose in terms of absolute dollars; however, smaller margins that smaller businesses operate under vastly magnify the impact an attack can have on a small business.

Despite the need, there is very little help being offered to this community. The very first conclusion reached by the Best Practices task force you formed, Mr. Chairman, on the Corporation Information Security Working Group, was that available IS guidance as a whole is not readily scalable to meet the varying needs of large, mid-size, and small organizations.

We decided to approach this project in a market-driven way and asked the target audience what they needed to know and how we could best motivate them. We coordinated with the National Association of Manufacturers, the National Federation of Independent Businesses, and the U.S. Chamber of Commerce. Each of these organizations agreed to gather for us a group of their membership and we conducted 10 focus groups, involving nearly 100 actual small businesses, to discuss their cyber security needs.

We learned that small businesses are aware of the potential impact of cyber attacks but they are also aware of the costs both in time and money to constantly keep up with the ever evolving threats and vulnerabilities. Attempting to address the needs of small businesses and cyber security without realistically address-

ing the costs of their full participation is shortsighted and will ultimately be ineffective.

Having been educated by our audience, we produced a document that I believe looks unlike any other in the field. To speak to the small business owner's needs, we provided a real list of cast studies drawn from the media, the FBI Web site, and reported directly to us during our research. These are actual cases of small manufacturers, contractors, credit unions, hotels, diners, limo services, law firms, accountants, and venture capitalists, all of whom have had their businesses severely hurt by cyber attacks. They describe a wide variety of situations we believe the typical small business owner can relate to. We then outlined a 12-step program of cyber security specifically for small businesses including why they need to take the step, how to get started, who needs to be involved, the degree of technical skill required, and, specifically, the cost involved.

However, more important than the product we produced is what we learned while we were producing it. For too long, cyber security has been thought of as an IT problem with an IT solution. While obviously there are technology elements to cyber security, it is also a management problem, it is an economic problem, and it is a cultural problem. And to adequately address the need, we need to listen to the IT people of course, but also the users, the educators, the marketers, and the economists. We need a broad, market-centered, incentive-laden approach to the issue, rather than a narrow, techno-centered dogmatic approach.

We learned again that to achieve long term behavior change, which is the goal of education, we need to do more than simply share information. You noted it yourself, Mr. Chairman, in the letter you sent inviting us to today's hearing. You said, for example, the Blaster worm infected over 400,000 computers worldwide in less than 5 days, despite the fact that the patch that would have prevented the infection had been available for over a month. The information was there, Mr. Chairman, but the necessary incentives to use it were not. Speaking as a former teacher, who is married to an elementary school teacher with two small children in school, I can assure you that education takes more than providing information. Some students are motivated by praise, some by pride in good grades, some by the prospect of tangible rewards. Few are motivated by threats. Computer users are no different. Creative thinking needs to be done on the issue of incentives.

ISAlliance is taking the lead on this issue. In the first quarter of 2003, we signed an agreement with AIG, the world's largest provider of cyber insurance. Under this agreement, AIG will provide premium credits, where permitted, of up to 15 percent for companies who will join the Alliance and subscribe to our best practices. We believe this is the first operating program which specifically ties a widely independently endorsed set of cyber security best practices specifically to directly lower business cost. I understand that today we are here to discuss straightforward the issues of education. But I would urge the Chair to consider another hearing soon to discuss the complex issues of developing a market incentive program to compliment the educational initiatives.

I must thank you and your staff, particularly Mr. Dixon, Mr. Chairman, for the leadership you have shown in this regard. Thank you.

[The prepared statement of Mr. Clinton follows:]

Testimony of
Larry Clinton
COO
Internet Security Alliance

before the
Subcommittee on Technology, Information Policy, Intergovernmental Relations and the Census
Government Reform Committee
U.S. House of Representatives

regarding
Protecting Our Nation's Cyber Space: Educational Awareness for the Cyber Citizen

April 21, 2004

"I'm very busy. Do I really need to read this?"

That, Mr. Chairman, is the first line of the "Common Sense Guide to Cyber Security for Small Businesses" which the Internet Security Alliance released on its web site last month.

We decided to begin our publication in this unusual way because, during the course of the extensive market research we did in preparing the document, we re-learned a critical fact. That is, education is far more than simply raising awareness or disseminating information.

Education, resulting in behavior change, requires motivation.

In the next few minutes I'd like to tell you about the educational activities we have undertaken at ISAlliance. And while we are delighted to present this record to you, I think what is more important is what we have learned about **how** to conduct an educational campaign. As the Bible teaches us, give a man a fish you feed him for a day, teach a man to fish, and you feed him for a lifetime.

By way of background, the Internet Security Alliance was founded in April of 2001, five months prior to the events of 9/11, because even then we saw a growing need for improved information security. We are not, largely, a policy shop. We are interested in practical methods to achieve pragmatic behavior change resulting in improved security.

We are a collaboration between the CERT/cc at Carnegie Mellon University and the Electronic Industries Alliance here in the DC area. ISAlliance is unique in that we are an international organization with membership from 4 continents and multiple sectors of the economy. The ISAlliance membership comes primarily from the Internet user community spanning such diverse sectors as banking, insurance, entertainment, and traditional manufacturing, as well as telecommunications, security and consumer food products.

For the past three years we have provided our members under strict non-disclosure agreements, the absolute best Internet threat and vulnerability information in the form of several hundred technical e-mails each year from the CERT/cc. We also provide regular meetings on technical security issues.

We have taken this information and produced a series of best practices guides which are provided free of charge on our web-site as well as giving our members unique opportunities for discounts on education, training and insurance to provide market incentives for improved cyber security. We believe that only the creative use of the market forces can provide the continued motivation that will lead to maximum information security.

Realizing that corporate computer security needed to begin at the top, we published our first best practices manual in July 2002: "A Common Sense Guide for Senior Managers." The document was very well received. It was abstracted in the draft National Strategy to Secure Cyber Space and endorsed by organizations as varied as the National Association of Manufacturers, the US India Business Council and TechNet. We followed that up in 2003 with a

new best practices document, equally well received "A Common Sense Guide to Home Users and Mobile Executives."

Based on this work, the ISAlliance was asked at the National Cyber Security Summit in December 2003 to produce another best practices document, this time targeted to small business users.

This was a timely request. Small Businesses are particularly vulnerable to cyber attack. Earlier this year, research found that one out of every three small businesses was affected by the MyDoom virus, fully twice the rate of larger businesses. Obviously, larger organizations have more to lose in terms of absolute dollars; however, the smaller margins smaller businesses operate on vastly magnify the impact an attack can have on a small business.

Computer World recently quoted the effect a computer attack had on the owner of one company that had once been valued at over a million dollars, "My business is gone, and my wife's business is gone. Now we just hope we can hang on to our house."

Despite the extent and impact cyber attacks are having on smaller businesses, there was very little help being offered to this community. The very first conclusion reached by the Best Practices task force you formed, Mr. Chairman, as part of the Corporate Information Security Working Group, was "Available IS guidance as a whole … is spread over a wide continuum of abstraction and not readily scalable to meet the varying needs of large, mid-size and small organizations."

Most of the best practices documents that have been written in the cyber security field, including our previous efforts, are written the same way. An information technology expert is asked to tell the target audience what they need to know. We decided to approach the project in a different way, in a market driven way. We decided to ask the target audience what they needed to know and how we could best motivate them to act.

We were delighted with the cooperation we received from virtually all the major trade associations who hold small businesses as primary clients. We coordinated with the National Association of Manufacturers, The National Federation of Independent Businesses and the US Chamber of Commerce. Each of these organizations agreed to gather for us a group of their membership and we conducted 10 focus groups, involving nearly 100 actual small businesses, to discuss their cyber security needs.

By listening to our target market we learned a great deal, some of which I would summarize here.

First, we learned that while certainly sympathetic to national security needs, in real life not many small business owners were going to go to the time and expense of improving their cyber security based on the type of public policy appeals common in the existing literature. We needed to speak to their personal needs, not the broad national need.

Second, we learned that many small business owners were not intimately familiar with computer security technology and saw much of the existing material as excessively technical jargon. We learned that this material was unlikely to be read, let alone acted upon.

Third, we learned that although most small businesses were aware of the generalized needs for cyber security, there was an unrealistic hope that it wouldn't hit them, either because they are too small to be noticed or because they have taken rudimentary steps in the direction of security. Since many attacks are generalized to the network, and perpetrators are evolving their methods to circumvent initial defenses, we know that this is a very dangerous misconception.

Fourth, we learned that even if we could convince small businesses that they needed to be more proactive toward cyber security, much of the material available to them was irrelevant. Much of the previous material was written for technical experts presumably on staff. Small businesses often don't have IT staffs. So, for example, they don't want a "how-to" instruction on configuring their network, they want a "how-to" section on how to evaluate a consultant to come in and do it for them. That calls for a very different type of book.

Finally, we learned, again, that to achieve long-term behavior change we needed to do more than simply share information. You noted it yourself in the letter inviting us to today's hearing Mr. Chairman. You said "For example the Blaster worm infected over 400,000 computers world wide in less than 5 days…despite the fact that the patch that would have prevented infection had been available for over a month." The information was there, the necessary behaviors were not.

We learned from the small businesses we spoke with that they were aware of the potential of cyber attacks, but they are also aware of the costs both in time and money to constantly keep up with the ever evolving threats and vulnerabilities. Attempting to address the needs of small businesses and cyber security without realistically addressing the costs of their full participation is shortsighted and will ultimately be ineffective.

Having been educated by our audience, we produced a document that I believe looks like no other in the field, including our own previous work. To speak to the small business's personal needs we provided a list of real case studies drawn from the media, listed on the FBI website, or reported directly to the Internet Security Alliance during our research.

These are actual cases of small manufacturers, contractors, credit unions, hotels, diners, limo services, law firms, accountants and venture capitalists, all of whom have had their businesses severely hurt by cyber attacks. They describe a wide range of situations we believe the typical small business owner can relate to. We call these sections "this could happen to you."

We utilized a true expert, Carol Woody from the CERT/cc, to outline a simple, but by no means simplistic, "12-step program" of cyber security for small businesses. Each section provides step-by-step information including why they need to take the step, how to get started, who needs to be involved, the degree of technical skill required and, specifically, the cost involved.

Understanding that many small businesses, for whatever reason, were reluctant to resolve cyber security issues on their own, we added a totally new section on selecting a consultant.

Although the booklet is both unique and barely a month old, we are delighted with the reception it has already received. In addition to being available through the Internet Security Alliance web site and the National Cyber Partnership web site, it is also being provided through the National Association of Manufacturers site and the Electronic Industries Alliance site. I'm told the US Chamber of Commerce anticipates endorsing the publication shortly and is linking its members to the publication. The Financial Services Sector Coordinating Council, an alliance of 28 financial services trade associations and companies that work together to improve critical infrastructure protection and homeland security, will be making the guide available to its members. Additionally, the financial sector is holding a series of meetings with thousands of its members where the guide will be highlighted.

We are currently in contact with a wide range of other associations to assist in distributing the publication.

However, more important than the product we produced is what we learned about how to produce it. For too long, cyber security has been thought of as an "IT problem" with an "IT solution." While obviously there are technology elements to cyber security it is also a management problem. It is an economic problem. It is a cultural problem. And, to adequately address it we need to listen to the IT people of course, but also to the users, the educators, the marketers and the economists. We need a broad, market centered, and incentive-laden approach to the issue, rather than a narrow, techno-centered dogmatic approach.

Speaking as a former teacher, who is married to an elementary school teacher with two school aged children, I can assure you, education takes more than providing information. Some students are motivated by praise, some by pride in good grades, some by the prospect of tangible rewards. Few are motivated by threats. Computer users are no different. Creative thinking needs to be done on the issue of incentives. I understand that today we are here to discuss the straightforward issues of education. But I would urge the chair to consider another hearing soon to discuss the complex issues of developing market incentives as a compliment to educational initiatives.

Mr. Chairman, the Internet Security Alliance congratulates you on all you are doing to spread the word about information security. We also are proud to be before your committee today with several of our colleagues with whom we are working together in this effort. And while we believe we are working hard and learning more and more how to be more effective, we are also aware that there is still much work to be done. For example, we as yet have no funding to make the guide I have spoken of today available in hard copy.

For this we look forward to greater participation from both industry and government. There is a great deal of work to be done on technology, on education and on developing appropriate incentives. We look forward to continuing our work together.

Thank you.

The Executive Board of the ISAlliance is made up of representatives of the following corporations: AIG Insurance, Ceridian, Cable & Wireless, the Frank Russell Company, Mellon Financial, National Association of Manufacturers, Nortel Networks, Northrop Grumman Mission Systems, Raytheon, Red Siren, Sony, TATA Consulting, VeriSign, Verizon, Visa.

For more information, please contact:

Larry Clinton: 703.907.7028
2500 Wilson Blvd, Arlington, VA 22201
www.isalliance.org

Mr. PUTNAM. Thank you, Mr. Clinton.

Our next witness is Andrew Howell. Mr. Howell is the vice president of Homeland Security for the U.S. Chamber of Commerce, the world's largest business federation. As such, he is the organization's principal spokesman on homeland security issues and responsible for building and maintaining relationships with the administration and regulatory agency leaders. He is also responsible for developing the organization's overall homeland security policy strategy and ensuring that it is implemented. Prior to his current position, Mr. Howell served as senior vice president of the National Chamber Foundation, a public policy research arm of the U.S. Chamber of Commerce.

Welcome to the subcommittee. You are recognized for 5 minutes.

Mr. HOWELL. Thank you and good afternoon, Chairman Putnam, Congressman Clay. My name is Andrew Howell. I am vice president of homeland security for the U.S. Chamber of Commerce. The Chamber is the world's largest business federation representing more than 3 million businesses and organizations of every size, sector, and region.

Thank you for giving me this opportunity to discuss the Chamber's cyber security awareness efforts with you all. Also, Mr. Chairman, I would like to thank you for your leadership on this issue, and for recognizing the importance of enhancing awareness of cyber security among the public and private sectors.

"The National Strategy to Secure Cyberspace," released in February 2003, called for a comprehensive, national awareness program to empower all Americans—businesses, the general work force, and the general population—to secure their own parts of cyberspace. This strategy asserts that everyone who uses the Internet has a responsibility to secure the portion of cyberspace that they control.

The Chamber supports this view. It is the responsibility of a person using a product to know how to use that product safely. However, we do not believe that raising awareness is the only step in our journey to enhancing cyber security. Instead, it is one very important leg in this trip. Enhancing cyber security requires the combined efforts of users, technologists, and senior executives, those that use software and hardware, those that make software and hardware, and those that manage enterprises that rely on software and hardware to make the company operate. While technologists have a responsibility to make secure products, end users have a responsibility to use those products securely.

