AUTHENTICATED
U.S. GOVERNMENT
INFORMATION
GPO

LOCKING YOUR CYBER FRONT DOOR—THE CHALLENGES FACING HOME USERS AND SMALL BUSINESSES

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

JUNE 16, 2004

Serial No. 108–234

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

96–994 PDF WASHINGTON : 2005

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

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
BETTY MCCOLLUM, Minnesota

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*
DAVID MCMILLEN, *Minority Professional Staff Member*

CONTENTS

	Page
Hearing held on June 16, 2004	1
Statement of:	
Yoran, Amit, Director, National Cyber Security Division, Department of Homeland Security; J. Howard Beales III, Director, Bureau of Consumer Protection, Federal Trade Commission; Cheryl A. Mills, Associate Administrator, Entrepreneurial Development, Small Business Administration; and Ed Roback, Chief, Computer Security Division, National Institute of Standards and Technology, Department of Commerce	12
Letters, statements, etc., submitted for the record by:	
Beales, J. Howard, III, Director, Bureau of Consumer Protection, Federal Trade Commission, prepared statement of	23
Clay, Hon. Wm. Lacy, a Representative in Congress from the State of Missouri, prepared statement of	10
Dailey, Thomas M., chair and president, U.S. Internet Service Provider Association, general counsel, Verizon Online, prepared statement of	80
Frischmann, Don, senior vice president, communications and brand management, Symantec Corp., prepared statement of	73
Kurtz, Paul, executive director, Cyber Security Industry Alliance, prepared statement of	126
Mills, Cheryl A., Associate Administrator, Entrepreneurial Development, Small Business Administration, prepared statement of	44
Putnam, Hon. Adam H., a Representative in Congress from the State of Florida, prepared statement of	5
Reitinger, Philip, senior security strategist, Microsoft Corp., prepared statement of	63
Roback, Ed, Chief, Computer Security Division, National Institute of Standards and Technology, Department of Commerce, prepared statement of	49
Tevanian, Avadis, Apple Computer, Inc., prepared statement of	68
Yoran, Amit, Director, National Cyber Security Division, Department of Homeland Security, prepared statement of	15

LOCKING YOUR CYBER FRONT DOOR—THE CHALLENGES FACING HOME USERS AND SMALL BUSINESSES

WEDNESDAY, JUNE 16, 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 2:30 p.m., in room 2154, Rayburn House Office Building, Hon. Adam Putnam (chairman of the subcommittee) presiding.

Present: Representatives Putnam, Clay and Murphy.

Staff present: Bob Dix, staff director; John Hambel, senior counsel; Dan Daly, professional staff member and deputy counsel; Juliana French, clerk; Felipe Colon, fellow; Colin Samples and Katlyn Jahrling, interns; David McMillen, Mark Stephenson, and Adam Bordes, minority professional staff members; and Cecelia Morton, minority office manager.

Mr. PUTNAM. A quorum being present, this hearing on the Subcommittee on Technology, Information Policy, Intergovernmental Relations and the Census will come to order. I want to welcome everyone here today to this hearing entitled, "Locking your Cyber Front Door—The Challenges Facing Home Users and Small Businesses."

We will immediately go into my opening statement and the witnesses' opening statements as quickly as possible. We are expecting a series of five votes which will pretty well mutilate the bulk of the afternoon. We are going to move as expeditiously as possible.

In the past few years, the growth in access and use of the Internet, the increase in "always on" high-speed connections, and the rapid development and deployment of new computing devices has resulted in expanding global computing network. Although these advances have improved the quality of life, this network is susceptible to viruses and worms that can circle the world in a matter of minutes.

The potential for more sophisticated and malicious cyber attacks is growing at an alarming rate. While businesses, educational institutions and home users enjoy the benefits of using the Internet, they are not always adequately informed about the potential dangers of computer systems left vulnerable and unprotected.

This hearing is a continuation of a series of oversight hearings that the subcommittee has conducted during the 108th Congress on

the issue of cyber security. On April 21st, the subcommittee held a hearing specifically on educational awareness for all cyber citizens. Most recently, on June 2nd, the subcommittee conducted an oversight hearing on cyber security and vulnerability management issues facing large enterprises. The purpose of this hearing is to focus attention on the challenges facing home users and small businesses.

Today we will examine the difficulties these users confront in protecting their computers; the actions taken by the Federal Government to create partnerships that will assist home users and small businesses and their efforts; the role of software and hardware manufacturers in responding to the expectations and demands of the user community to provide the market place with higher quality and more secure products; the role of Internet service providers in helping to educate and protect their subscribers; and the tools and strategies available to home users and small businesses to lessen their exposure.

Home users and small businesses are in a uniquely vulnerable position because their computers often face the same worms, viruses, and automated attacks that business and Government computers face. Yet, these users may not have the same level of resources available to mitigate those risks.

Accordingly, it is critically important that all stakeholders examine tools and strategies to comprehensively address this challenge. Right now, home and small business users face a number of types of risks. Viruses and worms can disable home user systems. Home users may also be tricked into downloading spyware. These programs can 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. Home users also face the threat of fraud and identity theft, including a newer approach known as "phishing."

Small businesses face these same threats as well, but their challenges are compounded by the fact that they may have a network of machines to manage, as well as the challenge of employees using laptops and remote access. Of even greater concern, small businesses face the threat of disgruntled insiders who were once trusted users.

Finally, small businesses may also have private information from their customers and data bases that are connected to the Internet. Cyber criminals who gain access to this information may attempt to extort money out of small businesses to keep the breach quiet. The loss of reputation from such an incident could be devastating to a small business.

There are existing and emerging protections against these threats. Home users and small businesses can arm themselves with virus-protection software to help stop any potential impacted viruses and worms. The use of firewalls can help prevent some forms of spyware and attempts at unauthorized access to a user's machine. Automated patches are also a step in the right direction to help users stay up-to-date with protections against the most recently published vulnerabilities.

However, employment of these well-known protections is still inconsistent. Awareness of the available protections needs to be ele-

vated so that basic computer security hygiene becomes a common practice among all users. Increasing cyber security awareness will help users to protect themselves, but 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.

We can no longer simply blame the users for their failure to mitigate vulnerabilities. The users are not responsible for the flaws and defects in the products that are the source of the vulnerabilities. We will continue to examine the progress being achieved by manufactures of hardware and software products in responding to the consumer and public demand for higher quality and more secure products in the market place. I am encouraged by what I see as signs that the manufacturers have taken this demand very seriously and are working diligently to remedy it.

Vendors are starting to release products that are secure by default, by enabling secure technical control settings, and by requiring affirmative action of the user to enable features that would make the product less secure. Software and hardware vendors are making more significant commitments to their quality assurance programs in an effort to identify bugs prior to the deployment of new systems. Collaboration among vendors to offer a bundled suite of security products to users, along with a more concerted effort to configure systems in a more secure manner out-of-the-box will produce a more secure computing environment.

In addition to the efforts of the vendors to improve security of their products, the Federal Government needs to help improve the security of computer products and services through R&D. Inadequate tools exist in the market place today to conduct effective code evaluation in advance of deployment to identify flaws, defects, and the potential of a malicious code willfully inserted in a software product.

By collaborating with partners in the world of academia and the private sector, the Federal Government should be working to support the development of such tools and other quality assurance tools that can make a meaningful difference in improving the quality and security of new IT products. The Federal Government has an important role in targeting research and development efforts to address these critical issues.

As a Member of Congress, a home computer user, and a champion of small business, this problem hits close to home. I intend to continue my efforts to improve cyber security in every sector of our Nation. In furtherance of this effort, we have 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 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. 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 home users, the group suggested targeted efforts aimed at the mass market that would help to educate these users. The group is seeking to build upon existing relationships and to forge new partnerships between organizations, corporations, and Government.

I will continue my support for these initiatives and intend to reconvene the Corporate Information Security Working Group at the end of this month to further develop a number of the recommendations that were produced in phase I. We have also taken an important step in furtherance of a recommendation from that working group.

Yesterday, along with Chairman Tom Davis, I introduced H.R. 4570 to amend the 1996 Clinger-Cohen Act to place a greater emphasis on computer security within the Federal Government. The bill brings Clinger-Cohen in line with the realities of today's information technology world by requiring agencies to specifically consider security when conducting systems planning and acquisition. We are confident that once it is signed into law, it will help to strengthen the Federal Government's overall efforts to improve the information security profile of its systems.

In closing, I want to make clear that securing the Nation's cyber space is an urgent challenge and we all have a role to play. The threat is real. The vulnerabilities are extensive. The time for action is now. Unfortunately, there are no simple solutions. We will continue to examine the role that Congress and the Federal Government can and should play in being a partner-in-progress, in elevating the attention to this matter for all stakeholders. Education and awareness is a key element to advise all users about the tools and strategies to reduce the risks associated with a very real cyber threat.

I look forward to all the testimony from today's witnesses. Today's hearing can be viewed live via Webcast. At this time I would be happy to recognize the ranking member.

[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

"Locking Your Cyber Front Door – The Challenges Facing Home Users and Small Businesses"

Wednesday, June 16, 2004
2:30 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 oversight hearing on "Locking Your Cyber Front Door – The Challenges Facing Home Users and Small Businesses."