A good analogy to this is the automobile. While cars provide individuals with great benefits, they also can be dangerous. Therefore, cars come equipped with seatbelts and airbags. However, ultimately, it is the driver's responsibility to buckle his seatbelt and know how to operate the vehicle safely. The vehicle must be maintained regularly, and when there is a recall notice, the owner has the responsibility to take the car in for repair. At the same time, automakers continue to design cars with new and innovative features, including new ones oriented to improve safety, and market them to the consumer.

By promoting user awareness, we are not, as some maintain, blaming users for cyber vulnerabilities. Instead, it is through

awareness that we highlight the issue of cyber security, inform people what they can do to manage online risks, and, in the process, create a market of consumers who can intelligently factor security into their purchasing decisions. By informing users about what they can do to enhance their cyber security, we will reduce the number of breaches, mitigate economic losses, and create a market that demands more secure products.

Moving the market to demand more secure products is an important component of enhancing our Nation's level of cyber security preparedness. Ultimately, we believe the market is better able to respond to security challenges than regulations will ever be. Whereas market forces propel companies to be flexible, innovative, and customer oriented, regulations are reactive and constrictive. As companies of all types become more aware of information security risks and protective steps they can take, we are confident they will demand more secure products. Companies that recognize this market shift and sell products that exploit it will have an advantage over their competitors. The market remains a powerful vehicle for increasing cyber security, but before this power is fully realized, we need to better inform consumers on why cyber security is an issue that matters to them.

For these reasons, the U.S. Chamber of Commerce is committed to increasing the awareness of cyber security in the business community and explaining cyber security in terms that businesses understand. For too long the issue of cyber security has been talked about in technological terms, as Larry mentioned. As a result, many corporate leaders and small business owners view it as a technology issue that should be solved by technologists. From our perspective, this is a mistaken perception that must be corrected.

The U.S. Chamber has regularly used our membership publications, including USChamber.com, to provide tips and guidance to small business owners, to explain why cyber security is important to their businesses, and to offer easy to implement advice on how to better secure their networks. Included with my prepared statement is one such article which appeared in the April edition of our monthly newsletter.

Mr. Chairman, my prepared statement details activity the Chamber has undertaken to implement the awareness component of the National Strategy. Given our limited time, I will not go into detail about these activities. However, as you know, the Chamber co-chaired the Awareness in Education Group that was created as part of your Corporate Information Security Working Group, and we serve as secretariat of the National Cyber Security Summit Awareness and Outreach Task Force. Both our National Cyber Security Summit Task Force Report and reports to the CISWG were submitted with my prepared statement.

Mr. Chairman, thank you again for this opportunity. I would be pleased to answer any questions at the end of this panel you or anyone else might have. Thank you.

[The prepared statement of Mr. Howell follows:]

Testimony of Andrew Howell
Vice President, Homeland Security
U.S. Chamber of Commerce

To the House Government Reform Committee
Subcommittee on Technology, Information Policy, Intergovernmental Relations and the Census

April 21, 2004

Chairman Putnam, Vice Chair Miller and Congressman Clay, my name is Andrew Howell, and I am Vice President of Homeland Security for the U.S. Chamber of Commerce. The U.S. Chamber of Commerce is the world's largest business federation representing more than three million businesses and organizations of every size, sector and region.

Thank you for giving me this opportunity to discuss the Chamber's cyber security awareness efforts. Also, Mr. Chairman, I would like to thank you for your leadership on this issue, and for recognizing the importance of enhancing awareness of cyber security among the public and private sectors.

The National Strategy to Secure Cyberspace, released in February of 2003, called for a "comprehensive, national awareness program to empower all Americans—businesses, the general workforce and the general population—to secure their own parts of cyberspace" (Page 37). The strategy asserts that everyone who uses the Internet has a responsibility to secure the portion of cyberspace that they control.

The Chamber supports this view. It is the responsibility of a person using a product to know how to use that product safely. However, we do not believe that raising awareness is the only solution to enhancing cyber security. Instead, it is one part of

the solution. Enhancing cyber security requires the combined efforts of users, technologists, and senior executives—those that use software and hardware, those that make software and hardware, and those who manage enterprises that rely on software and hardware to make the company operate. While technologists have a responsibility to make secure products, end users have a responsibility to use those products securely.

A good analogy to this is the automobile. While cars provide individuals with great benefits, they also can be dangerous. Therefore, cars come equipped with seatbelts. However, ultimately, it is the driver's responsibility to buckle his seatbelt and know how to operate the vehicle safely. The vehicle must be maintained with regular maintenance, and when there is a recall notice, the owner has a responsibility to take the car in for repair. At the same time, in the interest of selling more products, automakers continue to design cars with more safety features, and market those features to the consumer.

By promoting user awareness, we are not, as some maintain, blaming users for cyber vulnerabilities. Instead, it is through awareness that we highlight the issue of cyber security, inform people what they can do to manage risks, and, in the process, create a market of consumers who can intelligently factor security into their purchasing decisions. By informing users about what they can do to enhance their cyber security, we will reduce the number of breaches, reduce economic loss, and create a market that encourages the production of more secure products.

Moving the market to demand more secure products is an important component of enhancing our nation's level of cyber security preparedness. Ultimately, the market is better able to respond to security challenges than regulations will ever be. Whereas

market forces propel companies to be flexible, innovative and customer oriented, regulations are reactive and constrictive. As consumers of all types become more aware of information security risks and protective steps they can take, they will demand more secure products. Companies that recognize this market shift and sell products that exploit it will have an advantage over their competitors. The market remains a powerful vehicle for increasing cyber security, but before this power is fully realized, we need to better inform consumers on why cyber security is an issue that matters to them.

For these reasons, the U.S. Chamber of Commerce is committed to increasing the awareness of cyber security in the business community and explaining cyber security in terms that businesses understand. For too long, the issue of cyber security has been talked about in technological terms. As a result, many corporate leaders and small business owners view it as a technology issue that should be solved by technologists. From our perspective, this is a mistaken perception that must be corrected.

Recognizing this, in February of 2002, before the release of *The National Strategy*, we helped to create, organize and support the National Cyber Security Alliance (NCSA), a public-private coalition dedicated to raising cyber security awareness among small business owners and home users. Doug Sabo, of McAfee Security is an NCSA Board Member and will provide you with more details about the Alliance and its work.

At the same time, the U.S. Chamber of Commerce has regularly used our membership publications, including *USChamber.com*, to provide tips and guidance to small business owners, to explain why cyber security is important to their business and to offer easy

to implement advice on how to better secure their networks. Attached is the most recent version of this publication, which includes some tips for small business owners.

In December of 2003, the Chamber partnered with the Information Technology Association of America, the Business Software Alliance, TechNet and the Department of Homeland Security to host the National Cyber Security Summit. As part of the Summit process, an Awareness and Outreach Task Force was created to provide recommendations on implementing the awareness component of *The National Strategy*. The Chamber volunteered to serve as Secretariat for that Task Force, which is chaired by Dan Caprio of the Federal Trade Commission, Ty Sagalow of AIG, and Howard Schmidt of e-Bay.

Early in the process, the Task Force decided that it wanted to change user behavior and, as much as possible, provide incentives that will encourage people to do so. We targeted five key markets: small businesses, large enterprises, home users, state and local governments and K-12 schools and institutions of higher education. On March 18, 2004 the Task Force released its first report, detailing its completed work and next steps.

Soon after the summit in December, as part of Chairman Putnam's Corporate Information Security Working Group (CISWG) process, the Chamber was asked, along with NFIB, to co-chair the sub group on awareness. The work of the CISWG sub group focused on three audiences: small businesses, large enterprises, and home users. Mr. Chairman, as you well know, on March 3, 2004 we presented our report to you, detailing some recommendations our group thought were good next steps for these target markets.

Both our National Cyber Security Summit Task Force report and our report to the CISWG are attached to this testimony. I ask that that they be included in the hearing record.

To quickly summarize our findings, let me just touch on some highlights. For the small business audience, it was evident that before small business owners would upgrade or enhance their cyber security, they needed to understand their level of cyber risk. A company called nuServe, whose CEO, Kai Tamara Hare, Chaired the National Cyber Security Summit Small Business Working Group, agreed to make available, on a complimentary basis, the company's Cyber RiskProfiler. This interactive online tool allows small business firms to better understand their information security risks.

Also, it was clear to the Task Force, after some extensive research, that there is no practical guidance for small businesses seeking to better manage the risks they face online. To fill this void, the Task Force asked the Internet Security Alliance to produce a *Common Sense Guide to Cyber Security for Small Businesses.* As part of the process, Larry Clinton and his colleagues hosted 10 focus groups with 100 small business owners to better understand the needs of this particular market. Larry will discuss the Guide in more detail, but let me just say that initial feedback is very positive.

Finally, as an incentive to follow this Guide and use the RiskProfiler, AIG eBusiness Risk Solutions has agreed to provide cyber insurance credits, where legally permitted. All a company must do is demonstrate they use the RiskProfiler and follow the recommendations of the Guide.

For large enterprises, we proposed that the Department of Homeland Security partner with industry on a series of regional homeland security forums to discuss the role of the private sector in homeland security in general, and cyber security specifically. We envision this being a partnership between DHS, our task force and corporate C-Suite executives.

For home users, we noted our support for a national public service campaign to increase the level of cyber security awareness. Also, our participants contributed to the National Cyber Security Alliance's recently released "Top 10" tips for home users and small businesses.

All of the aforementioned recommendations were made by the National Cyber Security Summit Awareness and Outreach Taskforce and the CISWG Education and Awareness group. Yet let me also tell you about two additional markets covered by the National Cyber Security Summit Awareness and Outreach Task Force. One focused on K-12 Schools and Institutions of Higher Education, and the other on State and Local Government.

Rodney Peterson, Security Task Force Coordinator of EDUCAUSE serves as a Co-Chair of the Awareness Task Force's education working group, and will tell you about the great work that is going on in that field. He, along with Co-Chair Jim Teicher, Executive Director of CyberSmart!, produced a detailed plan with specific actions by set dates.

For state and local governments, we gathered a group of talented and dedicated leaders committed to raising cyber security awareness in this target market. Among the many accomplishments this group made were: the recommendation to establish a

national awards program, in conjunction with DHS, to recognize outstanding achievement from teams of state and local government information security specialists; the development of web-based cyber security tutorials; and the compilation of best practices tools for state and local governments. The working group also has identified distribution channels for this compilation.

One of the most rewarding aspects of leading the awareness segments of both of these efforts was seeing the tremendous interest in our work. School boards, teacher's unions, Fortune 500 firms, and small businesses all contributed to our efforts and will be essential to our ultimate success. And there is no better manifestation of this commitment than the fact that our next National Cyber Security Summit Awareness and Outreach Task Force Meeting is set for Friday, April 30.

Mr. Chairman, thank you again for this opportunity. I would be happy to answer any questions you or your committee might have.

Awareness and Outreach Task Force
Report to the National Cyber Security Partnership
March 18, 2004

Executive Summary

About the Task Force
The Awareness and Outreach Task Force, an industry-led coalition of interested security experts from the public and private sectors, was created as part of the National Cyber Security Summit process. Task force members include representatives from trade associations, nonprofit organizations, publicly traded and privately held companies, and state, local, and federal government. Task force members participated voluntarily, donated their time, and were not paid.

The task force is not an advisory group to the Department of Homeland Security (DHS) or any other state, local, or federal government department or agency. Instead, it operates under the guidance and coordination of the National Cyber Security Partnership, a coalition of trade associations, including the U.S. Chamber of Commerce, the Information Technology Association of America, TechNet, and the Business Software Alliance, that sponsored and organized the National Cyber Security Summit held in Santa Clara, California, on December 2—3, 2003.

TASK FORCE MISSION
Originally, this task force was charged with developing an awareness campaign to inform small businesses and home users about the importance of cyber security. However, during the December 2--3, 2003, National Cyber Security Summit, the task force expanded its scope beyond small businesses and home users to more accurately reflect the priorities of the *National Strategy to Secure Cyberspace*. The current mission and description of the taskforce follows:

Mission: To promote a comprehensive national awareness program to empower all Americans—businesses, the general workforce, and the general population—to secure their own parts of cyberspace.

Description: The Awareness and Outreach Task Force has developed implementation strategies and tactical plans that target home users, small businesses, large enterprises, schools and institutions of higher education, and state and local governments. Recognizing that we all have a role to play, each constituency has provided practical steps to increase awareness, accountability, and understanding to take action to manage the risks we face in today's constantly changing environment.

Task Force Co-Chairs:
- Dan Caprio, Chief of Staff to Commissioner Orson Swindle, Federal Trade Commission
- Ty Sagalow, Worldwide Corporate Product Development, Deputy Chief Underwriting Officer and DBG-Vice President, American International Group and COO, AIG eBusiness Risk solutions.
- Howard Schmidt, Vice President and Chief Information Security Officer, E-Bay, Inc.

The U.S. Chamber of Commerce serves as the Task Force Secretariat. The Task Force Co-Chairs thank Andrew Howell, Vice President for Homeland Security, and Scott Algeier, Manager for Homeland Security, both at the U.S. Chamber of Commerce, for their significant contributions to this report.

PROBLEMS and CHALLENGES

- Although the Internet has increased communication and productivity has provided businesses with access to new markets, it has also given hackers, thieves, disgruntled employees, fraudsters, and other criminals new opportunities to cause economic and social damage on a broader scale and has created new potential weapons of terrorism, more quickly than ever before.

- Generally, many private enterprises, public entities, and home users lack the resources to adequately manage cyber security risk.

- A large number of entrepreneurs and home users are not aware of how their individual cyber security preparedness affects security overall.

- Internet users must be made aware of the importance of sound cyber security practices and given more user-friendly tools to implement them.

RECOMMENDATIONS and NEXT STEPS

Small Businesses

- Develop and distribute a cyber security guidebook for small businesses and encourage the development of market-based incentives such as insurance and risk profile analysis that reward small businesses that enhance their cyber security preparedness.

Home Users

- Support, promote, and launch a national public service campaign on cyber security.

- Develop a cyber security tool kit for home users.

- Work with the Internet Service Provider (ISP) communities to identify ways to use their access to their customers to promote cyber security.

Large Enterprises

- Create and implement, in September, 2004, in partnership with DHS, a series of regional homeland security forums for CEOs of large enterprises. A portion of the program should highlight the roles of CEOs in cyber security.

- Begin, in July 2004, a direct mail campaign to C-Suite executives of the 10,000 largest companies in America to provide senior corporate executives with key messages and activities that are necessary for enterprisewide cyber security.

- Designate September 2004 as Cyber Security Month, and market to CEOs of large enterprises the importance of focusing on cyber security and participating in the DHS CEO regional homeland security forums.

- Distribute and raise awareness of the cyber risk management tools being developed by the Cyber Security Summit's Corporate Governance Task Force.

K-12 Schools and Higher Education

- Inventory, catalogue, and share best practices on raising cyber security awareness to home users, large enterprises, small businesses, K—12 schools and institutions of higher education, and state and local governments.

- Partner with education groups, school boards, superintendents, teachers, and colleges and universities to develop and distribute materials to school children and institutions of higher education that raise awareness of appropriate cyber security behavior.

- Provide cyber security and ethics curricula and explore opportunities for introducing awareness content as part of courses.

- Consider replicating the DHS Homeland Security CEO Forums for university presidents. A portion of the program should highlight the roles of university presidents in cyber security.

State and Local Government

- Develop, in conjunction with DHS, a Cyber Security Excellence Award to recognize teams, rather than individuals, at the state and local government levels.

- Create a Web-based training tool for state and local governments, as well as for businesses and home users, featuring a series of webcasts hosted by a variety of vendors, which are offering their services pro bono.

- Consider replicating the DHS Homeland Security CEO Forums for governors. A portion of the program should highlight the roles of governors and mayors in cyber security.

CONCLUSIONS

A major role for the Awareness Task Force has been, and will continue to be, to leverage existing awareness and outreach efforts and to initiate and enhance public-private partnerships. Promoting a secure cyberspace is the responsibility of every citizen, all levels of government (state, local, and federal), academia, and industries, regardless of size or sector. The list of key stakeholders involved in the solution is limitless, and therefore, the solution will only come as a result of coordinated, public-private partnerships.

The progress of the task force demonstrates the effectiveness of the public-private partnership model. Task force members believe that more can be accomplished by working together, rather than by working separately. The task force has catalogued existing best practices, developed strategies to market those practices to specific audiences, created incentive plans to ensure acceptance of those practices, contributed

to the development of a national advertising campaign, and developed a strategy to communicate to public and private CEOs across the country about the importance of cyber security and their role in enhancing it. Recognizing the role of our students, teachers, and schools and universities, a strategy has been created to bring cyber security directly to them. In addition, the task force has a team of dedicated state and local public servants who have taken shared responsibility in enhancing cyber security awareness in state and local government agencies throughout each state.

While these accomplishments are extensive, the task force recognizes that there is much more to do. The task force also acknowledges that there are other groups who are making positive contributions to cyber security awareness and encourages interested parties to comment on this report and join in the task force's efforts.

PUBLISHED BY THE U.S. CHAMBER OF COMMERCE • APRIL 2004

uschamber.com

FIGHTING FOR YOUR BUSINESS

FEATURE

Protect Your Computers and Business

Chamber Unveils Free Resources

Just because you're a small business doesn't mean you're not vulnerable to a cyber attack. Virtually all small businesses retain customer lists, employee records, and credit card information on their computers, all of which are prime targets for online fraud, identity theft, and other security breeches.

To help businesses manage this information security challenge, the U.S. Chamber is offering several new resources to help firms protect their valuable information and the networks in which it is stored.

The first such product is a preliminary online cyber security guide written specifically for entrepreneurs who don't have technical expertise, yet need to protect their information. This guide is free at **www.cyberpartnership.org**. (Readers are encouraged to provide feedback to Andrew Howell at AHowell@uschamber.com. Feedback will help in finalizing the print edition of this guide, which is expected to be available soon.)

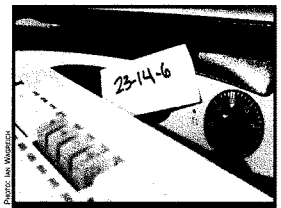


Photo: Ian Worpole

Don't leave your password lying around. Keep it secret and change it often.

"Unlike large enterprises that have large information technology departments, small businesses generally rely on someone who has many other responsibilities," says Andrew Howell, vice president for homeland security at the Chamber. "That's why it is so important for us to provide nontechnical information that allows companies to manage the risks they face online."

The Chamber partnered with the Internet Security Alliance, a respected publisher of information security guides, to create the initial online guide. "We wrote the online version only after talking to 100 small business owners about the technology issues that matter most to them," Howell adds. "Then we took it back to them for their comments and made revisions until their priorities were addressed."

To protect your information, recommended practices include not opening e-mail attachments from unknown senders, implementing firewalls, using anti-virus software to monitor your computers, and installing patches for software. The guide is easy to read and full of real-world examples of why information security is critical for small firms.

AIG eBusiness Risk Solutions (eBRS), a unit of the property and casualty subsidiaries of American International Group, Inc., and a global leader in identifying, evaluating, and managing network security-related risks, has agreed to provide credits on network security insurance policies for businesses that demonstrate that they adhere to the practices outlined in the guide and decrease their network security risk. eBRS understands that small businesses that implement the practices recommended in the guidelines should increase their security awareness and pose less of a network security risk.

Considering the vital information stored on your computers, information security provides a strong return on investment. "A cyber attack could mean giving away your competitive edge," says Howell. "But by taking the steps we recommend, you can manage your online risks effectively."

Reprinted by permission. uschamber.com. April 2004. Copyright 2004. U.S. Chamber of Commerce.

Mr. PUTNAM. Thank you, Mr. Howell.

Our next witness is Rodney Petersen. Mr. Petersen is policy analyst with EDUCAUSE, and the project coordinator for the EDUCAUSE/Internet2 Computer and Network Security Task Force. EDUCAUSE is a nonprofit association whose mission is to advance higher education by promoting the intelligent use of information technology. Mr. Petersen recently co-edited the book "Computer and Network Security in Higher Education." He was formerly the director of IT policy and planning in the office of the vice president and chief information officer at the University of Maryland. In addition, he was the founder of Project Nethics at the University of Maryland, a group whose mission is to ensure responsible use of information technology through user education and enforcement of acceptable use policies.

You are recognized for 5 minutes. Welcome to the subcommittee.

Mr. PETERSEN. Thank you, Mr. Chairman and members of the committee. I want to thank you for the opportunity to testify today regarding education and awareness for the cyber citizen. Later in my testimony, I have a video and some slides I would like to display, and with your permission, Mr. Chairman, I would like them added to the record.

By holding this hearing today, you signal the importance of education and awareness as part of an overall strategy to improve the cyber security of the Nation. The present challenges of cyber security require the establishment of a life-long culture of security from the cradle to the grave. And to emphasize something you said earlier, Mr. Chairman, in your opening remarks, education and awareness is a necessary but insufficient approach to protecting our Nation's cyber space.

I am here today, as you said, on behalf of the EDUCAUSE Internet2 Computer and Network Security Task Force. EDUCAUSE is a nonprofit association of nearly 2,000 colleges and universities. Internet2 develops and deploys advanced network applications and technologies for research and higher education, accelerating tomorrow's Internet.

EDUCAUSE and Internet2 established a Computer and Network Security Task Force in July 2000. The Security Task Force is coordinating its efforts on behalf of a diverse group of associations and types of educational institutions, including research universities, State colleges and universities, Land-Grant institutions, independent colleges and community colleges; some 4,000-plus colleges and universities across the United States.

The Security Task Force prepared the higher education contribution to the National Strategy to Secure Cyber Space. And more recently, we participated in the National Cyber Security Summit. I was a member of the Awareness Task Force that has been previously referenced, where I served as the co-chair for the Subcommittee on Schools and Institutions of Higher Education. Therefore, my testimony today will address education and awareness from kindergarten through college based upon the findings and recommendations of that subcommittee.

Colleges and universities have long been interested in supporting the efforts of elementary and secondary schools to improve awareness of students on issues such as cyber ethics and security. After

all, life-long habits are formed early, and the better we educate students about online safety in the K through 12 setting, the less we will be required once they arrive to college. Similarly, cyber security awareness facilitated by schools and colleges will benefit companies and government agencies that will eventually employ a new generation of technology-savvy and security conscious workers.

While at the University of Maryland, I was the founder of the group you previously described, Project NEThics. Every spring, the university hosts Maryland Day, which so happens to be this coming weekend, and we invite members of the local community to come onto the College Park campus for family fun and educational activities. One year, Project NEThics, in partnership with our Prince Georges County computer forensics unit, hosted a computer lab where we invited children and their parents to participate in activities designed to increase their awareness for online safety. We talked to parents about the important role of adult supervision and watching their children's online activities and wanting to acquaint parents with the risks and benefits of computer use. And we left parents with literature, including an online safety pledge provided by the Center for Missing and Exploited Children.

Project NEThics also works closely at the University of Maryland with the College of Education to develop seminars for teachers and school media specialists on cyber ethics and security. This summer, the university will host a conference entitled "Cyberethics, Cybersecurity, and Cybersafety for Professional Educators."

The Consortium on School Networking is a national nonprofit organization whose mission is to advance the K through 12 education community's capacity to effectively use technology to improve learning. COSN is currently working to help superintendents, chief technology officers of local school districts better integrate effective security practices into district management, operations, and the user experience.

And CyberSmart is a nonprofit organization that develops and provides curricula and training programs for teachers, school administrators, and students.

The EDUCAUSE/Internet2 Computer and Network Security Task Force has been pursing efforts to increase education and awareness in higher education. To this end, we have developed a working group that has identified a set of target audiences, among them including executives, all users relevant to this panel, members of the information assurance team, users of business systems, IT staff, faculty staff, students, and guests. Individuals interact with technology differently depending on their specific roles or responsibilities and the educational levels as well as cultural influences may vary. Therefore, education awareness is often customized to meet the target population. For example, at this time I would like to show you an awareness video developed for students at the University of Virginia.

Mr. PUTNAM. We have to keep it short.

[Video presentation follows:]

Student. When I go to UVA——

Student. I want to open e-mail attachments from strangers and get a virus.

Student. I want to post obscene messages on the Internet.

Student. Commit fraud using someone else's online identity.

Student. I want to run a business from my UVA personal Web page.

Student. I want to share my address and phone number——
Student. My password——
Student. My private fantasies with faceless creeps on the Net.
Student. When I go to UVA——
Student. When I go to UVA, I want to leave my e-mail open so strangers can read my incoming messages and answer them.
Student. Filing a copy I lost by pirating music and posting it on the Web.
Student. Harass people by sending threatening e-mails or chain letters or pornographic URLs.
Student. I want to hack into government computers and go to Federal prison.

[End of video presentation.]

Mr. PETERSEN. So I think the video underscores the need for messages that are creative and targeted toward the audience they are intended to address.

Because of time, I am going to skip over some further slides here that have examples of posters. But the one that is currently before you is a campaign where the slogan is "Passwords are like underwear" and some of the themes are "change yours often," "don't leave yours lying around," "don't share with a friend," "the longer the better," "be mysterious." And you can get the point that you have to reach students where they are and humor is a key ingredient.

Let me just say one thing and then I will conclude by talking about Cyber Security Day. Several colleges and universities did recently observe the Cyber Security Day, and we expect a number of campuses to plan activities during the week of October 31st to observe the next Cyber Security Day.

In conclusion, first, the improvement of cyber security is needed, and we need to see support both from the public and the private for what is happening in our schools and institutions of higher education. Second, the baseline information that is required of all users must be kept to a minimum. Third, there should be consistency in the basic awareness messages. And finally, our efforts to increase awareness and education regarding cyber security must happen in parallel to the development of more secure technologies. Thank you.

[The prepared statement of Mr. Petersen follows:]

Testimony and Statement for the Record

Rodney J. Petersen
Policy Analyst and Security Task Force Coordinator
EDUCAUSE

Hearing on
"Protecting Our Nation's Cyber Space:
Educational Awareness for the Cyber Citizen"

Before the
Subcommittee on Technology, Information Policy, Intergovernmental
Relations and the Census
Committee on Government Reform
United States House of Representatives

April 21, 2004
2154 Rayburn House Office Building

Mr. Chairman and members of the committee, thank you for the opportunity to testify today regarding education and awareness for the cyber citizen. Educational institutions, from kindergarten through college, are familiar with the importance of education and are actively preparing citizens who will contribute to the information economy. I am especially pleased that by holding this hearing you recognize the importance of education and awareness as part of an overall strategy to improve the cyber security of our Nation. The present challenges of cyber security require the establishment of a life-long culture of security from the cradle to the grave.

I must stress at the outset, however, that education and awareness will not be enough. The driver of an automobile must understand the rules of the road and be trained to drive safely. However, if the car is not manufactured for safety or the road is not appropriately engineered and professionally maintained, no amount of driver safety education will prevent accidents. Similarly, education and awareness are a necessary but insufficient approach to protecting our nation's cyberspace. I believe that the series of hearings that you held during the fall and the subsequent work of the Corporate Information Security Working Group appropriately recognizes that cyber security is a multifaceted problem requiring diverse and complementary solutions.

EDUCAUSE and Internet2

I am here today on behalf of the EDUCAUSE/Internet2 Computer and Network Security Task Force <www.educause.edu/security/task-force.asp>.

EDUCAUSE <www.educause.edu> is a nonprofit association whose mission is to advance higher education by promoting the intelligent use of information technology. The current membership comprises nearly 1,900 colleges, universities, and education organizations, including more than 170 corporations. EDUCAUSE has offices in Boulder, Colorado, and Washington, D.C.

Internet2 <www.internet2.edu> develops and deploys advanced network applications and technologies for research and higher education, accelerating the creation of tomorrow's Internet. Led by more than 200 U.S. universities and working with industry and government, Internet2 recreates the partnerships among academia, industry, and government that helped foster today's Internet in its infancy.

Computer and Network Security Task Force

EDUCAUSE and Internet2 established the Computer and Network Security Task Force in July 2000. The Task Force is working to improve awareness among the EDUCAUSE and Internet2 memberships and throughout higher education. The Security Task Force actively promotes effective practices and solutions for the protection of information assets and critical infrastructures. The Security Task Force is coordinating its efforts on behalf of institutions of higher education with the support of the Higher Education Information Technology Alliance <www.heitalliance.org> whose members include the American Council on Education, Association of American Universities, National Association of State Universities and Land-Grant Colleges, American Association of State Colleges and Universities, National Association of Independent Colleges and Universities, and the American Association of Community Colleges.

National Strategy to Secure Cyberspace

The Security Task Force prepared the *Higher Education Contribution to the National Strategy to Secure Cyberspace*. The *National Strategy* encourages colleges and universities to secure their cyber systems by establishing some or all of the following as appropriate:

- one or more Information Sharing and Analysis Centers to deal with cyber attacks and vulnerabilities;
- an on-call point of contact to Internet service providers and law enforcement officials in the event that the school's IT systems are discovered to be launching cyber attacks;
- model guidelines empowering chief information officers to address cyber security;
- one or more sets of best practices for IT security; and,
- model user awareness programs and materials.

The Security Task Force was also well represented at the recent National Cyber Security Summit and participated on each of the five task forces. I was a member of the Task Force on Awareness for Home Users and Small Businesses. The scope of the task force was expanded to include large enterprises and state and local government, as well as schools and institutions of higher education. I served as the co-chair for the Subcommittee on Schools and Institutions of Higher Education. Therefore, my testimony today will address education and awareness from kindergarten through college based upon the findings and recommendations of the subcommittee.

Elementary and Secondary Schools

Colleges and universities have long been interested in supporting the efforts of elementary and secondary schools to improve the awareness of students on issues such as cyber ethics and security. After all, life-long habits are formed early—the better we educate students about online safety in the K-12 setting, the less we will need to do so when they arrive at college. Similarly, cyber security awareness facilitated by schools will benefit companies and government agencies that will eventually employ a new generation of technology-savvy and security-conscious workers.