In the past few years, the growth in access and use of the Internet, the increase in "always on" high-speed connections, and the rapid development and deployment of new computing devices has resulted in an expanding global computing network. Although these advances have improved the quality of life, this global network is susceptible to viruses and worms that can circle the world in a matter of minutes. The potential for more sophisticated and malicious cyber attacks is growing at an alarming rate. While businesses, educational institutions, and home users enjoy the benefits of using the Internet, these groups are not always adequately informed about the potential dangers of computer systems left vulnerable and unprotected.

This hearing is a continuation of a series of oversight hearings that the Subcommittee has conducted during the 108th Congress on the issue of cyber security. On April 21, the Subcommittee held a hearing specifically on educational awareness for all cyber citizens. Most recently on June 2, the Subcommittee conducted an oversight hearing on the cyber security and vulnerability management issues facing primarily large enterprises. The purpose of this hearing is to specifically focus attention on the challenges facing home users and small businesses. Today, the Subcommittee will examine the difficulties that these users confront in protecting their computers; actions taken by the federal government to create partnerships that will assist home users and small businesses

in their efforts to protect themselves against a variety of potential cyber threats; the role of software and hardware manufacturers in responding to the expectations and demands of the user community to provide the marketplace with higher quality and more secure products; the role of internet service provider's in helping to educate and protect their subscribers; and the tools and strategies available to home users and small businesses to lessen their exposure to risks.

Home users and small businesses are in a uniquely vulnerable position because their computers often face the same worms, viruses and automated attacks that business and government computers face. Yet, these users may not have the same level of resources available to mitigate these risks. Accordingly, it is critically important that all stakeholders examine tools and strategies to more comprehensively address this growing challenge.

Right now, home and small business users face many types of risk. Viruses and worms can disable home users' systems. Home users may also be tricked into downloading spyware. These programs can 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. Home users also face the threat of fraud and identity theft schemes, including a newer approach known as "phishing."

Small businesses face these same threats as well, but their challenges are compounded by the fact that they may have a network of machines to manage, as well as the additional challenge of employees using laptops and remote access. Of even greater concern, small businesses face the threat of disgruntled insiders who were once trusted users. Finally, small businesses may also have private information from their customers in databases that are connected to the Internet. Cyber criminals who gain access to this information may attempt to extort money out of small businesses to keep the breach quiet. The loss of reputation from such an incident could be devastating to a small business.

There are existing and emerging protections against these threats. Home users and small businesses can arm themselves with virus protection software to help stop any potential impact of worms and viruses. Use of firewalls can also help prevent some forms of spyware and attempts at unauthorized access to a user's machine. Automated patches are also a step in the right direction to help users stay up to date with protections against the most recently published vulnerabilities.

However, employment of these well-known protections is still inconsistent. Awareness of the available protections needs to be elevated so that basic computer security hygiene becomes a common practice amongst all users.

Increasing cyber security awareness will help users to protect themselves, but 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 enough regard to security. We can no longer simply blame the users for their failure to mitigate vulnerabilities. The users are not responsible for the flaws and defects in the products that are the source of the vulnerabilities in the first place. I will continue to examine the progress being achieved by the manufacturers of software and hardware products in responding to the consumer and public demand for higher quality and more secure

products for the marketplace. I am encouraged by what I see as signs that the manufacturers are taking this demand seriously.

Vendors are starting to release products that are "secure by default" by enabling secure technical control settings and by requiring affirmative action by the user to enable features that could make the product less secure. Software and hardware vendors are making more significant commitments to their quality assurance programs in an effort to identify "bugs" and flaws prior to deployment of new systems. Collaboration among vendors to offer a bundled "suite" of security products to users, along with a more concerted effort to configure systems in a more secure manner "out of the box" will produce a more secure computing environment.

In addition to the efforts of the vendors to improve security of their products, the federal government needs to help improve the security of computer products and services through research and development. Inadequate tools exist in the marketplace today to conduct effective code evaluation in advance of deployment in an effort to identify flaws, defects, and even the potential of malicious code willfully inserted in a software product. By collaborating with partners in the world of academia and the private sector, the federal government should be working to support the development of such tools and other quality assurance tools that can make a meaningful difference in improving the quality and security of new IT products. The federal government has an important role in targeting R & D efforts to address such critical issues.

As a member of Congress, a home computer user, and a champion of small business, this problem hits close to home for me, and I plan to continue my efforts to improve cyber security in every sector of our nation. In furtherance of this effort, 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 (CISWG). 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. 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. I understand that efforts are under way to make this recommendation a reality.

For home users, the group suggested targeted efforts aimed at the mass market would help to educate these 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 hygiene. I will continue my support for these initiatives and plan to reconvene the Corporate Information Security Working Group at the end of this month to further develop a number of the recommendations that were produced in Phase I.

On a related note, I would like to announce that I have taken an important step in furtherance of a recommendation from the CISWG. Yesterday, along with Chairman Tom Davis, I introduced H.R. 4570 to amend the 1996 Clinger-Cohen Act to place a greater emphasis on computer security within the Federal government. H.R. 4570 brings Clinger-Cohen in line with the realities of today's IT world by requiring agencies to specifically consider security when conducting systems planning and IT acquisition. I am confident that once H.R. 4570 is signed into law that it will help to strengthen the Federal government's overall efforts to improve the information security profile of its systems.

In closing, I want to make clear that securing the nation's cyber space is an urgent challenge, and we all have a role to play. The threat is real...the vulnerabilities are extensive...and the time for action is NOW! Unfortunately, there are no simple solutions. I will continue to examine the role that the Congress and the federal government can and should play in being a "partner in progress" in elevating the attention to this matter for all stakeholders. Education and awareness is a key element to advise all users about the tools and strategies to reduce the risks associated with a very real cyber threat.

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

Mr. CLAY. Thank you, Mr. Chairman.

Let me thank the chairman for holding today's hearing on cyber security and the challenges facing America's small businesses and home user communities. I thank the witnesses before us today and hope their insights on methods for computer security will be both technologically realistic and practical for our target audiences.

Mr. Chairman, I will stop there since we do have a vote going. I would like to just make an abbreviated statement in reference to my entire opening statement. In the interest of time, I would ask that the remainder be submitted for the record.

Mr. PUTNAM. Without objection, so ordered.

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

STATEMENT OF THE HONORABLE WM. LACY CLAY
AT THE HEARING ON
Computer Security

June 16, 2004

Thank you Mr. Chairman for holding today's hearing on the cyber security challenges facing America's small businesses and home user communities. I thank the witnesses before us today, and hope their insights on methods for computer security will be both technologically realistic and practical for our target audiences.

While the federal government has improved its collaboration with the public and private sectors to fend off cyber security threats, we need to develop better measurements on security vulnerabilities and intrusions among home users and small businesses, as opposed to industry or large organizations. As reported by the CERT Center at Carnegie-Mellon University, there were approximately 13,000 security vulnerabilities that resulted from software flaws beginning in 1995 through 2003. More, the number of computer security incidents reported to the CERT Center increased from roughly 10,000 in 1999 to over 137,000 in 2003. For us to have a better understanding of the cyber security problem, however, we need to have a better handle on the statistics among each user sector, including small business and home users.

While constant change in technology and methods used by hackers make a permanent solution improbable, GAO does tell us that approximately 95% of all network intrusions can be

avoided by keeping systems updated. This means educating the small business and home user communities on the importance of system management is central to fending off a widespread security breach among both large networks and individual users. DHS must also continue to be a central resource for providing information about widespread cyber security threats, and a clearinghouse for guidance that can be utilized by users seeking to avoid future cyber security violations.

We know that the small business and home user communities often do not have access to an on-site IT staff in order to provide adequate stewardship of networks or systems. Thus, it is paramount for the government to increase its efforts in making both sectors aware of the economic and personal losses that are associated with cyber security threats throughout our nation.

Once again, I thank our Chairman for his continued work and dedication to these issues. This concludes my remarks, and I ask that they be inserted into the record.

Mr. PUTNAM. The committee will stand in recess.

[Recess.]

Mr. PUTNAM. The committee will come to order.

Let us move directly into testimony for panel I. Before we do so, let us administer the oath. If all of our witnesses, and anyone traveling with you to assist you in answering our questions, would please rise and raise your right hands.

[Witnesses sworn.]

Mr. PUTNAM. As a note for the record, all the witnesses responded in the affirmative.

Our first witness is Amit Yoran. Mr. Yoran is the Director of the National Cyber Security Division of the Department of Homeland Security. Before joining the Department, he served as the vice president of Worldwide Managed Security Services at Symantec, Corp. Prior to that, he founded Riptec, an information security company.

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

STATEMENTS OF AMIT YORAN, DIRECTOR, NATIONAL CYBER SECURITY DIVISION, DEPARTMENT OF HOMELAND SECURITY; J. HOWARD BEALES III, DIRECTOR, BUREAU OF CONSUMER PROTECTION, FEDERAL TRADE COMMISSION; CHERYL A. MILLS, ASSOCIATE ADMINISTRATOR, ENTREPRENEURIAL DEVELOPMENT, SMALL BUSINESS ADMINISTRATION; AND ED ROBACK, CHIEF, COMPUTER SECURITY DIVISION, NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY, DEPARTMENT OF COMMERCE

Mr. YORAN. Good afternoon, Chairman Putnam and distinguished members of the subcommittee. I am pleased to have an opportunity to appear before the committee to discuss cyber security challenges facing home users and small businesses. Small businesses do not have the same security resources as large companies, and as a result, their systems are often more vulnerable. Many home users are not aware of cyber security threats, or how to protect themselves.