There is a legion—54 million strong—of young people who can lead the nation in secure and trustworthy computing. Many will enter a high-tech-enabled workforce during this decade. The U.S. Department of Education counts 53.8 million children (K–12) in our nation's public and private schools. Together, these students have at least 75 million parents or household caregivers. A systematic program for teaching secure and trustworthy computing skills K–12, therefore, has the opportunity to "trickle up" and reach at least 125 million people. This is nearly the number of Americans—146 million—who currently use the Internet. Because of this trickle-up phenomenon, investment in cyber security education and Internet-skills training will begin to pay off immediately.

Our current notion of cyber security must start in kindergarten

In the past, cyber security has been the domain of computing professionals and law enforcement agencies. But with the mainstreaming of the Internet, cyber security is now a shared responsibility of adults and tech-savvy children alike.

At this juncture, young people must be taught effective cyber skills from the moment they are first allowed to touch a computer mouse. As soon as children enter kindergarten, they are capable of embracing age-appropriate, responsible computing practices. Their parents and older siblings will be challenged to catch up with them.

Developing good habits young is essential to building a positive culture of cyber security

Once habits are formed, they are difficult to break regardless of age. Whether the habit is weight control, fingernail biting, or poor information security practices, it is better to mold positive behavior than to modify negative behavior. Research in youth crime prevention suggests that intervention with at-risk children at a very young age curbs the onset of

delinquent behavior by up to 80 percent. Hence, it's reasonable to infer that positive cyber skills must be introduced at the youngest possible age. For adults, this means making it more convenient and easier to "do the right thing" and making each adult an individual stakeholder in the practice of secure cyberspace habits.

Project NEThics at the University of Maryland

While at the University of Maryland, I was the founder of Project NEThics <www.umd.edu/NEThics>—a group dedicated to the promotion of legal and ethical use of computing resources. Every spring, the University hosts Maryland Day, inviting members of the local community onto the College Park campus for family fun and educational activities. One year, Project NEThics in partnership with the Prince George's County Computer Forensics Unit set up a computer lab where we invited children along with their parents to participate in activities designed to increase the awareness of children for online safety. We also talked with parents to encourage adult supervision of their children's online activities and to acquaint them with the benefits and risks of networked computer use. We provided literature to parents, including an online safety pledge provided by the Center for Missing and Exploited Children.

Project NEThics also collaborates with the College of Education to develop seminars for teachers and school media specialists on cyber ethics and security. This summer, the university will host a conference entitled "Cyberethics, Cybersafety, and Cybersecurity for Professional Educators" <www.edtechoutreach.umd.edu/cyberethicsseminar2004.html>. The conference will address implications for classroom and higher education technology instruction. The program flyer notes:

> Unfortunately, while the teaching of technology processes and skills has been handed to the classroom teacher, most educators lack the knowledge and up-to-date information related to security issues. Teachers, in many instances, model incorrect protocol and behavior to their students. Not only does this increase the risks to the security of the teacher's own classroom and local school system's information systems, but it also increases the chances that students will follow their behaviors.

Consortium on School Networking (COSN)

COSN <www.cosn.org> is a national non-profit organization whose mission is to advance the K-12 education community's capacity to effectively use technology to improve learning through advocacy, policy and leadership development. COSN members represent school districts, state and local education agencies, nonprofits, companies and individuals who share the organization's vision.

COSN, in partnership with Mass Networks Education Partnership (Mass Networks), is developing a program – Cyber Security for the Digital District - to provide schools and school districts with vital information on education networks in order to ensure the privacy and the security of data within their systems. The three-year project combines both government and private sector support to help the superintendents and chief technology officers of local school districts better understand how to deal with cyber security. COSN is creating materials to raise awareness of school administrators and to help them raise the awareness of their community. COSN is creating tools that K–12 leaders can use, developing a Web site for dissemination and sharing of information, and planning training workshops and other activities. More information about the project, Cyber Security for the Digital District, is available at securedistrict.cosn.org.

CyberSmart!

CyberSmart! <www.cybersmart.org> provides curricula and training programs teaching secure, responsible, and effective computer and Internet use. The CyberSmart! K–8 Curriculum is a free "owner's manual" for students' safe, responsible, and effective use of computers and the Internet. It complements all academic subjects, emphasizing character building and skill-based decision making related to successful technology use.

Developed by professional educators, curriculum experts, and Internet industry innovators, the CyberSmart! Curriculum meets the needs of school administrators, teachers and students by

- enabling schools to successfully execute technology plans;
- addressing the social, legal, and ethical issues associated with technology use;
- supporting teachers in their efforts to successfully integrate technology into the classroom;
- providing students with the tools they need to navigate the Internet safely, sensibly, and effectively; and,
- involving families.

CyberSmart! proposes the following action agenda for securing the nation's digital resources:

- Federal, state, and local governments must participate in funding for cyber security education programs, particularly those involving America's 50 million K–12 students.

- Industry, government, and other interested parties must engage in coordinated public awareness campaigns that stress the value of individuals—both adults and young people—to communicate and share information responsibly and securely online.

- The core group of industry trade associations and nonprofits involved with promoting Internet education must expand. Now is the time to reach out to outlying trade groups to enlist broad-based industry support for cyber security education. Organizations representing securities, banking, health care, media, education, and other industries all have significant roles to play.

- The high-tech industry must implement practical cyber security technologies that combine ease-of-use convenience, low cost to widespread deployment, and respect for privacy.

- Both the private sector and government should engage in research to determine the best information security educational practices.

- Schools must teach secure, responsible computing skills as part of a mandated component of K–12 curriculum nationwide.

- The U.S. Department of Education and states must prioritize teacher training for cyber skills, including information security skills, in order to effectively leverage technology in support of student achievement and to prepare students to enter the technology-enabled workforce.

- The benefits associated with teacher training must be communicated to the senior education administrators who allocate and administer funds.

- The essential role of librarians as highly skilled navigators of an increasingly complex web of data sources must be acknowledged and support provided to librarians—in schools, universities, and public and private settings—to strengthen the use of the Internet to sustain the integrity of academic achievement, life-long learning, and the democratic processes.

Colleges and Universities

The EDUCAUSE/Internet2 Computer and Network Security Task Force received a grant from National Science Foundation to identify and implement a coordinated strategy for computer and network security for higher education. The following strategic goals have been identified:

- **Education and Awareness.** To increase the awareness of the associated risks of computer and network use and the corresponding responsibilities of higher education executives and end users of technology (faculty, staff, and students), and to further the professional development of information technology staff.

- **Standards, Policies, and Procedures.** To develop information technology standards, policies, and procedures that are appropriate, enforceable, and effective within the higher education community.

- **Security Architecture and Tools.** To design, develop, and deploy infrastructures, systems, and services that incorporate security as a priority; and to employ technology to monitor resources and minimize adverse consequences of security incidents.

- **Organization and Information Sharing.** To create the capacity for a college or university to effectively deploy a comprehensive security architecture (people, process, and technology) and to leverage the collective wisdom and expertise of the higher education community.

Security Task Force Education and Awareness Working Group

The Security Task Force has created an Education and Awareness Working Group to identify and take steps to implement and publicize various methods by which awareness of information technology security issues are raised among university and college computer and network users, administrators, and executives. The working group has identified categories of audiences for which to target education and awareness:

- **Executives:** The first item in the "Framework for Action" developed by the Security Task Force in 2002 was to "make IT security a higher and more visible priority in higher education." As reported in the Corporate Governance Task Force report issued earlier last week, chief executives and governing boards must assume direct responsibility for securing their computer networks.

- **All Users:** Raising the consciousness of the end users of networked computers is a goal higher education holds in common with government and industry. The EDUCAUSE/Internet2 Security Task Force is proud to affiliate with the National Cyber Security Alliance to assist them in the development of a broad national campaign for home users. A baseline of information is needed by everyone, and we are striving to keep messages consistent across groups that are developing awareness materials.

- **Members of Information Assurance (IA) Teams:** Information security is no longer just the concern of the IT security officer. Auditors, risk managers, legal counsel, business officers, police and public safety officers, chief information officers, data stewards, and chief security officers play critical roles in an enterprise information security program. The training and professional development needs of IA team members are significant and must be supported on an ongoing basis.

- **Users of Business Systems:** Certain individuals are granted privileges to access critical systems that contain sensitive data. In higher education, administrative computer systems typically contain data related to personnel, student information and education records, grants and contracts, financial information, and other confidential or proprietary information. Special care must be taken to safeguard confidential information and records.

- **Information Technology Staff:** A skilled IT workforce is critical to efforts to protect information assets and critical infrastructures. Employees responsible for system administration, network operations, database administration, Web development, and applications development require continual training and professional development to keep up with the growing demands for security. Help desk personnel must also understand cyber security best practices so they can effectively convey security awareness messages to end users.

- **Faculty, Staff, Students, and Guests:** Individuals interact with technology differently depending on their specific roles or responsibilities within a college or university. Educational levels as well as cultural influences may vary among audiences. Therefore, education and awareness should be customized to address target populations in academic or residential settings.

Campus security awareness efforts

A number of campuses have instituted cyber security awareness programs. Techniques range from distributing note cards and flyers and displaying posters to video performances, skits, presentations and seminars, and letters from campus officials. Increasingly, efforts are made to convey important security and policy information to students at the time of new student orientation. In a few cases, institutions have implemented online quizzes or mandatory information sessions as a condition for obtaining access to the campus network.

A listing of college and university security awareness initiatives is available at www.educause.edu/security/resources/awareness.asp.

Cyber Security Day

Colleges and universities across the country recently planned security education and awareness events between March 29 and April 2, 2004, to help promote Cyber Security Day (April 4, 2004). The Security Task Force fulfilled one of the recommendations of the Awareness Task Force report by encouraging and supporting events at higher education institutions that observe Cyber Security Day (see the appendix). The Education and Awareness Working Group of the Security Task Force is building momentum toward the next Cyber Security Day on October 31, 2004. We expect a number of campuses to plan activities during the week prior to the day or throughout the month of October.

National Information Assurance Training and Education Center (NIATEC)

NIATEC <www.niatec.info> is a consortium of academic, industry, and government organizations developed to improve awareness, training, and education standards in Information Assurance. It is the federally designated cornerstone for essential education and training components of a strong Information Assurance initiative. The NIATEC is associated with Idaho State University Center of Academic Excellence. The Centers of Academic Excellence and NIATEC are components of a plan to establish a federal cyber corps to defend against cyber-based disruption and attacks. The national plan proposes to address the increasing vulnerability to such attacks; emphasizes the role of academia in cyber defense; and calls for active partnerships among private sector, academia, and governmental organizations. Key to building such a cyber corps is the implementation of robust graduate and undergraduate curricula in Information Assurance.

Conclusion

Tremendous progress has been achieved but much work remains to be done. First, if the improvement of cyber security is indeed a national priority, as we think it should be, then we need to see an infusion of public and private support flowing to our schools and institutions of higher education.

Second, the baseline information required by all users of networked computers to operate safely online must be kept to a minimum to accommodate a diverse range of learning styles and educational levels.

Third, there should be consistency in basic awareness messages whether presented to kids in schools, adults in college, employees in the workplace, or home users. The messages should be simple, straightforward, and easy to understand.

Finally, efforts to increase awareness and education regarding cyber security and ethics must happen in parallel to the development of more-secure technologies.

Schools and institutions of higher education must also develop more-secure technical architectures and provide security-related services, and the IT vendor community must strive to improve the security of hardware and software widely used in open, collaborative educational environments.

Appendix

FOR IMMEDIATE RELEASE

Contacts:
Rodney Petersen
Policy Analyst and Security Task Force Coordinator
EDUCAUSE
rpetersen@educause.edu
202-331-5368

Michelle Pollak
Media Relations Manager
Internet2
mpollak@internet2.edu
202-331-5345

****
COLLEGES AND UNIVERSITIES RECOGNIZE CYBER SECURITY DAY WITH CAMPUS EVENTS
****

Washington, D.C., March 26, 2004—Setting your clocks forward or back for daylight saving time and replacing the batteries in smoke detectors are rituals repeated every spring and fall. Similarly, the National Cyber Security Alliance (<http://www.staysafeonline.info>) established April 4, 2004, as Cyber Security Day to raise awareness about Internet safety and computer security issues. Colleges and universities across the country are planning security education and awareness events between March 29 and April 2 to help promote Cyber Security Day.

Rutgers University is encouraging its students, faculty, and staff to "Spring Ahead to Security!!" on a Web site devoted to National Cyber Security Day (<http://rusecure.rutgers.edu/cybersecurityday/>). In addition to campus presentations on identity theft, the Web site suggests steps that the campus community can take "in the quest for better security" such as using antivirus software and keeping it up-to-date weekly, exercising caution when opening e-mail attachments, selecting hard-to-guess passwords and keeping them private, backing up important files, downloading and installing operating system update patches, avoiding risks of file sharing, using a password-protected screensaver, locking up computers when not in use, and using a firewall to protect computers from intruders. Lance D. Jordan, director of Information Protection and Security at Rutgers, said, "Providing personal information over the Internet has become a risky proposition, and our

community needs to be aware of the risks and protective measures that are easily practiced to surf cyberspace safely."

The George Mason University IT Security Office is featuring a week-long lineup of lunchtime presentations promoting cyber security awareness (<http://security.gmu.edu/nationalcybersecurityday.html>). Topics include network security and denial-of-service attacks, desktop strategies to secure your cyberspace, file sharing, and more. Joy Hughes, CIO and vice president for Information Technology at George Mason, believes that it is important for faculty, staff, and students to have a role in planning security awareness events. She said, "Our workshop content is determined by consulting with the members of the university-wide Systems Administrators' Leadership Team; the Security Review Panel; and other faculty, staff, and student groups working to improve security."

The University of Arizona developed a series of humorous posters to reinforce messages that are designed to prevent identity theft and other consequences of improperly secured computers (<http://security.arizona.edu/posters.html>). The slogan for the Arizona campaign emphasizes that the key to security is derived from the word itself: sec-U-R-IT-y. In other words, "You Are It!" Kelley Bogart, an analyst in the Information Security Office at the University of Arizona, is co-chair of the Education and Awareness Working Group of the EDUCAUSE/Internet2 Computer and Network Security Task Force that is encouraging higher education institutions to hold events in conjunction with Cyber Security Day. "We want information technology users to understand that they are part of the solution. Although good security should be practiced every day throughout the year, we believe there is benefit in colleges and universities participating in a national campaign that focuses everyone's attention on the critical problems associated with information security," Bogart said.