The Department of Homeland Security's U.S. CERT has established a series of programs focused on home users and small businesses to target their specific needs. These programs leverage several mechanisms to enhance our communication to the public. December's National Cyber Security Summit established an Awareness and Outreach Task Force to provide recommendations for increasing awareness among home users and small businesses.

In March, the Task Force submitted its recommendations to the National Cyber Security Partnership. We have implemented a number of recommendations, as I will describe this afternoon, and are considering others as part of our overall awareness efforts. Many of these recommendations and efforts are consistent with the recommendations of your CISWG.

DHS is a sponsor of the National Cyber Security Alliance and Staysafe Online, a public/private organization created precisely to educated home users and small businesses on cyber security best practices. Other NCSA sponsors include the Federal Trade Committee, AT&T, America On-Line, Computer Associates, ITAA, Net-

work Associates, Symantec, and recently the Cyber Security Industry Alliance.

The Department of Homeland Security has provided matching funds to expand NCSA's outreach campaign. DHS' U.S. CERT launched the National Cyber Alert System in January of this year. The National Cyber Alert System is an important mechanism for delivering targeted, timely, and actionable information to help Americans protect their systems.

We have already issued several alerts and a periodic series of best practices and how-to guides. These tips help educate home users and small businesses on security practices and increase awareness. Some topics have included: Understanding Firewalls, Good Security Habits, Choosing and Protecting Passwords, and Why Cyber Security is a Problem.

I am pleased to announce that DHS' U.S. CERT and the Multi-State Information Sharing and Analysis Center [MSISAC], are developing a series of national Webcasts to examine critical and timely cyber security issues. The first Webcast planned for this series will take place next Tuesday, June 22nd.

These Webcasts will be archived and put on the U.S. CERT.gov Web site and available for public viewing. This national Webcast initiative is a collaborative effort between Government and private sector to help strength our Nation's cyber readiness and resilience. Webcasts will feature a variety of cyber security topics of interest to Government agencies, enterprises, and small businesses. Future sessions will focus on home users. These Webcasts are a strategic awareness tool to help home users and small businesses improve their cyber security posture and practices.

In addition, DHS' U.S. CERT supports the Internet Security Alliance's Common Sense Guide to Cyber Security for Small Businesses. This guide was produced as a result of focus groups, in coordination with the U.S. Chamber of Commerce, the National Association of Manufacturers, and the National Federation of Independent Businesses, and the Electronic Industry Alliance. NCSA is posting this guide on the U.S. CERT.gov Web site and requests that it also be placed on other appropriate homeland security and Government Web sites.

DHS and the Department of Justice's Bureau of Justice Statistics are producing a study on the effects of cyber crime in the United States, including those crimes affecting home users and small businesses. The goal of this survey is to provide comprehensive and statistically relevant information on the subject of cyber crime in the United States. This information can be used in a number of ways, including strategic information, technology, security planning, and resource allocation. It can help better prepare small businesses to address their cyber security challenge.

While we are optimistic that many of these efforts will help home users and small businesses increase their awareness and better protect themselves, we also believe that effective cyber security is a difficult challenge for these groups. The Department of Homeland Security is working with leading Internet service providers and technology providers in the private sector to make cyber security simpler to achieve for all.

Thank you for the opportunity to testify before you today. I would be pleased to answer any questions you may have. I would ask that my testimony be included in its entirety.

Mr. PUTNAM. Without objection, so ordered.

[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
"Locking Your Cyber Front Door – The Challenges Facing Home Users and Small Businesses"

Before the Subcommittee on Technology, Information Policy, Intergovernmental Relations, and the Census
Committee on Government Reform
U.S. House of Representatives
June 16, 2004

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 (NCSD) of the Office of Infrastructure Protection in the Department of Homeland Security's (DHS) Information Analysis and Infrastructure Protection Directorate. As we approach NCSD's one-year anniversary, I am pleased to have an opportunity to appear before the committee again to discuss the cyber security challenges facing home users and small businesses. It is important to understand the unique challenges that small businesses and home users face in their cyber security. Small businesses typically do not have the same information technology resources as large companies, and, as a result, their systems may be more vulnerable. While there is now a proliferation of computers in people's homes, many home users are not aware of cyber security threats, nor what steps they need to take to protect themselves. To help all of these groups increase their cyber security, we have established a series of programs geared towards home users and small businesses that focus specifically on their needs and level of understand. Thus, the outreach, awareness, and education initiatives by NCSD provide crucial information and resources to help secure the computers of home users and small businesses.

Introduction

NCSD was created in June 2003 to serve as the 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. Since our creation, we have been evaluating and securing our areas of greatest vulnerability, in partnership with private industry.

DHS is working closely with our partners in the federal government, the private sector, and academia on a variety of programs and initiatives. DHS recognizes that each entity may bring unique capabilities, responsibilities, and/or authorities to bear on cyber security issues. We recognize that the challenge of securing cyberspace 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, the cyber environment in

which the world operates is constantly changing. We recognize that information sharing, education and awareness, and coordination are crucial to improving our overall national and economic security. Cognizant of these realities, our cyber security initiatives 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

Tools and Strategies Available to Home Users and Small Businesses

A core component of Priority III of the Strategy is to promote a comprehensive national awareness program to empower all Americans, business, the general workforce, and the general population, to secure their portion of cyberspace. The Strategy clearly identifies home users, small and 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 as the users and cyber security stakeholders. 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 a 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 has built a cyber watch and warning capability and is launching the US-CERT Partner Program to build situational awareness, cooperation, and coordination with U.S. Government agencies and the private sector to deter, prevent, respond to and recover from cyber – and physical – attacks. Through the Homeland Security Information Network (HSIN)/US-CERT secure portal, US-CERT is a crucial component of – and a distribution tool for – cyber security awareness activities.

DHS and the US-CERT are engaged in several activities that enhance our communication to the public in a variety of ways. I will outline them in my testimony today, but first I want to share with you our newest initiative. I am happy to announce that US-CERT and the Multi-State Information Sharing and Analysis Center (MS-ISAC) are forming a joint partnership focused on developing a series of national webcasts which will examine critical and timely cyber security issues. The first webcast to be launched in this series will be open to government participants and will take place next Tuesday, June 22nd. Embracing the concept that *security is everyone's responsibility*, these webcasts will be archived, put on the website, and will be open to public view to help raise awareness and knowledge levels. The National Webcast Initiative is a collaborative effort between government and the private sector to help strengthen our Nation's cyber readiness and resilience. Webcast sessions will feature variety of cyber security topics that are both technical and non-technical, and future sessions may focus specifically on home users and small businesses. There is no charge for participation in the webcasts, which makes them accessible to home users and small businesses. DHS views these webcasts as another strategic awareness tool that will further help home users and small businesses improve their cyber security posture.

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. It is our responsibility to provide actionable information to the public so that they can take the necessary precautions to protect their systems. Furthermore, it is also important to inform the public about the true nature of a given incident, what the facts and possibilities are, and, most importantly, what the potential consequences may be if preventative action is not taken. This information is especially crucial in helping home users and small businesses secure their systems. The offerings of the National Cyber Alert System provide detailed and accurate information about imminent threats and incidents. We have already issued several alerts and the initial products in a periodic series of "best practices" and "how-to" guidance messages. To help educate home users and small businesses, regardless of computer skill-level, the alert system provides information in both technical and non-technical format. Additionally, US-CERT cyber tips help to educate home users on basic security practices and increase overall awareness. Since the release of the system, DHS has issued alerts on such topics as: "Understanding Firewalls;" "Good Security Habits;" "Choosing and Protecting Passwords;" and "Why is Cyber Security a Problem?"

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.

DHS is aware of the power of the media as an education and awareness vehicle, as well as a significant form of outreach to home users and small businesses. 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.

An industry-led coalition of interested security experts from the public and private sector was created as part of the National Cyber Security Summit process in December of 2003. At that time, the Awareness and Outreach Task Force was established to provide recommendations for increasing awareness among home users and small businesses. In March, 2004, this task force submitted its recommendations to the National Cyber Security Partnership. A number of these recommendations are being considered by DHS as a part of both an overall awareness effort and the partnership between DHS and the National Cyber Security Alliance and other groups.

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, Information Technology Association of America, 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. Coinciding 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. 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.

NCSD is also partnering with the Department of Justices' Bureau of Justice Statistics (DOJ/BJS) to study the effects of cyber crime in the U.S, including crimes affecting home users and small businesses. Although a number of other studies related to cyber crime are conducted every year, none of these studies has ever been statistically valid, due to their scope, format, question samples, or response rate. NCSD was approached earlier this year by the DOJ/BJS to partner in this significant effort to undertake the first widespread and statistically valid study of cyber crime. The initial distribution will be to 36,000 thousand individuals and businesses, including small businesses, covering all of the critical infrastructure sectors and the goal survey response

rate is 60 percent. By comparison, the most widely referenced, current, annual survey on cyber crime is distributed to less than 2000 businesses, and has never received a response rate of better than 15 percent. The goal of the survey is to provide comprehensive and statistically relevant information on the subject of cyber crime in the United States for the first time. This information can be used by industry in any number of ways, including strategic information technology security planning and resource allocation, and can help better prepare small businesses target specific, cyber security needs.

Finally, the U.S. Government is pursuing a number of avenues to address cyber security in our education system and working closely with the research and academic communities to better educate and train future cyber analysts. Recent successes include a Memorandum of Agreement (MOA) between DHS and the National Security Agency (NSA) to expand NSA's Centers of Excellence in Information Assurance Program into a national program. This will accelerate and expand the current program, attain national prominence, and result in participation from additional universities. The net result is that the U.S. 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.

Conclusion

DHS is committed to providing effective cyber security tools and education to home users and small businesses through our many outreach, awareness, and education efforts. The establishment of the US-CERT and its National Cyber Alert System provide the first step toward a national awareness campaign. As previously described, the alert system provides periodic alerts, tips, best practices and other guidance for dissemination to all sectors of our society. DHS also provides cyber security tips to home users and small businesses through the National Cyber Security Alliance *StaySafeOnline* campaign to help educate all users about basic security practices and to increase overall awareness as well as cyber security tool kits that can be disseminated to both groups.

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

Mr. PUTNAM. Thank you very much. I appreciate your adhering to our 5-minute rule so that we can get as much done as possible this afternoon.

Our next witness is J. Howard Beales. Mr. Beales is the Director of Federal Trade Commission's Bureau of Consumer Protection. He was appointed in June 2001. He has experience in both academia and Government. His major areas of expertise and interest include law and economics, the economic and legal aspects of marketing and advertising, and other aspects of Government regulation of the economy.

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

Mr. BEALES. Thank you, Mr. Chairman. I appreciate the opportunity to appear before you today to discuss the challenges that consumers and businesses face in protecting their computer systems and the information contained in them, as well as the FTC's role in promoting a culture of security.

Today, maintaining the security of our computer-driven information systems is essential to every aspect of our lives. Our interconnected information systems provide enormous benefits to consumers, businesses, and Government alike. But serious vulnerabilities threaten the security of the information they contain, as well as the continued viability of the systems themselves. Every day security breaches cause real and tangible harms to businesses and other institutions, as well as to consumers.

The FTC has sought to address concerns about the security of our computer systems through a combined approach that stresses education, law enforcement actions, and international cooperation.

Regarding education, one of our most successful strategies is to hold public workshops designed to educate the agency and the public about issues related to information security. One such workshop held in two sessions during May and June of last year, specifically explored the issues before the committee today.

Workshop participants identified a range of challenges facing consumers, industry, and policymakers. For example, many consumers do not buy the privacy tools now on the market because they are often available only as expensive hard-to-use system add-ons. Consumers also use these tools improperly. For example, failing to configure their firewalls appropriately, using easily guessed passwords, or using anti-virus software and operating systems without properly updating them.

Moreover, many consumers are largely unaware of the consequences of poorly protected systems and personal information. Panelists also urged technology vendors to make security support and updates easier and more automatic for consumers. Many panelists agreed that privacy-enhancing technologies, in order to be most effective, should be more tightly integrated or baked into systems so that even novice users can easily enjoy their protections.

To help businesses better develop ways to protect their systems, panelists urged the adoption of a comprehensive risk-management strategy that incorporates four critical elements—people, policy, process, and technology. Companies must train their people about the threats to the information systems and the steps they should take to address them. Companies must also develop and communicate policies regarding the appropriate use of information and

computer systems, and put in place processes to ensure that polices are implemented. Finally, they must deploy technology effectively and securely.

One valuable tool to help consumers understand the importance of information security, and to use privacy tools more effectively are educational campaigns similar to the campaigns launched to increase seatbelt use or discourage smoking. Such campaigns can take awhile to produce changes in consumer behavior, but they can help consumers play a more effective role in protecting themselves and society as a whole.

The FTC has, for several years, engaged in a broad outreach campaign to educate businesses and consumers and 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, Dewey the E-Turtle, who hosts a portion of the FTC Web site devoted to educating businesses and consumers about security.

We published Business Guidance regarding common vulnerabilities in computer systems and responding to information compromises. Commissioners and the staff have made speeches. We have worked with the Department of Homeland Security and such organizations as the National Cyber Security Partnership. We have reached out to the international community.

Even if consumers do everything right, however, their personal information may still be vulnerable if the businesses who obtain that information fail to protect it. Therefore, the Commission has also pursued law-enforcement actions in appropriate cases. In four separate settlements with companies that collected sensitive information from consumers, we have alleged that the companies violated the FTC Act by making promises that they would take appropriate steps to protect sensitive information obtained from consumers. In fact, we found their security measures to be inadequate and their claims, therefore, deceptive.

The Commission also has responsibility for enforcing its Gramm-Leach-Bliley-Safeguards Rule which regards financial institutions to protect customer information. In brief, the rule requires them to develop a written information security plan that includes certain elements basic to security. These include identifying and assessing the risks in each relevant area of the company's operation, and designing and implementing appropriate safeguards for controlling these risks. Companies must also regularly monitor and test their programs and evaluate and adjust the program in light of relevant circumstances.

In addition to our domestic efforts, the Commission has taken an active international role in seeking to establish a culture of security. We have worked on cyber security initiatives with OECD, as well as other international organizations.

Security presents challenges for everyone in our global information-based economy, but particularly for consumers and small businesses. We are committed to continuing our work promoting security awareness and sound information practices through education,

enforcement, and cooperation.

Thank you for the opportunity. I look forward to questions. I would ask that my testimony be included in its entirety.

Mr. PUTNAM. Without objection, so ordered.

[The prepared statement of Mr. Beales 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

INFORMATION SECURITY –
CHALLENGES FOR CONSUMERS AND BUSINESSES

June 16, 2004

I. Introduction

Mr. Chairman and members of the subcommittee, I am Howard Beales, Director of the Federal Trade Commission's Bureau of Consumer Protection.[1] I appreciate the opportunity to appear before you today to discuss the challenges consumers and businesses face in protecting their computer systems – and the information contained in them – as well as the Commission's role in promoting a culture of security.

Today, maintaining the security of our computer-driven information systems is essential. A secure information infrastructure is required for the operation of everything from our traffic lights to our credit and financial systems, nuclear and electrical power supplies, and emergency medical service. Consumers rely on and use computers at work and at home; increasingly, 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 them, 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] Securing these systems against an ever-changing array of threats is challenging, particularly for consumers and small businesses.

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 its other

consumer protection efforts. The Commission has sought to address concerns about computer security through a combined approach that includes educating consumers and businesses about emerging threats and the fundamental importance of good security practices; targeted law enforcement actions; and international cooperation. The Commission's educational efforts include public workshops to highlight emerging issues, consumer and business education to help identify risks to personal information and promote a "Culture of Security," and business education to promote compliance with relevant laws. In information security matters, the Commission's enforcement tools derive from Section 5 of the FTC Act,[3] which prohibits unfair or deceptive acts or practices, and the Commission's Gramm-Leach-Bliley Safeguards Rule ("Safeguards Rule" or "Rule").[4] In addition, in an increasingly global economy, international collaboration is fundamental to ensuring the security of consumers' information.

A. Workshops, Education, and Outreach

1. Security Challenges and Possible Solutions

One of the Commission's most successful strategies in this area is to hold public workshops designed to educate the agency and the public about issues related to information security. One such workshop, held in two sessions during May and June 2003, specifically explored the issues before this subcommittee today – namely, the challenges consumers and businesses face in securing their computers.[5] Titled "Technologies for Protecting Personal Information: The Consumer and Business Experiences," the workshop also examined the role of technology in meeting these challenges.[6] What the agency learned from that workshop is summarized in a recently released Staff Report,

available on the FTC website.[7]

Workshop participants included industry leaders, technologists, researchers on human behavior, and representatives from consumer and privacy groups. The panelists identified a range of challenges facing consumers, industry, and policy makers. For example, many consumers do not buy the privacy tools now on the market because they are often available only as expensive, hard-to-use system add-ons. Consumers also use these tools improperly – for example, failing to configure their firewalls appropriately, using easily-guessed passwords, or using anti-virus software and operating systems without properly updating them. Moreover, many consumers are largely unaware of the consequences of poorly protected systems and personal information. These consequences can range from identity theft to converting personal computers to "zombie drones" that spew out spam, to the use of a consumer's system in an attack on a commercial Web site or on part of the nation's critical infrastructure. Some consumers also have difficulty understanding businesses' privacy policies.

In addition, a number of panelists cited the shortcomings of existing technological tools used by both consumers and businesses, such as secure socket layer (SSL) encryption and virtual private networks. Many agreed that SSL should be implemented more widely; however, they cautioned that SSL may give users a false sense about the security of their data at its ultimate destination, as it only encrypts data in transit and does not assure that information will be stored securely or used as stated in a privacy policy. Some also cited the security risks posed by the connection of unsecure machines to virtual private networks, which allow employees away from their offices to connect to their employer's systems. If an employee's machine is not properly configured, attackers could use it to access the virtual private network and enter the employer's system.

Finally, panelists criticized the rapid introduction of technology, hardware, and software without adequate testing and quality assurance. They also noted the general trend toward poor accountability and limited IT training budgets for the protection of consumer information.