Shirley Payne, director of Security Coordination and Policy in the Office of Information Technologies at the University of Virginia and a member of the Security Task Force Education and Awareness Working Group, remarked, "Think of this scenario: The CEO of a major corporation is hearing about cyber security at work. When she gets home, her young son shows her a poster he's crafted to submit to a cyber security poster contest. Turning on the TV, she sees a public service announcement concerning the need to secure her home computer, and driving to work the next day, she hears an NPR interview on the great successes of higher education in reducing the impact of viruses and worms." Payne has published on the topic of developing campus-wide security education and awareness in *EDUCAUSE Quarterly* ([PDF 57 KB]

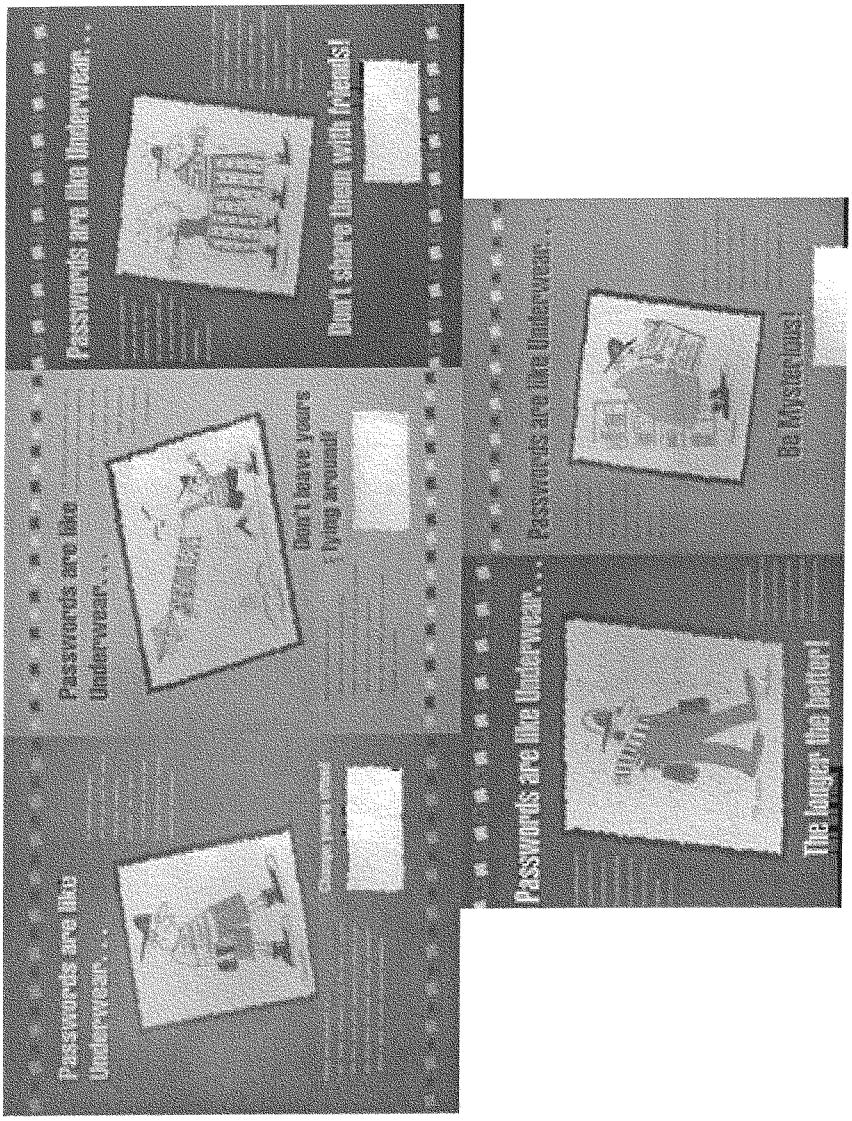
<http://www.educause.edu/ir/library/pdf/EQM0347.pdf>) and in a new book entitled "Computer and Network Security in Higher Education." The University of Virginia is also part of the Virginia Alliance for Secure Computing and Networking (VASCAN) that has compiled a collection of security tools and best practices from Virginia universities (<http://www.vascan.org/categories/security_awareness.html>).

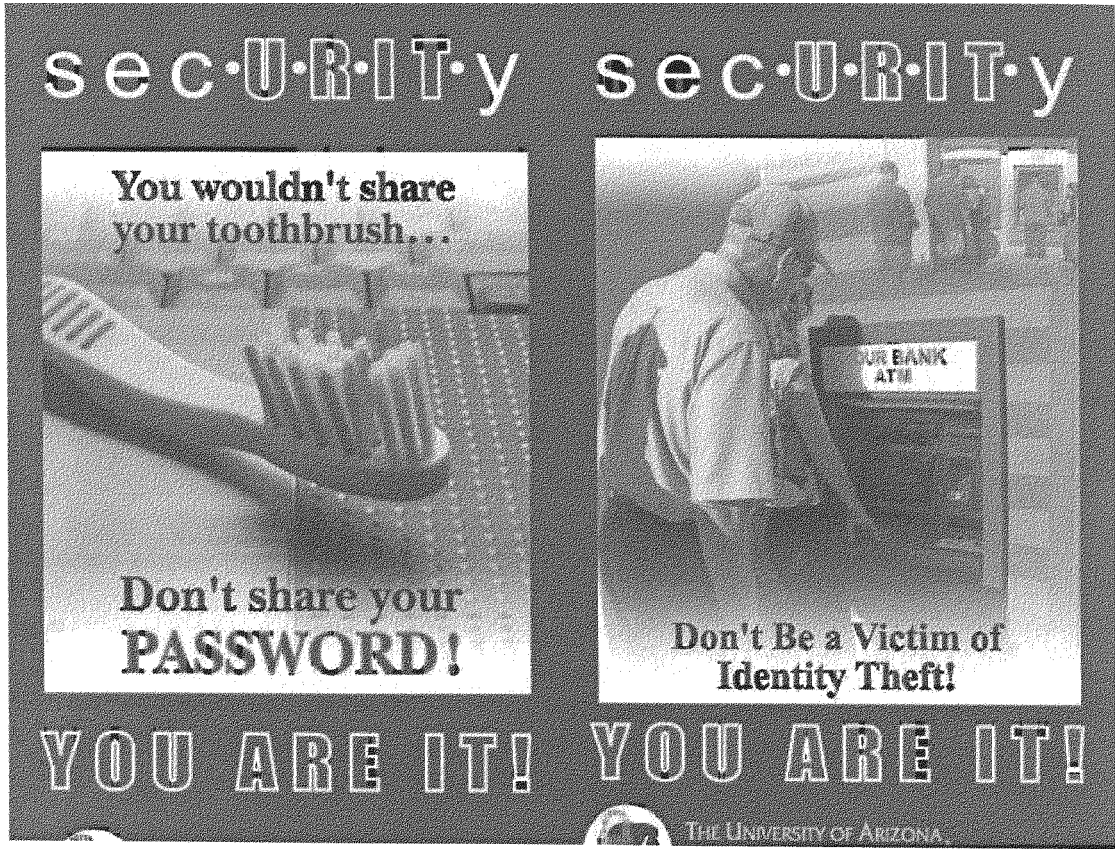
The EDUCAUSE/Internet2 Security Task Force is a sponsor of the National Cyber Security Alliance and supports efforts to promote online safety and create security awareness among the general public. The Security Task Force also contributed to the Awareness and Outreach Task Force report released on March 18 by the National Cyber Security Partnership (<http://www.cyberpartnership.org/>). The Security Task Force is fulfilling one of the recommendations of the report by encouraging and supporting events at higher education institutions that observe Cyber Security Day. The next Cyber Security Day will be on October 31, 2004.

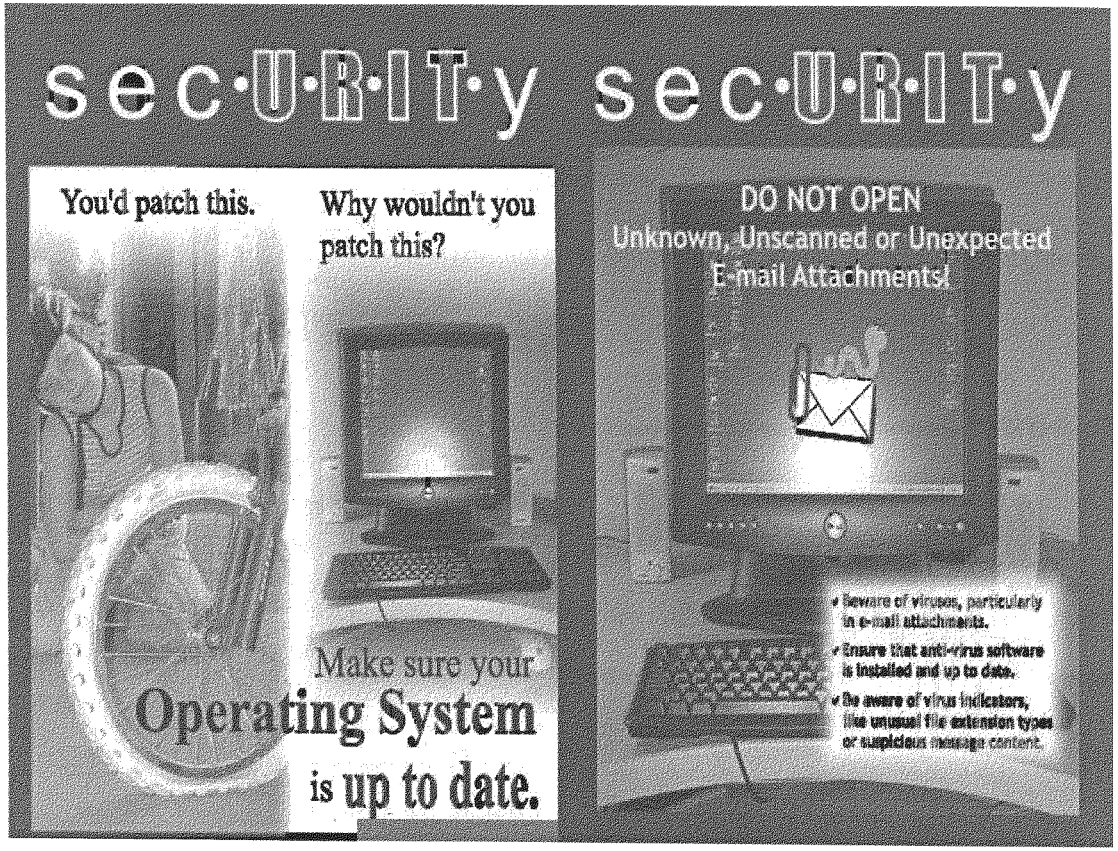
****

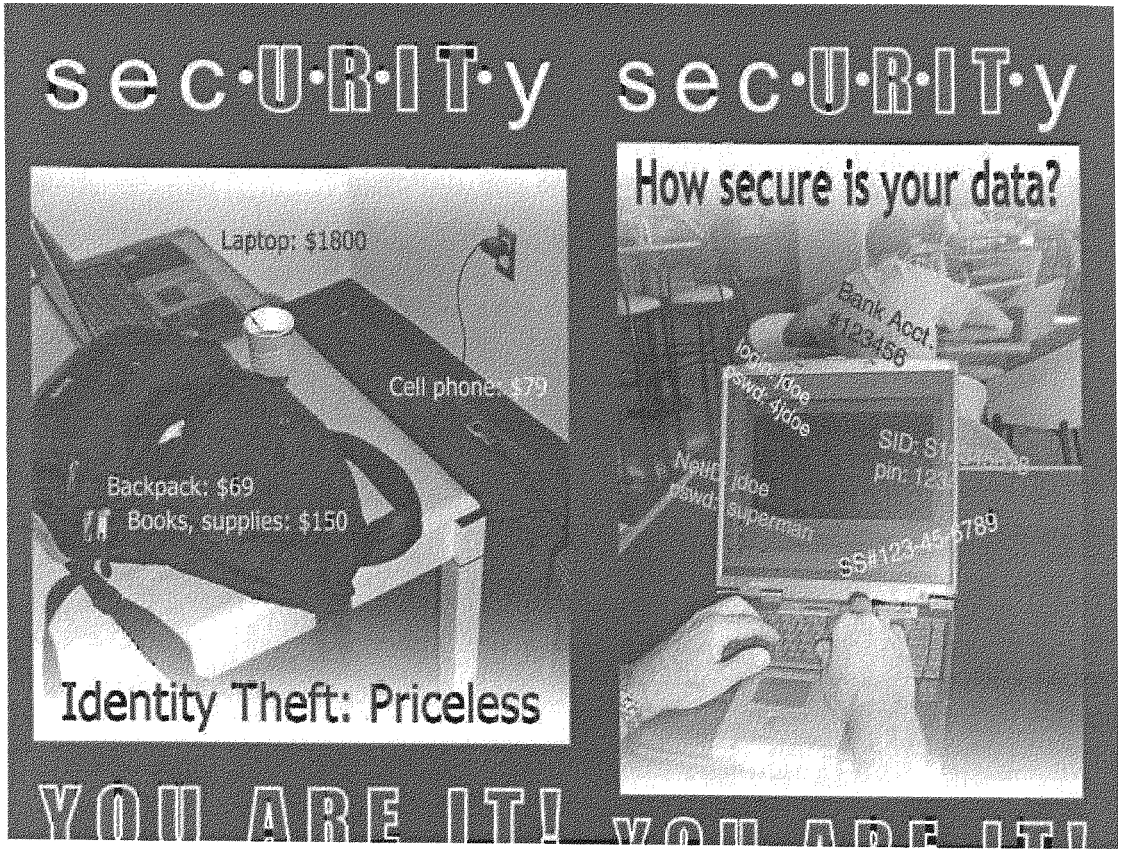
ABOUT EDUCAUSE
EDUCAUSE is a nonprofit association whose mission is to advance higher education by promoting the intelligent use of information technology. The current membership comprises nearly 1,900 colleges, universities, and education organizations, including more than 170 corporations. EDUCAUSE has offices in Boulder, Colorado, and Washington, D.C. Learn more about EDUCAUSE at <http://www.educause.edu/about/>.