Panelists discussed a variety of ways to address these challenges. To help consumers understand the importance of information security and use privacy tools more effectively, panelists discussed the value of an educational campaign similar to the ones launched to increase seatbelt use or discourage smoking. Such a campaign may take time to produce changes in consumer behavior, but could ultimately teach consumers to take a more proactive role in protecting their computers and their personal information. Panelists also urged technology vendors to make security support and updates easier and more automatic for consumers, especially for legacy systems that remain in widespread use and are highly vulnerable to intrusion. Many panelists also agreed that privacy-enhancing technologies, in order to be most effective, should be more tightly integrated or "baked in" to systems so that even novice users can easily enjoy their protections.

To help businesses develop better ways to protect their systems, panelists urged the adoption of a comprehensive risk-management strategy that incorporates four critical elements: (1) people, (2) policy, (3) process, and (4) technology. Panelists discussed how each of these elements plays a role in security problems and solutions. For example, companies must (1) train their *people* about the threats to information systems and the steps they should take to address them; (2) develop and communicate *policies* regarding the appropriate use of information and computer systems; (3) put in place *processes* to ensure that policies are implemented; and (4) deploy *technology* effectively and securely. Panelists also discussed a variety of recent initiatives, in both the public and private sectors, that have applied these principles. For example, companies have worked to reduce security

flaws in code, ship products in a more secure configuration, add new security features to products, and provide better security support, such as patching and warnings, to their already-deployed products. The Department of Homeland Security has also successfully deployed its new National Cyber Alert System to warn businesses and consumers quickly about urgent security threats, and provide information on effective security policy and processes.

Panelists also discussed the extent to which benchmarks and standards can help provide guidance to industry on the effective management of security issues and, in particular, how to develop effective security programs. For example, the Center for Internet Security (CIS)[8] has produced benchmarks for a variety of technologies, including operating systems, routers, and databases, which provide detailed guidance on how to configure technologies for increased security. Business have used these benchmarks to develop minimum security requirements for merchants authorized to accept certain payment cards and to set configuration requirements in connection with large technology purchases.

2. FTC's Information Security Campaign

In addition to holding workshops, the FTC has for several years engaged in a broad outreach campaign to educate businesses and consumers about 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;[9] publication of business guidance regarding common vulnerabilities in computer systems[10] and responding to information compromises;[11] 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[12] has registered more than 620,000 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 also participated in more than 20 town-hall meetings about consumer protection and information security issues. Further, 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.

In addition, the FTC is working with the Department of Homeland Security (DHS) and such organizations as the National Cyber Security Partnership and the National Cyber Security Alliance Stay Safe Online[13] to promote its educational campaign more broadly. The National Cyber Security Partnership created five task forces to examine (1) home user awareness; (2) corporate governance; (3) cyber security early warning; (4) software development; and (5) technical standards and common criteria. This Spring, 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.

Finally, the Commission uses opportunities that arise in non-security cases to educate the public about security issues. For example, when the Commission filed a case challenging an alleged practice that bombarded consumers' computers with repeated Windows Messenger Service pop-up ads,[14] the agency also issued a consumer alert providing instructions on how to disable the Windows Messenger Service to avoid other pop-up spam. The alert[15] also discusses the use of firewalls to block hackers from accessing consumers' computers.

3. "Phishing"

The Commission has also issued a number of alerts to consumers about "phishing."[16] Phishing is an increasingly common 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.

4. Spyware

Finally, just this April, the Commission hosted a workshop to explore issues associated with "spyware" – software that is loaded on personal computers without users' consent.[17] The discussion at the workshop clarified that some of this software can cause privacy, security, and functionality problems for consumers. In particular, spyware may harvest personally identifiable information from consumers through monitoring computer use without consent. It also may facilitate identity theft by surreptitiously planting a keystroke logger that records the characters typed on a user's personal computer, including passwords, credit card numbers, and other personal information. Spyware may create security risks if it exposes communication channels to hackers. It also may affect the operation of personal computers, causing crashes, browser hijacking, home page resetting, and the like. These harms are problems in themselves, and could lead to a loss in consumer confidence in the Internet as a medium of communication and commerce.

The Commission's workshop also clarified how spyware can cause problems for businesses,

too. Companies may incur costs as they seek to block and remove spyware from the computers of their employees. Employees will be less productive if spyware causes their computers to crash or they are distracted from their tasks by a barrage of pop-up ads. Spyware that captures the keystrokes of employees could also be used to obtain trade secrets and other confidential information from businesses.

Fortunately, substantial efforts are currently underway to address spyware. In response to market forces, industry is developing and deploying new technologies to assist consumers. Consumers and businesses are becoming more aware of the risks of spyware, and they are responding by installing anti-spyware products and other measures. Industry representatives have indicated that they will explore best practices and consumer education on issues related to spyware. Government and industry-sponsored education programs, as well as industry self-regulation, could be instrumental in making users more aware of the risks of spyware, thereby assisting them in taking actions to protect themselves. All of these efforts are very encouraging. We are also actively investigating particular instances of questionable practices, and will take law enforcement actions as appropriate.

B. Law Enforcement

Regardless of how well consumers secure their own information and computer systems, their personal information may still be vulnerable if the businesses with which they interact fail to implement safeguards. Therefore, in addition to its education and outreach efforts, the Commission has also protected consumers by pursuing law enforcement actions in appropriate cases.

1. 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."[18] To date, the Commission's security cases have been based on deception,[19] 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.[20] In four separate cases, brought against Eli Lilly,[21] Microsoft,[22] Guess,[23] and Tower Records,[24] the Commission alleged that the companies 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 were, therefore, deceptive.

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

- ***Security Procedures Should Be Appropriate Under the Circumstances***

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.

- ***Not All Security Breaches Are Violations of FTC Law***

In the information security area, 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 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.

- ***Law Violations Without a Known Breach of Security***

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 threats before a compromise occurs.

- ***Good Security is an Ongoing Process of Assessing 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.

2. GLB Safeguards Rule

In addition to 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.[25] 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 non-bank 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 significantly reduce risks to this information, including identity theft.

The Rule requires covered 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 gives each company the flexibility to develop a plan that takes into account 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 Commission has issued guidance on the Rule[26] and met with a variety of trade associations and companies to promote compliance. Currently, Commission staff is conducting non-public investigations of covered entities.

Finally, pursuant to the Fair and Accurate Credit Transactions Act of 2003 ("FACT Act"),[27] the Commission recently issued a proposed rule designed to enhance the security of consumer report information.[28] The proposed rule is designed to prevent unauthorized disclosure of consumer information and to reduce the risk of fraud or identity theft by ensuring that records

containing sensitive financial or personal information are appropriately redacted or destroyed before being discarded. The Commission anticipates the issuance of a final rule by the end of the year.

C. International Efforts

In addition to its law enforcement and education efforts, the Commission has taken an active international role in promoting cybersecurity. The Commission recognizes 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. The Commission is 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."[29] 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 will remain 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."[30] 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.[31]

III. Conclusion

Security presents challenges for everyone in our global information-based economy, but particularly for consumers and small businesses. The Commission is committed to continuing its work promoting security awareness and sound information practices through education, enforcement, and international cooperation.

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 Commissioner.

2. For example, the Commission's 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. In May 2002, the Commission also held a workshop on Consumer Information Security. For more information, including transcripts of the workshop, *see* http://www.ftc.gov/bcp/workshops/security/index.html.

6. The workshop agenda and transcripts are available at www.ftc.gov/bcp/workshops/technology.

7. The Staff Report is available at http://www.ftc.gov/bcp/workshops/technology/finalreport.pdf.

8. The Center for Internet Security is a non-profit organization whose mission is to help organizations around the world effectively manage the risks related to information security. CIS manages a consensus process in which members identify security threats of greatest concern, then participate in development of practical methods to reduce the threats. CIS also provides methods and tools to improve, measure, monitor, and compare the security status of Internet-connected systems and appliances. *See* http://www.cisecurity.org.

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

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

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

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

13. The National Cyber Security Partnership is a 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.

14. *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.

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

16. *See*, e.g., http://www.ftc.gov/bcp/conline/pubs/alerts/phishregsalrt.htm. Working closely with the FBI and Department of Justice, the Commission has also brought enforcement actions challenging unfair and deceptive practices in connection with "phishing." *See* cases cited *infra* note 19.

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

18. 15 U.S.C. § 45 (a) (1).

19. 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. Dec. 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.

20. 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.).

21. Final Decision and Order at www.ftc.gov/os/2002/05/elililldo.htm; Complaint at www.ftc.gov/os/2002/05/elililldycmp.htm.

22. Final Decision and Order at http://www.ftc.gov/os/2002/12/microsoftdecision.pdf; Complaint at http://www.ftc.gov/os/2002/12/microsoftcomplaint.pdf.

23. Final Decision and Order at http://www.ftc.gov/os/2003/06/guessagree.htm; Complaint at http://www.ftc.gov/os/2003/06/guesscmp.htm.

24. Final Decision and Order at http://www.ftc.gov/os/caselist/0323209/040602do0323209.pdf; Complaint at http://www.ftc.gov/os/caselist/0323209/040602comp0323209.pdf.

25. 16 C.F.R. Part 314, available online at http://www.ftc.gov/os/2002/05/67fr36585.pdf. Pursuant to Section 501(b) of the Gramm-Leach-Bliley Act, the federal banking agencies have issued similar security guidelines that apply to the financial institutions they regulate. *See* Interagency Guidelines Establishing Standards for Safeguarding Customer Information, 12 C.F.R. Parts 30, app. B (OCC); 208, app. D-2 and 225, app. F (Board); 364, app. B (FDIC); 570, app. B (OTS).

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

27. The Fair and Accurate Credit Transactions Act of 2003 ("FACT Act"), Pub. L. No. 108-159 (2003). In general, the FACT Act amends the Fair Credit Reporting Act to enhance the accuracy of consumer reports and to allow consumers to exercise greater control regarding the type and amount of marketing solicitations they receive. The Act also contains a number of provisions intended to combat consumer fraud and related crimes, including identity theft.

28. *See* Disposal of Consumer Report Information and Records, 69 Fed. Reg. 21,388 (2004) (to be codified at 16 C.F.R. Part 682); available at http://www.regulations.gov/fredpdfs/04-08904.pdf.

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

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

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

Mr. PUTNAM. Thank you very much.

Our next witness is Cheryl Mills. Ms. Mills is the Associate Administrator, Entrepreneurial Development for the U.S. Small Business Administration. She manages SBA's Technical Assistance Programs, providing information, training, and business counseling for 1.4 million small business owners nationwide. Her office provides this service through a variety of business-development networks across the Nation.

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

Ms. MILLS. Thank you very much, Mr. Chairman. Chairman Putnam and members of the subcommittee, I appreciate the opportunity to testify before you today about an issue that is of utmost importance in today's business world—securing our Nation's vast information technology network.

There are 25 million small businesses in America, but today's small businesses are nothing like the Mom-and-Pop entrepreneurs of 50 years ago, whose market place was often limited to their local community. In 2004, America's small businesses are national and global enterprises who ship their products across the country and around the globe. The main reason for this change to the small business landscape is computer technology. Today's entrepreneurs use computers and the Internet to market their products, purchase supplies and equipment, and correspond quickly with customers.

While the SBA is most often associated with our successful loan program, we are also very proud of the valuable technical assistance that we provide to America's entrepreneurs. As ADA for entrepreneurial development, I am responsible for seeing that program.

The SBA provides technical assistance through our core infrastructure of small business developmental centers, women's business centers, SCORE counselors, and our district offices. The resources are spread throughout the country in over 1,200 locations. In 2003, these resource partners provided technical assistance to over 2 million small businesses.

Through this infrastructure, the SBA has worked to address the challenges of IT security. One way we see of doing this is obviously by partnering with other Federal agencies, as well as the private sector to educate small businesses about the benefits and the risks associated with today's technology-based business world.

In 2002, SBA teamed up with the Hartford to distribute over 25,000 copies of a guidebook entitled, "Managing Your Risk: The Smart Approach to Protecting Your Business." It provided management guidance on a variety of topics including computers and E-Commerce risks.

Throughout 2003, SBA and the Hartford conducted 10 risk-management seminars for 500 small business entrepreneurs and published an audio tape and CD ROM on IT security. In addition, the SBA is working in collaboration with the FBI and NIST on a series of regional meetings on IT securities for small businesses. These meetings have provided small business with an overview of information on security threats, vulnerabilities, and corresponding protective tools and techniques. Through this partnership, we have reached over 800 small businesses just in 11 seminars.

Like the cosponsorship agreement with the Hartford, SBA is currently considering collaboration with the U.S. Chamber of Commerce to publish a guide to cyber security. The SBA and the Chamber will work together to ensure this publication will be distributed to as many small businesses as possible.

Also, through our Small Business Training Network [SBTN], at www.sba.gov/training we provide on-line training and have provided that already to nearly 650,000 entrepreneurs in 2003. We offer a variety of E-Commerce counseling courses. One of the most popular is entitled, Information Security Basics. That was developed in collaboration with the George Washington University. This multi-part course is designed to help a small business to understand the importance of implementing a sound information security plan.

SCORE also provides counseling on a range of E-Commerce topics from How to Combat Computer Viruses to Understanding Customer Privacy Issues. Earlier this year, the Association of Small Business Developmental Centers partnered with Microsoft to develop and introduce the E-Security Guide for Small Business. I have provided the subcommittee with a copy of this guide which is also available on-line. SBDC can utilize the E-Security Guide's information when working now with a small business client.

Mr. Chairman, I want to assure you that this administration remains committed to providing our Nation's small businesses with the tools they need to survive in today's global market place. I look forward to listening to the other panelists, and also working with the subcommittee to continue serving the IT security needs of the small business community.

Thank you. I would be happy to answer any questions. I would ask that my testimony be included in its entirety.

Mr. PUTNAM. Without objection, so ordered.

[The prepared statement of Ms. Mills follows:]

Testimony of
U.S. Small Business Administration (SBA)
Associate Deputy Administrator Cheryl Mills
before the
House Government Reform Subcommittee on
Technology, Information Policy, Intergovernmental Relations,
and, the Census

June 16, 2004

Chairman Putnam, Ranking Member Clay, Members of the Subcommittee, I appreciate the opportunity to testify before you today about an issue that is of the utmost importance in today's business world; securing our nation's vast Information Technology (IT) network. My name is Cheryl Mills, and I serve as the Associate Deputy Administrator for Entrepreneurial Development at the U.S. Small Business Administration.

There are 25 million small businesses in America, but today's small businesses look nothing like the "mom and pop" entrepreneurs of fifty years ago whose marketplace was often limited to their local community. In 2004, America's small businesses are national, even global, entrepreneurs who ship their products across the country and around the globe.

The main reason for this change to the small business landscape is computer technology. Today's entrepreneurs use computers and the Internet to market their products, purchase supplies and equipment, and to run their businesses more efficiently. Basically, IT has allowed small business to compete in the world of big business.

However, as this Subcommittee is well aware, there are also risks associated with this new technology age. Cyber-security affects all Internet users, including small business. And for many small businesses, effectively managing this risk is the difference between a successful business and failure.

Assisting small businesses in meeting the varied and often unique challenges they face on a daily basis is one of the reasons the U.S. Small Business Administration (SBA) was created. While the SBA is most often associated with our successful loan programs, we are also very proud of the valuable technical assistance that we provide to America's entrepreneurs. As ADA for Entrepreneurial Development, I am responsible for overseeing the SBA programs that provide technical guidance and assistance to small businesses across the country.

The SBA provides technical assistance to our Nation's small businesses through our core infrastructure of Small Business Development Centers (SBDC), Women's

Business Centers (WBC), the Service Core of Retired Executives (SCORE), and our district offices. These resources are spread throughout the country in over 1,200 locations. In FY 2003, these resource partners provided technical assistance to over 900,000 small businesses.

Through our core infrastructure, the SBA has worked to address the challenges of IT security. One way of doing this is by partnering with other Federal agencies, state and local entities, as well as the private sector, to educate small businesses about the benefits and risks associated with today's technology-based business world.

In 2002, SBA teamed up with The Hartford to distribute a guidebook entitled "Managing Your Risk: The Smart Approach to Protecting Your Business." This provided management guidance on topics ranging from product liability to workers' compensation. Included in this guidebook was a section on "Computers and E-Commerce Risks---Feel More Secure." SBA distributed over 25,000 copies of this guidebook through our network of resource partners.

Throughout 2003, SBA and The Hartford conducted 10 seminars for 500 small business entrepreneurs, and also published an audio tape and CD-ROM on IT security.

Also, the SBA signed a memorandum of understanding with the Federal Bureau of Investigations (FBI) and the National Institute of Standards and Technology (NIST) to conduct a series of regional meetings on IT security for small businesses. These meetings have provided small businesses with an overview of information security threats, vulnerabilities, and corresponding protective tools and techniques. A special emphasis is placed on providing useful information that small business IT personnel can apply directly or use to task contractor personnel.

Through this partnership, we have reached over 800 small businesses during 11 seminars.

Also, SBA is currently considering collaboration with the U.S. Chamber of Commerce (Chamber) to put out a guide to cyber security. Like the cosponsorship agreement with The Hartford, SBA would collaborate with the Chamber to ensure that this publication was distributed to as many small businesses as possible.

As I mentioned earlier, SBA's core infrastructure also plays a role in this process. In fact, the SBA offers an online counseling course entitled, "Information Security Basics," in collaboration with The George Washington University. This multi-part course provides training and guidance on network security, e-mail security and security policies. The course is designed to help a small business understand the importance of implementing a sound information security plan.

In addition, our webpage features other e-commerce counseling courses. SBA's online courses can be found by visiting our Small Business Training Network at *www.sba.gov/training*.

Similarly, SCORE provides counseling on a range of e-commerce topics, from how to combat computer viruses to understanding customer privacy issues. Along with that, our SCORE volunteers have a wide range of their own business experiences that they rely upon when counseling a small business.

In San Francisco, the SBDC has created a Technology Advisory Program (TAP) that help clients understand how information technologies can specifically improve the way they operate, identify the most appropriate technology solutions, adopt and properly utilize the recommendations. The TAP program offers a course entitled "Information Security for the Small Business."

Earlier this year, the Association of SBDCs partnered with Microsoft to develop and introduce the *e-Security Guide for Small Business.* This guide is available online, and SBDC counselors can utilize this information when working with a small business client. I have provided a copy of this guide for the Subcommittee's review.