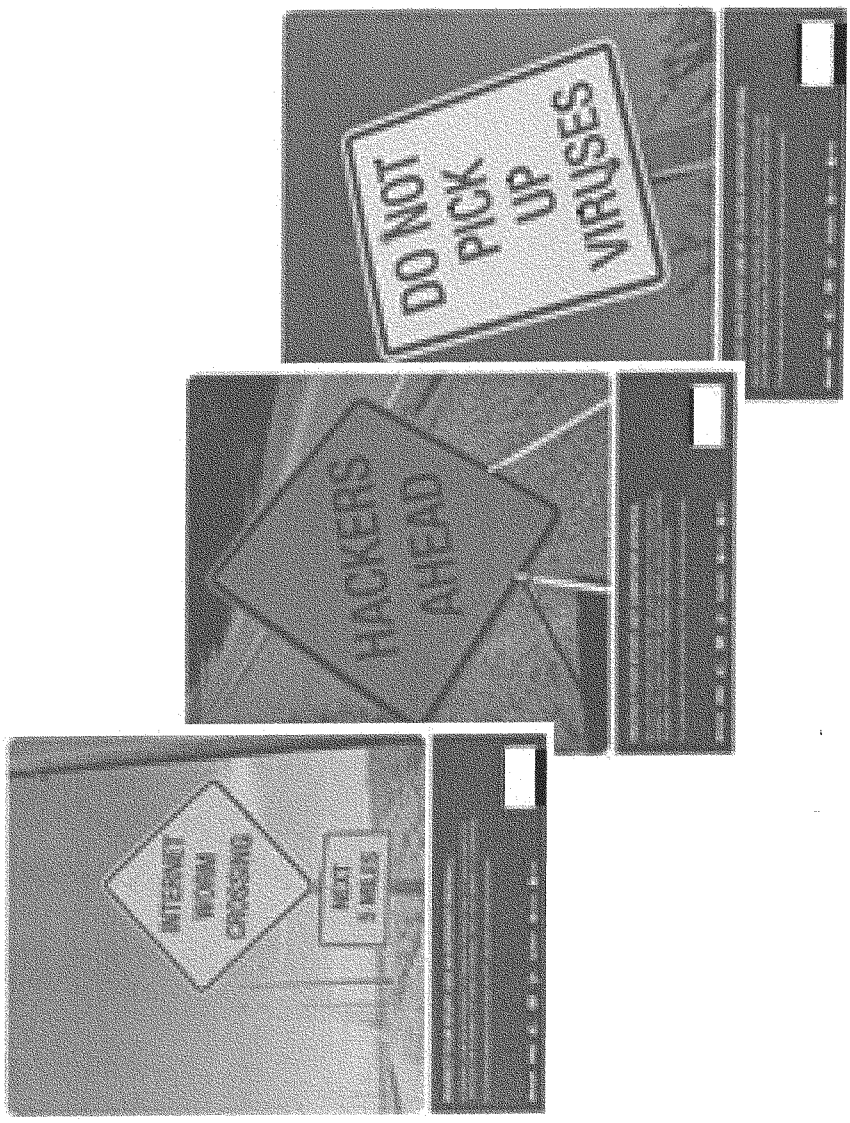
ABOUT INTERNET2
Led by more than 200 U.S. universities, working with industry and government, Internet2 develops and deploys advanced network applications and technologies for research and higher education, accelerating the creation of tomorrow's Internet. Internet2 recreates the partnerships among academia, industry, and government that helped foster today's Internet in its infancy. For more information about Internet2, see <http://www.internet2.edu>.


Passwords are like Underwear...
Change them often!
Passwords are like Underwear...
Don't leave yours lying around!
Passwords are like Underwear...
Don't share them with friends!
Passwords are like Underwear...
The longer the better!
Passwords are like Underwear...
Be Mysterious!


sec·U·R·I·T·y
You wouldn't share your toothbrush...
Don't share your PASSWORD!
YOU ARE IT!
sec·U·R·I·T·y
Don't Be a Victim of Identity Theft!
YOU ARE IT!
THE UNIVERSITY OF ARIZONA


sec·U·R·I·T·y
You'd patch this.
Why wouldn't you patch this?
Make sure your
Operating System
is up to date.
sec·U·R·I·T·y
DO NOT OPEN
Unknown, Unscanned or Unexpected
E-mail Attachments!
• Beware of viruses, particularly in e-mail attachments.
• Ensure that anti-virus software is installed and up to date.
• Be aware of virus indicators, like unusual file extension types or suspicious message content.


sec·U·R·I·T·y
sec·U·R·I·T·y
Laptop: $1800
Cell phone: $79
Backpack: $69
Books, supplies: $150
Identity Theft: Priceless
How secure is your data?
Bank Acct.
$123456
pin: 123
SS#123-45-6789
YOU ARE IT!


INTERNET
ROOM
OPEN 24 HRS
HACKERS
AHEAD
DO NOT
PICK
UP
VIRUSES

Mr. PUTNAM. Thank you, Mr. Petersen.

Our final witness on the second panel is Douglas Sabo. Mr. Sabo is appearing today in his role as a member of the board of directors of the National Cyber Security Alliance. He is also the director of government and community relations for McAfee Security. In that role, Mr. Sabo addresses domestic and international public policy issues affecting the company and oversees the company's corporate citizenship activities. McAfee Security, headquartered in Santa Clara, CA, is a leading supplier of security and intrusion protection solutions for e-businesses. Mr. Sabo also serves as chair of the Security Working Group of the Business Software Alliance and co-chair of Department of Commerce's International Outreach Subcommittee of the Economic Security Working Group.

You are recognized for 5 minutes.

Mr. SABO. Thank you. I am not sure how I am going to followup a discussion of underwear. [Laughter.]

Good afternoon, Mr. Chairman, Ranking Member Clay, and members of the subcommittee. My name is Douglas Sabo. I am a member of the board of directors of the National Cyber Security Alliance and I testify this afternoon on behalf of that organization. And as you mentioned, Mr. Chairman, I am also director of government and community relations for McAfee Security. I join with my colleagues on this panel in thanking you for your personal leadership on the cyber security issue, both through your series of cyber security hearings as well as your working groups with industry. I also commend your staff for being first-rate on all of these issues.

As you have heard others mention, the National Cyber Security Alliance [NCSA], is a unique partnership among the Federal Government, leading private sector companies, trade associations, and educational organizations, including all of the organizations testifying here today. Our fundamental purpose is to contribute to our Nation's overall cyber security by improving the behaviors of consumers, small businesses, and our youth from kindergarten to higher ed. And Mr. Chairman, we share your concerns about bombarding citizens with too many messages from too many sources. We hope that our partnership will contribute to avoiding that problem.

Others have already talked today about the overall challenge and the important role that these audiences do play. The NCSA strongly agrees with these assessments. And rather than reiterate this information, I would like to introduce you to initiatives that we hope will reach our three main audiences. First, for small businesses, the NCSA is developing cyber security tool kits to discuss vulnerabilities and threats as well as tips and steps for responding. These tool kits, which will be available in soft and hard copy, will include materials, guidebooks, and training programs on the cyber security essentials. We are in discussions with a number of organizations to develop and distribute these tool kits, including the Small Business Administration, InfraGard, the ISP community and others, and we hope to begin distribution by mid-June.

Second, we are focusing on educating our youth on cyber security practices to make sure the next generation of users is cyber secure. Through partnering with outside organizations such as EduCalls and CyberSmart!, we hope to develop and disseminate cyber secu-

rity curriculum to educators across the country. These materials already are developed for the K through 8 audience, with 9 through 12 pending. And to reach our youngest audience, the NCSA also supported a national poster contest in which students were asked to creatively depict the importance of cyber security. We plan to hold this contest again this fall.

Finally, I would like to use a couple minutes to focus on the consumer audience. Already the NCSA has launched our flagship Web site, www.staysafeonline.info, which received over 1 million hits in its first month alone. This site contains our top 10 cyber security tips, self-tests, tech talks, and more. In addition, we have held semi-annual National Cyber Security Days timed with Daylight Savings Time changes. While these have not been as successful as we had hoped, we are busy working to relaunch these this fall.

But what the NCSA is most excited about in the consumer area is what we hope will be the cornerstone of the NCSA effort, a multi-year national cyber security awareness campaign. This campaign, targeted at home users, will use public service announcements and other creative methods to raise awareness of the cyber security issue and steps people should take to protect themselves, and thus all of us. While our efforts certainly will depend on the resources we are able to raise for this campaign, we hope that our national cyber security awareness campaign will be on the level of many of those that I am sure you are familiar with, healthy lifestyles, wildfire prevention, drunk driving prevention, the importance of voting, drug abuse prevention, and terrorism emergency preparedness. These broad campaigns have imprinted our culture with a number of easily recognizable campaign catch phrases, such as, "Don't drink and drive," "Buckle Up," "Only you can prevent wildfires," and "Take a bite out of crime." Perhaps our effort will add a new one.

Are public awareness campaigns effective? We certainly believe they can be. Consider please the results of the Ad Council, a nonprofit organization that uses volunteer talent from the advertising and communications industries. Applications, for example, for Big Brothers, Big Sisters mentors increased by 75 percent in the first 8 months of their campaign. Destruction of our forests by wildfires has been reduced from 22 million acres to less than 4 million acres per year since their forest fire prevention campaign began. And safety belt usage rose from 14 percent to 79 percent since their safety belt campaign launched in 1985, saving an estimated 85,000 lives. With the proper resources, we believe the NCSA national awareness campaign can achieve the same level of success for cyber security behavior. It will not be a silver bullet, but together with all the other NCSA efforts as well broader initiatives to reduce vulnerabilities, improve security usability, expand R&D, and enhanced corporate governance, we can truly make a difference.

Mr. Chairman and members of the subcommittee, I thank you again for the opportunity to testify today. And I look forward to answering any questions you may have.

[The prepared statement of Mr. Sabo follows:]

Testimony of Douglas Sabo

Member, Board of Directors, National Cyber Security Alliance
Director, Government & Community Relations, McAfee Security

Before the
House Committee on Government Reform
Subcommittee on Technology, Information Policy, Intergovernmental Relations and the Census

"Protecting Our Nation's Cyber Space:
Educational Awareness for the Cyber Citizen"

April 21, 2004

Chairman Putnam, Vice Chairwoman Miller, Ranking Member Clay, members of the Subcommittee, I want to thank you for inviting me to testify today on the important topic of cyber security educational awareness initiatives. My name is Douglas Sabo, and I am a Member of the Board of Directors of the National Cyber Security Alliance (NCSA) as well as the Director of Government and Community Relations for McAfee Security, a provider of cyber security and intrusion prevention solutions based in Santa Clara, California. I am honored to be invited to be here today on behalf of the NCSA, and I look forward to joining my distinguished colleagues from government and industry alike to discuss with this Subcommittee the challenges of awareness and education in cyber security. Today's hearing on the cyber secure citizen is a timely and important topic, and on behalf of the National Cyber Security Alliance, I appreciate your willingness to examine the issue and highlight its importance.

The National Cyber Security Alliance is a unique partnership among the Federal government, leading private sector companies, trade associations and educational organizations. Through the NCSA's Web site, www.staysafeoneline.info, this partnership aims to educate Americans about the need for computer security and encourage all computer users to protect their home and small business systems. In its efforts, the NCSA has worked particularly closely with the National Cyber Security Division of the US Department of Homeland Security. Assistant Secretary for Infrastructure Protection Robert Liscouski and National Cyber Security Division Director Amit Yoran both have been extremely supportive of the NCSA's efforts.

Before I talk about the NCSA's initiatives, it is important to underscore why this issue of the cyber secure citizen is important.

Trends in Cyber Security: Why Education and Awareness are Important

In order to understand the increasing importance of education and awareness and the role of the consumer and small business, allow me to discuss two particular trends in cyber security:

1. Threats are Changing

The cyber security threat is changing. No longer are we in a world where cyber exploits take months to gain momentum around the globe. Today, the "exploit window" (or, the time from the discovery of a new vulnerability to the release of an attack exploiting that vulnerability) is rapidly shrinking. At the same time, these exploits or attacks are becoming more sophisticated, more aggressive and more prolific at a faster speed than ever before.

In recent attacks, the time taken for a threat to be created to exploit a vulnerability has been about three weeks. This is the time between when the vulnerability exploited by Lovsan/Blaster, for example, was announced and when Lovsan/Blaster itself was discovered. This timeframe is significantly down from the six months that elapsed before CodeRed took advantage of the vulnerability in Microsoft IIS. In parallel, the exploits themselves, once unleashed, are much more prolific and harmful. The Code Red and Nimda denial of service worms spread around the globe in a day or less. In January 2003, the Slammer worm infected over 5,000 servers around the world in under three minutes, and infected 90 percent of vulnerable systems worldwide in just 15 minutes.

2. Growing (False) Sense of Security

As these threats are changing, there is a concern that a growing false sense of security among many Internet users has emerged. In some ways, perhaps we have become victims of our own success.

In recent years, the public's attention to cyber security issues has risen dramatically, particularly as more and more Internet users transition to broadband connections. No longer is it unusual for us to hear about viruses and worms on the morning news or while gathered around the office water cooler. Most users (though not all) know it is critical to have anti-virus software. Many users (but certainly not all) also understand the importance of personal firewalls. But how do their practices compare to their understanding?

The National Cyber Security Alliance, in conjunction with AOL, has conducted a number of surveys on these questions. In a June 2003 study, 86 percent of users felt their computer was very or somewhat protected from online threats, with 76 percent having anti-virus software and 59 percent having personal firewall protection. Obviously, that leaves 24 percent without anti-virus software and 41 percent without firewall protection. But we must look more closely at those who do have those protections. According to our study, 62 percent of those with anti-virus software do not regularly update it, and 67 percent of those with firewall protection do not have properly and securely configured firewalls. While the number of those with anti-virus and firewall protection has risen dramatically, a majority of those with these protections is not practicing secure behaviors. There is a disconnect between beliefs and practice, and we fear a false sense of security is the result.

In light of these trends, the consumer and small business audience is a critical component, and one that would benefit from continued awareness and education initiatives. Of course, we aren't the only ones talking about this. The President's *National Strategy to Secure Cyberspace* itself acknowledges that awareness is a key component to ensuring our overall cyber security:

> Everyone who relies on part of cyberspace is encouraged to help secure the part of cyberspace that they can influence or control. To do that, users need to know the simple things that they can do to help to prevent intrusions, cyber attacks, or other security breaches. All users of cyberspace have some responsibility, not just for their own security, but also for the overall security and health of cyberspace. (*National Strategy to Secure Cyberspace*, pg 37, February 2003)

Our Response: National Cyber Security Alliance Initiatives

In response to these challenges, a coalition of companies, trade associations, organizations and government bodies came together to form the National Cyber Security Alliance (NCSA). The organizations sponsoring NCSA are diverse and bring a variety of expertise to the group. Industry representatives include: AOL, BellSouth, Cisco Systems, McAfee Security, Microsoft, RSA Security and Symantec. Trade associations include: Business Software Alliance, Cyber Security Industry Alliance, Information Technology Association of America, Internet Security Alliance and US Chamber of Commerce. Non-profit organizations include: CyberSmart!, EDUCAUSE, InfraGard and the Information Systems Security Association. Finally, government agencies include: US Department of Homeland Security (National Cyber Security Division), US Federal Trade Commission, Federal Bureau of Investigation and National Institute of Standards and Technology. We are actively looking for additional companies, organizations and government agencies to become sponsors of the NCSA.

This group of agencies, companies and organizations understands the important role that consumers, small businesses and our youth play in contributing to our overall cyber security. With that role in mind, the NCSA has created and developed a number of education and awareness initiatives addressing cyber security:

Initiative: National Cyber Security Awareness Campaign

First, as a cornerstone of our effort, the NCSA is developing what we hope (resource permitting) will be a three-year national cyber security awareness campaign. This campaign, targeted at home users and small businesses, will use various vehicles to raise awareness of the cyber security issue and steps people can take to protect themselves. Whether through radio, print or television, these public service announcements will talk about the important role all consumers play in ensuring the security of our information infrastructures. In developing this campaign, the NCSA is working closely with the US Department of Homeland Security, one of our major sponsors. A campaign of this size and scope does require significant resources. The NCSA has begun an effort to raise these resources.