Mr. Chairman, I want to assure you that this Administration remains committed to providing our Nation's small businesses with the tools they need to survive in today's global market place.

I look forward to listening to the other panelists and working with the Subcommittee to continue serving the IT security needs of the small business community.

Mr. PUTNAM. Thank you very much.

Our final witness on this panel is Mr. Ed Roback. Mr. Roback serves as Chief of the Computer Security Division at the National Institute of Standards and Technology, and supporting the agency's responsibilities to protect sensitive Federal information and promote security in commercial information technology products. The Computer Security Division's efforts include work in the area of security standards, testing E-Authentication, studying security issues with emerging technologies, and developing security guidelines for Federal agencies.

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

Mr. ROBACK. Thank you very much, Chairman Putnam and members of the subcommittee for this opportunity to testify today on the perspectives of the National Institute of Standards and Technology regarding the challenges facing home users and small businesses in better securing their systems and information.

Our broad work in the area of information security, generally speaking, is applicable to a wide variety of users, including small businesses as well as the larger agencies of the Federal Government. In particular, home users and small businesses face an enormous challenge in protecting their computers. Their systems are operated in environments where there is not normally full knowledge or understanding of potential risks or technology capabilities. The risks to our small systems are, in fact, so complex and pervasive, we cannot expect these small businesses to become experts in this area. Yet, they want to take advantage of new technologies along with all the risks that presents.

So today what I would like to do is to tell you a little bit about some work NIST has done in this area. As my colleague mentioned, NIST has formed a partnership with SBA and the Federal Bureau of Investigation's Infraguard Program to sponsor workshops and on-line support for small businesses. We have built a Small Business Resource Center on our Web site where we distribute training materials to be used by small businesses and in-house security sessions.

We have also provided briefings to organizations at various events engaged with small businesses across the country. NIST's manufacturing extension partnership also has developed a tool called E-Scan Security Assessment tool that provides the capability for small businesses to assess their security posture and recommends some security corrective measures.

In addition to these specific efforts, we believe that home users and small businesses can benefit broadly from the range of initiatives that are underway at NIST in the area of security guidelines, security research, security testing, and so forth. After all, we are all using the same commercial products.

I will not go into the details. That is all summarized in my written statement, but some of the guidelines such as wireless teleworking and other kinds of guidelines also obviously can apply to home users and small businesses.

I would like to highlight one piece of work in particular and that is our work with vendors to develop a Web-based repository on security check lists. As you know, many commercial products are delivered with security features turned off. The question for users is:

Well, what should I turn on in the area of security for my particular environment? We are in the process of developing IT security product checklists that provide settings and options to minimize the security risks associated with each computer hardware or software system widely used in the Federal Government which, of course, translates into nearly every commercial product.

In summary, Mr. Chairman, the challenges facing home users and small businesses is greater than it has ever been, but it is also very similar to those challenges facing Federal agencies and other users. We are all using the same products. We are all connected to the same networks.

If they are to maximize capabilities and efficiencies offered by these technologies while minimizing risks to their system, more must be done. Training efforts must be increased. More must be done in the area of secure configuration. More must be done in the area of product benchmarking, scanning tools, outreach, and indeed research so that we can improve the situation and simplify the current unfortunate complexity that exists in trying to secure these systems. We are at a situation right now where it is simply too much to expect small businesses to understand all the risks in order to be able to address their security needs.

Thank you, Mr. Chairman, for the opportunity to present our views regarding the security challenges facing home users. I would be pleased to take any questions you may have. I would ask that my testimony be included in its entirety.

Mr. PUTNAM. Without objection, so ordered.

[The prepared statement of Mr. Roback follows:]

Statement of

Edward Roback
Chief, Computer Security Division

National Institute of Standards and Technology
Technology Administration
U.S. Department of Commerce

Before the

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

"Locking Your Cyber Front Door – The Challenges Facing Home Users and Small Businesses"

June 16, 2004

Chairman Putnam, members of the Subcommittee, thank you for this opportunity to testify today on our perspective regarding the challenges facing home users and small businesses in better securing their systems and information. I would like to address the questions you asked in your invitation to testify and tell you about the numerous cybersecurity activities underway at NIST. Many of these can assist small businesses in implementing better security controls.

NIST has had a long-standing role in working effectively with industry and federal agencies in ensuring the protection of sensitive information and information systems. Our research helps protect the confidentially, integrity, and availability of information and system services. Helping to ensure secure flow of business-related information is essential to the functioning of our economy and indeed to our democracy. Our broader work in the area of information security is, generally speaking, applicable to a wide variety of users – from small business to the large agencies of the Federal government. Let me start by quickly reviewing our responsibilities in the area of information security.

NIST's Current Statutory Responsibilities

The Cyber Security Research and Development Act of 2002 assigned to NIST the following key responsibilities:

- Establish a program of assistance to institutions of higher education that enter into partnerships with for-profit entities to improve the security of computer systems;
- Institute a program to award post-doctoral research fellowships to individuals seeking research positions at institutions engaged in cybersecurity research;
- Develop checklists establishing settings and option selections that minimize security risks associated with federal government computer hardware or software systems;
- Support and consult with the Information System Security and Privacy Advisory Board, which has the mission to identify emerging issues related to computer security, privacy, and cryptography; and
- Conduct intramural cybersecurity security research.

The Federal Information Security Management Act (FISMA) of 2002 assigned NIST the following responsibilities:

- Developing IT standards and guidelines for the security of Federal systems;
- Conducting research to identify information security vulnerabilities and developing techniques to provide cost-effective security;

- Assessing private-sector policies, practices, and commercially available technologies;
- Assisting the private sector, upon request; and
- Evaluating security policies and practices developed for national security systems to assess potential application for non-national security systems.

With these broad legislative mandates in mind, let me now share our views on the issues posed by the Subcommittee.

Home users and small businesses face an enormous challenge in protecting their computers, which are connected to the Internet. These systems are operated in environments where there is normally not full knowledge or understanding of all of the potential security risks, created by connecting to the Internet. Indeed, the risks to our systems are so complex and pervasive, that we cannot reasonably expect small businesses people to become experts in this area. In addition, home users and small businesses, like all organizations, want to embrace and have available the latest advances in technology to make their tasks easier. For example, many may have no idea that their computers, if unprotected, can be used as zombies to launch distributed denial of service attacks. Many may not understand that sensitive information, residing on their machines, may be accessed and otherwise misused potentially resulting in great harm. Even if they have taken steps to minimize the opportunity for inappropriate access by investing in firewall technology and virus protection software, they may not have correctly installed, managed or updated those capabilities. They also face the challenges of trying to determine what security configuration settings should be in place for their systems (given their risk environments) – and then how to actually "turn on" those settings.

We are all experiencing receipt of an overwhelming amount of SPAM e-mail and unfortunately, although filters are available to assist in identifying and blocking SPAM, the spammers continue to find ways to circumvent these solutions. In large organizations, we are certainly better positioned both from a staffing and budget perspective to put very strong formal processes in place to monitor and manage our environments in order to make them more secure. SPAM is more than an inconvenience. SPAM may also deliver viruses or worms or have fraudulent intent. Phishing schemes, the Internet version of social engineering to fool individuals into divulging personal financial data such as credit numbers or social security numbers, have become pervasive. Uninformed home users and small businesses may become victims.

The vulnerability of any one small business may not seem significant to many other than the owner and employees. However, over 95 percent of all U.S. businesses are small or medium-sized. Many of these businesses house very sensitive personal information including healthcare or financial information. Many small businesses also provide services to our Federal, state, local and tribal governments and have access to government information or systems. Therefore a vulnerability common to a large

percentage of these organizations could pose a threat to the Nation's economy and overall security.

In the special arena of information security, vulnerable small businesses also run the risk of being compromised for use in crimes against governmental or large industrial systems upon which we all rely. Most small businesses cannot afford an extensive security program, or often even hire a single full time expert. Nonetheless, they confront serious security challenges and must address security requirements based on identified needs. The difficulty for these organizations is to identify cost-effective security mechanisms and obtain training that is practical and feasible for their environment. Such organizations also need to become more educated consumers in terms of security, so that their limited security resources are well applied to meet the most obvious and serious threats.

Hardware and software purchased by small businesses and home users today is frequently installed without making any changes from the original configurations delivered by the vendor. Unfortunately, in most cases, these configurations have not been optimized for security. This puts home users and small businesses at risk and they need to better educate themselves about security features and what the implications and risks are associated with poorly configured systems. Given the state of software insecurity today, vendors are frequently issuing security patches for their products. Users need to be aware of the importance of these patches, where to get up-to-date information about these patches, and procedures for installing them. I would point out that the efforts of the DHS US-CERT are particularly germane here. Lessening the burden on home users and small businesses must include greater efforts on the part of Government working with the IT vendor community in order to deliver more secure products to IT consumers.

In that regard, Mr. Chairman, I'd like to share with you some of the work NIST is doing to support security improvements in this area.

NIST has formed a partnership with the Small Business Administration (SBA), and the Federal Bureau of Investigation's InfraGard program to sponsor workshops and on-line support for small businesses. This Co-sponsorship, which began in FY2002, has just been renewed this year. Because our experience shows that it is often very difficult for a small business to spare a person even for a half-day workshop, we have built a Small Business Resource Center on the NIST web site where our training materials can be freely accessed and used by small businesses for distribution and in-house security sessions.