In conjunction with these awareness efforts, the campaign also will include dissemination of cyber security tips. This effort, referred to as "Stay Safe Online," already has begun through the NCSA's main website: www.staysafeonline.info. On this site, visitors can find self-tests, top security tips, helpful links and more. For our latest list of *Top Ten Cyber Security Tips*, please see Appendix A of this testimony.

Initiative: Tips and Toolkits

Our second major project involves developing toolkits for small businesses and specific subgroups within the home user audience. These toolkits will include materials, guidebooks and training programs for each group based on the NCSA's *Top Ten Cyber Security Tips*, including a version of the top ten tips for children (K-12). We are in discussion with a variety of other organizations, including the Small Business Administration, InfraGard, ISSA, NIST, FBI and the Internet security provider (ISP) community, to establish key partnerships so that the cyber security tips, toolkits and training programs can be disseminated as quickly and as far as possible to each targeted audience.

Initiative: Youth Education

Our third major effort will focus on educating our youth on cyber security practices to make sure the next generation of users is cyber secure. Through partnering with outside organizations such as CyberSmart!, we hope to develop and disseminate cyber security curriculum to educators across the country. The NCSA also supported a national poster contest in which students were asked to creatively depict the importance of cyber security.

In addition to these initiatives, the sponsors of the NCSA are actively developing other creative efforts as well. We look forward to sharing these with the Subcommittee in the future.

National Awareness Campaigns: A Glance

As we have stated, the NCSA expects our national cyber security awareness campaign to be a cornerstone of our effort to reach consumers and small businesses. In crafting this campaign, we have turned to many other examples of similar efforts, through which government and others came together to develop an educational effort to reach individuals, raise awareness and change behavior. We share a few leading examples here, gathered from the website of the Ad Council (http://www.adcouncil.org/campaigns), for informational purposes:

> **Issue: Homeland Security**
> Sponsor: US Dept of Homeland Security; Alfred P. Sloan Foundation
> Goal: To educate Americans on how to respond to future terrorism-related emergencies
> Campaign: Ready.gov

Issue: Healthy Lifestyles
Sponsor: US Dept of Health and Human Services
Goal: To lower the percentage of Americans who are overweight or obese due to sedentary lifestyles and unhealthy diet and exercise habits
Campaign: Healthy Lifestyles and Disease Prevention Campaign

Issue: Wildfire Prevention
Sponsor: USDA Forest Service, National Association of State Foresters
Goal: To remind Americans of the importance of outdoor fire safety and wildfire prevention
Campaign: Only You Can Prevent Wildfires

Issue: Drunk Driving Prevention
Sponsor: US Dept of Transportation/NHTSA
Goal: To reduce alcohol-related vehicular injuries and deaths
Campaign: Friends Don't Let Friends Drive Drunk

Issue: Crime Prevention
Sponsor: National Crime Prevention Council; US Department of Justice
Goal: To reduce crime and build safer communities by encouraging teens and adults to engage in their communities
Campaign: Invest in Youth for a Safer Future

Issue: Promote Voting
Sponsor: Federal Voting Assistance Program
Goal: To encourage 18-24 year olds to participate in upcoming elections
Campaign: Decision Guy

NCSA's Invitation

On behalf of the NCSA, I would like to formally invite you, Mr. Chairman, the Members of this Subcommittee and your Congressional colleagues to learn more about the National Cyber Security Alliance:

1) We invite Members to place a link and the NCSA logo on your website so that your constituents can be made aware of the information that is available to them in this area.

2) We invite Members to use our monthly cyber security tip newsletter (in development) to send out to their state and local publications.

3) We invite Members to turn to us to assist in educating their constituencies of the threats online and how to protect themselves. The NCSA has brochures and other materials that Members can use in town hall meetings. We are happy to assist your staff with coordinating these programs and will work to provide you a representative from the NCSA for your local events.

4) We invite you to look at our awareness campaign plans as well as other efforts that have had national exposure and impact.

Summary

Mr. Chairman, the challenge before us today is significant. Cyber attacks are accelerating and becoming more dangerous. Reported vulnerabilities are on the rise and are being exploited more frequently and faster. Consumers and small businesses are using the Internet at higher and higher rates. While many have basic security technologies in place, most are not following the practices needed for them to be effective.

There are steps we can take to make a real difference. As the NCSA, we have come together to develop real initiatives in awareness and education. We do not believe we have all the solutions. In fact, we embrace the philosophy, "let a thousand flowers bloom." But we do hope that our initiatives can contribute to the overall progress in educating consumers and small businesses to protect themselves–and in turn, all of us.

As is often said, security is a journey, not a destination. We applaud your Subcommittee and Congress for continuing to put energy into addressing the cyber security challenge. In return, we pledge to you the NCSA's support to continue to work with government, industry and academia to develop initiatives to address these specific challenges.

I thank you again for the opportunity to testify here today, and I look forward to answering any questions the Subcommittee may have.

Appendix A: NCSA's Cyber Security Tips

NCSA's Top Ten Cyber Security Tips for Home Users and Small Business
(from www.staysafeonline.info)

1. Use "anti-virus software" and keep it up to date.
2. Don't open email or attachments from unknown sources. Be suspicious of any unexpected email attachments even if it appears to be from someone you know.
3. Protect your computer from Internet intruders -- use "firewalls".
4. Regularly download security updates and "patches" for operating systems and other software.
5. Use hard-to-guess passwords. Mix upper case, lower case, numbers, or other characters not easy to find in a dictionary, and make sure they are at least eight characters long.
6. Back up your computer data on disks or CDs.
7. Don't share access to your computers with strangers. Learn about file sharing risks.
8. Disconnect from the Internet when not in use.
9. Check your security on a regular basis. When you change your clocks for daylight-savings time, reevaluate your computer security.
10. Make sure your family members and/or your employees know what to do if your computer becomes infected.

1. Use "*anti-virus software*" and keep it up to date.
Make sure you have anti-virus software on your computer! Anti-virus software is designed to protect you and your computer against known viruses so you don't have to worry. But with new viruses emerging daily, anti-virus programs need regular updates, like annual flu shots, to recognize these new viruses. Be sure to update your anti-virus software regularly! The more often you keep it updated, say once a week, the better. Check with the web site of your anti-virus software company to see some sample descriptions of viruses and to get regular updates for your software. Stop viruses in their tracks!

2. Don't open email or attachments from unknown sources. Be suspicious of any unexpected email attachments even if it appears to be from someone you know.
A simple rule of thumb is that if you don't know the person who is sending you an email, be very careful about opening the email and any file attached to it. Should you receive a suspicious email, the best thing to do is to delete the entire message, including any attachment. . If you are determined to open a file from an unknown source, save it first and run your virus checker on that file, but also understand that there is still a risk. If the mail appears to be from someone you know, still treat it with caution if it has a suspicious subject line (e.g. "Iloveyou" or "Anna Kounikova") or if it ortherwise seems suspicious (e.g., it was sent in the middle of the night). Also be careful if you receive many copies of the same message from either known or unknown sources. Finally, remember that even friends and family may accidentally send you a virus or the e-mail may have been sent from their machines without their knowledge. Such was the case with the "I Love You" virus that spread to millions of people in 2001. When in doubt, delete! If you receive an email from a trusted vendor or organization, be careful of phishing, a high-tech scam used to deceive consumers into providing personal data, including credit card numbers, etc. For information about "phishing" go to the FTC document titiled "How Not to Get Hooked By a

Phishing Scam", http://www.ftc.gov/bcp/conline/pubs/alerts/phishingalrt.pdf. The best way to make sure you're dealing with a merchant you trust, and not a fraudster, is to initiate the contact yourself. Type the merchant's address into your Internet browser instead of clicking on a link in an e-mail.

3. Protect your computer from Internet intruders – use "*firewalls*".
Equip your computer with a firewall! Firewalls create a protective wall between your computer and the outside world. They come in two forms, software firewalls that run on your personal computer and hardware firewalls that protect a number of computers at the same time. They work by filtering out unauthorized or potentially dangerous types of data from the Internet, while still allowing other (good) data to reach your computer. Firewalls also ensure that unauthorized persons can't gain access to your computer while you're connected to the Internet. You can find firewall hardware and software at most computer stores and in some operating systems. Don't let intruders in!

4. Regularly download security updates and "patches" for operating systems and other software.
Most major software companies today release updates and patches to close newly discovered vulnerabilities in their software. Sometimes bugs are discovered in a program that may allow a criminal hacker to attack your computer. Before most of these attacks occur, the software companies or vendors create free patches for you that they post on their web sites. You need to be sure you download and install the patches! Check your software vendors' web sites regularly for new security patches or use the automated patching features that some companies offer. Ensure that you are getting patches from the correct patch update site. Many systems have been compromised this past year by installing patches obtained from bogus update sites or emails that appear to be from a vendor that provides links to those bogus sites. If you don't have the time to do the work yourself, download and install a utility program to do it for you. There are available software programs that can perform this task for you. Stay informed!

5. Use hard-to-guess passwords. Mix upper case, lower case, numbers, or other characters not easy to find in a dictionary, and make sure they are at least eight characters long.

Passwords will only keep outsiders out if they are difficult to guess! Don't share your password, and don't use the same password in more than one place. If someone should happen to guess one of your passwords, you don't want them to be able to use it in other places. The golden rules of passwords are: (1) A password should have a minimum of 8 characters, be as meaningless as possible, and use uppercase letters, lowercase letters, symbols and numbers, e.g., xk2&LP97. (2) Change passwords regularly, at least every 90 days. (3) Do not give out your password to anyone! For enhanced security, use some form of two-factor authentication. Two-factor authentication is a way to gain access by combining something you know (PIN) with something you have (token or smart card).

6. Back up your computer data.
Experienced computer users know that there are two types of people: those who have already lost data and those who are going to experience the pain of losing data in the future. Back up small amounts of data on floppy disks and larger amounts on CDs. If you have access to a network, save copies of your data on another computer in the network. Many people make weekly backups of all their important data. And make sure you have your original software start-up disks handy and available in the event your computer system files get damaged. Be prepared!

7. Don't share access to your computers with strangers. Learn about file sharing risks.
Your computer operating system may allow other computers on a network, including the Internet, to access the hard-drive of your computer in order to "share files". This ability to share files can be used to infect your computer with a virus or look at the files on your computer if you don't pay

close attention. So, unless you really need this ability, make sure you turn off file-sharing. Check your operating system and your other program help files to learn how to disable file sharing. Don't share access to your computer with strangers!

8. Disconnect from the Internet when not in use.
Remember that the Digital Highway is a two-way road. You send and receive information on it. Disconnecting your computer from the Internet when you're not online lessens the chance that someone will be able to access your computer. And if you haven't kept your anti-virus software up-to-date, or don't have a firewall in place, someone could infect your computer or use it to harm someone else on the Internet. and help protect others: disconnect!

9. Check your security on a regular basis. When you change your clocks for daylight-savings time, reevaluate your computer security.
The programs and operating system on your computer have many valuable features that make your life easier, but can also leave you vulnerable to hackers and viruses. You should evaluate your computer security at least twice a year – do it when you change the clocks for daylight-savings! Look at the settings on applications that you have on your computer. Your browser software, for example, typically has a security setting in its preferences area. Check what settings you have and make sure you have the security level appropriate for you. Set a high bar for yourself!

10. Make sure your family members and/or your employees know what to do if your computer becomes infected.
It's important that everyone who uses a computer be aware of proper security practices. People should know how to update virus protection software, how to download security patches from software vendors and how to create a proper password. Make sure they know these tips too!

Mr. PUTNAM. Thank you, Mr. Sabo. Thank you to all of our witnesses.

We will begin with Mr. Clay's questions.

Mr. CLAY. Thank you very much, Mr. Chairman. Thank you all for being here today.

Mr. Clinton, we will start with you. What steps can the Federal Government take to use its procurement power to improve the security of computer software? Is the Internet security industry able to agree on some minimal standards for computer security hygiene? I guess that is a two-part question.

Mr. CLINTON. Thank you, Mr. Clay. We do think that the procurement process is probably the best first step for the Federal Government to take in terms of establishing benchmarks for appropriate security to be included within products that they purchase. I think what we think is most important about this is that it would be the Federal Government using its market forces rather than its regulatory forces to encourage behavior. We think absolutely that is the model that is going to be most effective is the use of the market. During the Corporate Information Security Working Group we discussed this quite a bit and talked about how if the Federal Government could act as a model through its procurement practices, as the Department of Energy already has started, that we might be able to make an awful lot of steps, and that has the effect on the rest of the market of likely lowering costs, making these sorts of devices or procedures more accessible to small businesses.

Now the second question, Mr. Clay, was whether or not we could agree on standards. It kind of depends on what you are talking about in terms of standards. There is an awful lot of standards activity that is already underway. If what you are suggesting is do we think that the Federal Government should be passing legislation or regulation mandating standards, we would think that is the wrong way to go. And let me explain why. It is not so much that we are opposed to standards. EIA is one of the largest standards producers in the entire world. It has to do, Mr. Clay, with the nature of the Internet.

The Internet is a 21st century technology. Most of the regulatory models that we use in the Federal Government now are 18th century models. The FCC and the SEC are modelled on the old ICC which regulated railroads. We are dealing with something that is entirely different now. We think that for security purposes we need a much more dynamic manager of the Internet and the only mechanism that we can identify that will be dynamic enough to keep up with the ever-increasing attacks and technologies of the attackers is to use market forces. So, more creative use of insurance, more creative use of liability carrots involving marketing for cyber security. And there is a range of things that we identified in our incentives group report we think are far more likely to succeed in our ultimate aim of achieving cyber security than a federally mandated standard.

Mr. CLAY. Oh, please do not misunderstand the question. I was just asking could the industry come together and establish the standards. I never made inference to a Federal law, and that is not where I am going with that.

Mr. CLINTON. I appreciate that. And, yes, we are working on that quite hard.

Mr. CLAY. Thank you for the answer. Mr. Sabo, do you believe the Federal Government's commitment to cyber security training and certification particularly at the systems and network administrator level is adequate? And how important is training and certification to cyber security?

Mr. SABO. Thank you, Ranking Member Clay. The National Cyber Security Alliance itself does not have a particular position on those areas. But if I could speak on behalf of myself and the company that I do work for during the day, I do think, and the organizations that support the NCSA would probably agree, there is significant training going on but that there is always more that could be done. I think we heard from the director of the NCSD previously about the number of programs that are out there, the scholarship for service and the other organizations, and I think there is certainly a lot more to be done. In our purview of the awareness side, we did talk significantly about awareness for home users. But I think you could take what we plan to do for home users and also put that for Federal Government workers, both as users that will then be going home and using their personal systems probably to even connect into Federal Government systems, and then also as employees of the Federal Government. So our awareness efforts certainly would be useful for that audience as well.

Mr. CLAY. OK. I thank you for that comment. Mr. Chairman, I think my time is up.

Mr. PUTNAM. You are welcome to continue.

Mr. CLAY. OK. Just one more question for Mr. Petersen. Before I ask the question, I just want to make you aware that I too am a University of Maryland graduate. So fear the turtle. [Laughter.]

Mr. PETERSEN. Yes. I was thinking of that earlier when Dewie was displayed. [Laughter.]

Mr. CLAY. On a serious note, though, is the Congress adequately funding research and development in the cyber security area? And what other methods could the Federal Government employ in order to achieve widespread cyber security?

Mr. PETERSEN. Thank you for your question. I do think you are on the right path to increasing funding for cyber security research and development efforts. The university environments are particularly participating in National Science Foundation solicitations, they currently are reviewing proposals now for a cyber trust solicitation. We have been working pretty regularly with the Science and Technology Directorate of the Department of Homeland Security, although I note that in their $1 billion-plus budget only $18 million are devoted to cyber security and many of us think that is wholly inadequate and perhaps symbolizes that cyber security is not thought to be the priority that it should be.

Having said that, I think there is more room for funding for R&D. But I do not want us to forget what we are here about today and certainly what our group represents, which is securing today's Internet. There are not nearly enough Federal Government funds available to deal with education and awareness of the mass populace, including kids in schools and higher education, and efforts needed to secure our current infrastructure.

Mr. CLAY. Thank you for that response. Mr. Chairman, I yield back the balance of my time.

Mr. PUTNAM. Thank you, Mr. Clay. Mr. Clinton, one of the key ingredients to a successful education and awareness campaign is clarity and credibility of the message. Given your experiences and knowledge of the work to identify cyber security best practices, what is the most direct and clear message that can be conveyed to home users and small businesses?

Mr. CLINTON. Thank you, Mr. Chairman. I was thinking of this when you asked the first panel the question. My answer is a little different. I support their view that people need to think. But I think they need to think of their computer in a different sense. My experience is that most home users tend to think, and I am saying most home users, not the sophisticates, most home users still think of their computer like it is a TV set, that you just turn it on and it provides you things. And that is the wrong way to think of your computer. I think a better way to think of your computer is like it is a gifted child; it is something you need to work with, it is something you need to interact with, and if you treat it well and protect it and develop it, it can do great things, but if you do not, it could come back and cause all sorts of tremendous problem. I think we need to get consumers to think of the technology very, very differently.

Most of us have become so comfortable with some of the rudimentary elements of the Internet we forget that just a few years ago e-mail scared us. I remember when I worked for my first Member here on Capitol Hill, and I will not say who that was, I had to show him how to turn on the computer. It was not that long ago. But I do not think that we have completely kept up with what is really behind this medium. It looks too easy. So I would say what we need to do is we need to get people to rethink what it is they are dealing with. They have to have an active relationship with their network, not just treat it as a passive appliance.

Mr. PUTNAM. Mr. Howell, your thoughts?

Mr. HOWELL. I agree entirely with Larry. And I would argue that a computer is also a gold mine which has tremendous potential and has to be exploited in order to achieve that potential. In one of our most recent efforts to educate our membership, we were talking to several of our small companies who had no concept of the fact that keeping customer information—customer invoices, sales lists, sales figures, revenue and expense items, their general ledger—on a computer that was accessible via high speed to the Internet without a firewall and without anti-virus was essentially a security risk. They just had not thought about their computer that way. I would agree with Larry, they viewed it as almost an entertainment vehicle, something there for their pleasure and their ease of use, and they did not view any of the risks that the sophisticated users see out there everyday. And it is because, frankly, we have not done enough to educate people about the threats that are facing them and, at the same time, make action to mitigate those threats possible.

Mr. PUTNAM. What is the appropriate role for the hardware and software vending community, not only to provide more secure and

higher quality products, but also to educate their consumers about basic cyber security practices?

Mr. HOWELL. I think that all three parts of this triangle, the hardware and software vendors as well as the user community, must do much more collaboratively to talk about risks, vulnerabilities, and mitigation of risk and vulnerabilities. Among large enterprises you are seeing much more collaboration on all three sides of that. But it has taken a long time to develop and a lot of those things develop based on trust and years of working with one another and the information technology industry is relatively young. At the same time, I think that we are seeing more medium-size enterprises catch up and do some of this. And the challenge therefore remains the small enterprise community. And as Larry mentioned, that was quickly viewed within our Corporate Information Security Working Group as an area where there is no targeted information on risk mitigation and what the real threats are. So I think it is a multifaceted process depending on what particular market you are looking at—the large enterprise market, I think it is a collaborative process; medium-size enterprises, I think they are moving toward that collaboration; small enterprises, it is still very much awareness and education oriented.

Mr. PUTNAM. Mr. Petersen, your thoughts on that?

Mr. PETERSEN. Your question about hardware and software reminded me of a story over the Christmas holidays. I had a friend who subscribed for the first time to Comcast cable and when he went to the local shopping mall he got a CD and the installation instructions and he came home and installed it and within a matter of seconds he got the Blaster worm. And in trying to help my friend troubleshoot the problem, the first thing that occurred to me is how come Comcast cable is not distributing information to its customers about the threats that currently existed at that point in time, that when you move from being off-line to broadband you better make sure your operating system is up to date, and, by the way, here is a CD that can provide you the latest patches and the latest anti-virus stuff. So I think absolutely there is a role for hardware and software and other service providers to play in providing consumers with educational and awareness materials.

Second, if you think about our parents and students who are buying computers for their children, think if they open that computer box and there is a label that said, you know, "Tear this off and be aware, if you do not do X, Y, and Z, you could lose your data and all the important work that you put into this machine." I do believe that, aside from our role in educating and making users aware, hardware and software vendors could help.

Mr. PUTNAM. Mr. Sabo, do you want to add anything to that?

Mr. SABO. Yes, thank you, Mr. Chairman. I do think there is significant information out there from the software/hardware vendors and the ISP community. But I think there is a fundamental research need that we all could perhaps support in looking at user behavior, benchmarks, metrics, in order to understand how we reach these users, what are the best messages—and I do not think there is a one size fits all message for security; I think what will motivate users will vary greatly among them; fundamental research in where to reach them, to what sites to go, what places in

the real world and the virtual world to place these messages' and then fundamental research in who to reach, who are these "users." I think a number of studies have shown that a majority of home users who are doing a lot of the financial transactions in households are the women in the households. I think that would impact therefore where we deliver these messages, what types of Web sites, what types of media that perhaps our awareness campaign will target. So I think there is a lot of information that is out there but, exactly as you said in your opening statement, perhaps we run the risk of having too much and we may need to really think about where are the best places to go and to put this information.

Mr. PUTNAM. That is a perfect segue into my next question. You have heard the FTC testify about the turtle, you have Stay Safe On Line, there are a number of other approaches to increasing awareness. Is that type of symphony of approaches helpful in that you are hitting different pieces of the audiences, or do you believe that there should be a more centralized message, centralized theme, centralized Web site for people to go for information on becoming more secure?

Mr. SABO. I definitely agree that we are in a period of "let a thousand flowers bloom." And perhaps in a way we have become victims of our own success, that we have talked about the important need for all these awareness efforts and we are starting to get them. And I think behind scenes we are also seeing a lot more effort to do the centralization, but centralization of the organization behind it. So you have the folks who are running these talking to each other much more. And I think there is a lot of room for improvement in that area. We certainly would commit ourselves to being part of any effort that would help with that. I do think, at the end of the day, each set of users are going to respond to different types of messages in different media.

Mr. PUTNAM. Mr. Petersen.

Mr. PETERSEN. I share your concern but I think we are headed in the right direction. I know even EDUCAUSE has more recently become a sponsor of the Alliance. We are working closely with the FTC. And when we look at our colleges and university environments, many of them, like Florida State University, Florida, University of Maryland, are large enterprises. So whatever messages we might be targeting toward large businesses probably apply to our large colleges and universities. Many of them are small colleges and community colleges and the small business environment messages are the same.

One of the things we have worked hard with the Alliance on is when you take their top 10 cyber tips, those should be the same top 10 cyber tips that all of our users hear about, our students, faculty, staff. So rather than us starting from scratch or writing our own messages, we are working hard to make sure their messages get put into the appropriate language so that we can use them and convey a consistent message.

Mr. PUTNAM. Mr. Clinton, do you want to add something to that?

Mr. CLINTON. I would agree that the messages should be consolidated. But I do want to caution that there is a problem if we think we have the right answer and so all we have to do is go out and make everybody understand the right answer. We have published

two best practices that we are very proud of and that got endorsed by a lot of people and we thought they were great. And we took our best practices to the small business guys and they said, "What are you talking about? We do not understand this. No small business guy would ever read this stuff." But the technologist people think, hey, this is the right message. And we found out by doing the market research it was not the right message.

So I think that there needs to be some consolidation with regard to messages, that we should not have conflicting messages, for sure. But I do not think we do. I would agree with the rest of the panel that I think we are moving in the right direction. But the way messages are presented need to be targeted differently to different audiences. We represent small companies and we represent enormous companies and they deal with these issues very, very differently. I think that the approach that we need to take is a market-centered approach. We need to go out to each target market. And small business may not be a target market. Small business may be an enormous market that needs to be much better segmented within that market in order to better appreciate these people. There are small technology companies and there are small marketing companies, and you talk to these guys in different ways.

So I do not think it is quite as simple as saying we have the message, all we have to do is get it out. I think that we have a lot of the right ideas but I think we need to continue to work on it and we need to involve the users, we need to involve the target audiences much more in developing the messages. And I think we are just at the beginning of that process.

Mr. PUTNAM. Mr. Howell.

Mr. HOWELL. I would agree. But I would just add one thing, and that is, you also have to look at the messenger and the affinity of the desired market to that messenger. Different organizations have different affinity with different type and sizes of organizations and companies. And agreed, having the same set or a similar set of messages is essential. But one organization that may be the best messenger might have absolutely no affinity with or relation to the target market, and therefore, if one were to follow our principles of not opening e-mails, for example, from an unknown sender, that e-mail would get deleted because there is no affinity to that sender. So that is the only other issue I would add here.

And at the same time, I think the National Cyber Security Summit, held last December and an ongoing vehicle, as well as NCSA, both have been fantastic vehicles, joining with your Information Security Working Group, in aggregating organizations that have been working just in an area of awareness alone to sit down at a table, think about how they can multiply or take advantage of their efforts and reduce waste and enhance efficiency and increase awareness. It has been tremendous. Every week, for example, since we started participating in your group we have been approached by at least one other association who wants to join in what we are trying to do on education and awareness. That has been one of the most rewarding things we have seen so far in all the education and awareness efforts.

Mr. PUTNAM. And finally, do you all believe that this issue has risen to the boardroom, to the C-level executives? All the talk about

worms and viruses and exploits, some attention through Sarbanes-Oxley and Section 404, are top level executives finally treating cyber security as a business risk? We will begin with Mr. Sabo and work down the table.

Mr. SABO. Thank you. I think today, compared to 2, even 3 years ago, we have come a significant way in getting the attention to that level. But I think there is certainly a lot more in the corporate governance side between the work that the Cyber Security Summit Working Group as well as your own has done is significant and the word needs to get out now. And that is I think the stage we are at.

Mr. PETERSEN. I would say no. In the college and university environment, we have a long way to go particularly at the president level and the board level. In fact, I would say that is one of the reasons why in my first bullet I said we need support from the private and government sector. It was not just referring to financial support. Many people in government and certainly part of corporations sit on college and university boards, and I am hoping the awareness that is being created within industry and government will translate to board members going to those board meetings and saying what are you doing about information security on your campus, why have we not talked about it in the context of governance. And I think the same message needs to be carried forward to our presidents and chancellors and other executive leaders. We are certainly doing our part as our task force to raise awareness, but I think we could use the assistance and support of other executives.

Mr. PUTNAM. Mr. Howell.

Mr. HOWELL. One of the recommendations that we made within our National Cyber Security Summit Large Enterprises Working Group was that our ad hoc coalition come together with DHS and we recommended a series of forums across the country with senior DHS officials and CEOs to discuss information security and corporate governance. And we hope that DHS will take up that recommendation because we believe that it is essential. I would agree with Doug, we have made progress. But I think much more remains to be done. At the same time, we need to move forward with a collaborative approach with a framework similar to what the Corporate Governance Task Force of the National Cyber Security Summit came out with recently. That is a great starting point, one of many materials that are out there. And moving forward with implementation of all of these documents is, I think, an essential next step.

Mr. PUTNAM. Thank you. Mr. Clinton.

Mr. CLINTON. I would have to say that we have maybe taken the first steps in this direction. But, no, Mr. Chairman, we have not at all reached the summit of the CEOs and the COOs. Just a couple of facts. I heard the first panel talk about how they were under the impression that Graham-Leach-Bliley, Sarbanes-Oxley may have increased awareness, and perhaps it has increased awareness some. But the fact is, Mr. Chairman, that the number of incidents last year and again early this year are going through the roof. The amount of money that is being lost is going through the roof. So if there is some increased awareness, it is not enough.

Another fact. The most recent study that I have seen on this, done by CSO magazine, indicated that most corporations they recommended should be increasing their IT cyber security budget by approximately 33 percent. They went back and looked at how many corporations had done that. They found that only 22 percent of the corporations had increased it, and only 7 percent of the corporations had increased it the amount that was required. So we are a long way away.

Mr. Chairman, this I think goes back into the conversation we just had on your last question, finding the right messages for this particular target audience, COOs, CEOs. I do not want to cast any aspersions on the CEOs and COOs who fund, frankly, my organization, but the fact of the matter is, Mr. Chairman, they are not going to do this because it is in the national interest. We need to find messages that speak to their corporate interest. We need to find issues that speak to the corporate interest. We need to do a better job demonstrating the return on investment to good cyber security. We need to do a better job of providing the sort of incentives that level of corporate executive pays attention to—lower business costs, less liability exposure. Those are the sorts of things that are talked about in CEO board rooms and CEO discussions. And we have not done that yet. I think that there is a tremendous amount that we have not yet gotten to in the public-private partnership in that area that lays still before us. And we are enthusiastic about working with the Congress in those areas. But we are just at the first couple steps, in my opinion, sir.

Mr. PUTNAM. Thank you, Mr. Clinton, particularly for your candor. We assume that is not going to be the punch-out quote in your monthly newsletter to your members.

Mr. CLINTON. No, sir. I am going to use your opening statement as our punch-out quote.

Mr. PUTNAM. I want to thank all of our witnesses for your efforts in this important arena. I know that your work continues to help our cyber citizens enjoy the benefits of the Internet in a safe and secure manner. I also want to thank Mr. Clay for his participation today. In the event that there are additional questions that we did not get to today, the record will remain open for 2 weeks for submitted questions and answers.

With that, the subcommittee stands adjourned.

[Whereupon, at 4:07 p.m., the subcommittee was adjourned, to reconvene at the call of the Chair.]

○