We have also provided briefings to organizations at various events engaged with small businesses to publicize these available resources such as the Association of Small Business Development Centers, The National Entrepreneurial Conference and Expo, SBA's Senior Corps of Retired Executives, and the American Association of Community Colleges where many small business owners may hire students. We also placed security tips in the SBA Solutions Newsletter, which reaches more than 14,000 business owners.

Another area in which NIST has provided assistance is through its Manufacturing Extension Partnership's eScan Security Assessment Tool. The eScan Security

Assessment provides the small business with a diagnostic tool designed to assess the electronic security infrastructure of a small business and provide an action plan for improving it through a set of recommendations to correct many security problems.

U.S. small manufacturers are dependent upon the secure and reliable processing, storage and transmittal of information to conduct their internal and external business. Information and knowledge about customers, orders, manufacturing and intellectual property are the primary assets of any private business. Unfortunately, many businesses are not aware of the latest strategies for ensuring the security of their physical workplace and their information systems. These issues are especially important in the many defense manufacturing supply chains, as the security of the information and the ability to maintain business continuity affect the security of the entire country.

The *e*Scan Security Assessment measures how well a business performs in these critical security areas:

- Strategies & Tactics for Virus Protection
- Physical Environment Security
- Contingencies for Mechanical Failures
- Security Policies & Procedures
- Internet and eCommerce Security
- File Permission Security
- Back-up Policies and Procedures
- Contingency Planning
- Miscellaneous Security Issues
- Operating System Security
- Wireless Security
- International eCommerce Concerns

The NIST MEP Centers are available to conduct the assessment and/or assist the company in solving their security issues. The eScan Security Assessment is available online at **http://escan.nist.gov/sat/index.nist**.

But in addition to these specific efforts, we believe that home users and small businesses can benefit greatly from a broad range of initiatives that we have undertaken. NIST continues to take strides toward securing the nation's infrastructure and support all users of information technology (IT) through its development of tools, standards, metrics and guidance.

Security Guidelines and Standards

We continue to develop standards and guidelines in support of our Federal responsibilities. Many of these are also used, on a voluntary basis, by organizations in the private sector. Hundreds of thousands of copies of our guidelines have been downloaded from our Computer Security Resource Center.

We recognize that the guidance, as written, has not been tailored for use by home users and small businesses, however, we are considering the development of a series of guidance which could be tailored for better usability by this group of users. The presentation would take the form of quick reference guides reinforcing good security principles and practices for specific IT components (Web, email, etc.).

A sample of some of our recent guidance releases is listed below:

- Wireless Network Security: 802.11, Bluetooth, and Handheld Devices;
- Security Guide for Interconnecting Information Technology Systems;
- Security for Telecommuting and Broadband Communications;
- Guidelines on Electronic Mail Security;
- Guidelines on Securing Public Web Servers;
- Systems Administration Guidance for Windows 2000 Professional;
- Guidelines on Firewalls and Firewall Policy;
- Procedures for Handling Security Patches;
- Contingency Planning Guide for Information Technology Systems; and
- Risk Management Guide for Information Technology Systems.

See http://csrc.nist.gov/publications/nistpubs/index.html .

Network Security

Mr. Chairman, I'm very pleased to note that at NIST, we are aggressively working on development of robust, resilient, agile networks as defense against the kind of distributed denial of services (DDoS) attacks cited in your invitation letter.

NIST's efforts in Internet security research are focused on both near term objectives of expediting significant improvements to the security and integrity of today's Internet technologies, and longer term objectives such as exploring the use of quantum information theory to develop ultra-secure networking technologies of the future.

Our near term research is directed at working with industry and other Government agencies to improve the interoperability, scalability and performance of new Internet security systems and to expedite the development of Internet infrastructure protection technologies. NIST staff is actively working with the Internet Engineering Task Force (IETF) to design, develop, standardize and test new protocols that will make authentication, confidentiality and integrity services inherent capabilities of all networks based upon Internet technologies. NIST has taken leadership roles within the IETF in the specification of public key infrastructure, network layer security and key management technologies. Working shoulder to shoulder with industry, NIST is contributing technical specifications, modeling and analysis results, research prototypes and test and measurement tools to the IETF community to expedite the standardization of ubiquitous Internet security services and to foster the rapid development of commercial products.

Another area of focus for our near term efforts is the research and development of technologies to protect the core infrastructure of Internet. NIST is working with the IETF and other government agencies to devise means to protect the control protocols and infrastructure services that underlie the operation of today's Internet. NIST's research and standardization efforts in this area include: extensions to the Domain Name System (DNS) to add cryptographic authentication to this most basic Internet service, and the design and analysis of protection and restoration mechanisms to improve failure resilience of core switching and routing infrastructures. Our future work in this area will focus on improving security and resilience of core Internet routing protocols.

Looking further into the future, we see the potential for new computational paradigms to threaten the mathematical underpinnings of today's cryptographic systems. In response, NIST is conducting research in the use of quantum information theory to devise ultra-secure network technologies that are not dependent upon today's cryptographic techniques.

Wireless Mobile Device Security

With the trend toward a highly mobile workforce, the acquisition of handheld devices such as Personal Digital Assistants (PDAs) is growing at an ever-increasing rate. These devices are relatively inexpensive productivity tools and are quickly becoming a necessity in today's business environment. Most handheld devices can be configured to send and receive electronic mail and browse the Internet. However, as handheld devices increasingly retain sensitive information or provide the means to obtain such information wirelessly, they must be protected.

Our efforts to date have focused on improving several aspects of security: user authentication, policy enforcement, and wireless communications. For user authentication we have developed a framework for multi-mode authentication that allows more than one authentication mechanism to contribute to the verification of a user's identity. For example, a biometric, such as voice input, may be required in combination with a security token, such as a smart card, before a user is permitted to access the contents of a device. In addition, we have invented a visual means of authentication that not only is easier than passwords for users to authenticate, but also significantly more powerful, and we have contributed updates to an open source code initiative that allow smart cards to be used on certain handheld devices.

For policy enforcement, we have developed a system that requires users to present a policy certificate to a device, as a means of moving from a restricted processing environment to one in which the privileges accorded a user via the policy certificate are enabled. Policy rules govern such things as application usage, file access, and communications interfaces, including wireless communications. This mechanism allows organization policy controls to be asserted on handheld devices, which typically are at the fringes of an organization's influence, and was designed to tie in with emerging Public Key Infrastructures.

For wireless communications, we have developed a highly-regarded publication on Wireless Network Security, aimed at reducing the risks associated with 802.11 wireless local area networks and Bluetooth wireless networks that are commonly used with handheld devices.

Security Awareness and Outreach

Timely, relevant, and easily accessible information to raise awareness about the risks, vulnerabilities and requirements for protection of information systems is urgently needed. This is particularly true for new and rapidly emerging technologies, which are being delivered with such alacrity by our industry.

We actively support information sharing through our conferences, workshops, web pages, publications, and bulletins. Finally, we also have a guideline available to assist agencies with their training activities and are an active supporter of the Federal Information Systems Security Educators' Association.

We sponsor the web-based Computer Security Resource Center (CSRC) to provide a wide-range of security materials and information to the community and link to the Federal Computer Incident Response Center at DHS and other emergency response centers. CSRC now has over 20 million "hits" annually. On CSRC, one of the most popular resources is the NIST-developed web-based tool known as ICAT that allows users to identify (and then fix) known vulnerabilities for their specific software. ICAT provides links to vendor sites at which the users can obtain patches to fix these vulnerabilities. This is important because many computer break-ins exploit well-known vulnerabilities. Over 6600 vulnerabilities are now catalogued in this NIST on-line database that receives over 200,000 hits per month. See http://icat.nist.gov/icat.cfm . While vulnerability patching is important, the sheer numbers of vulnerabilities and patches will become untenable in the long run. Users, including small businesses, should not be hesitant about expressing their needs for more secure, reliable, and robust software to vendors.

Security Assessment Guideline and Automated Security Self-Evaluation Tool (ASSET)

The Chief Information Officers Council and NIST developed a security assessment Framework to assist agencies with a very high level review of their security status. The Framework established the groundwork for standardizing on five levels of security and defined criteria agencies could use to determine if the levels were adequately implemented. By using the Framework levels, an organization can prioritize agency efforts as well as evaluate progress.

NIST Security Practices Web Sites

NIST operates the Federal Agency Security Practices (FASP) website to identify, evaluate, and disseminate best practices for CIP and security. The site contains many

agency policies, procedures and practices; the CIO pilot best practices; and, a Frequently-Asked-Questions section. Agencies are encouraged to share their IT security information and IT security practices and submit them for posting on the FASP site. Over 100 practices are now available via the site.

In accordance with tasking to NIST under FISMA, we are now expanding the service to share security practices from private-sector organizations.

Both of these sites may be of particular interest to small businesses.

IT Product Security Configuration Checklists

NIST is now in the process of developing IT product security checklists that provide settings and option selections that minimize the security risks associated with each computer hardware or software system that is, or is likely to become, widely used within the Federal Government. Vendors, agencies, and other reputable sources can use the template to construct and submit checklists that will populate a NIST public web-based repository. Within the next month we plan to publish a draft security guideline on checklist construction.

Closing

In summary, Mr. Chairman, the challenge facing home users and small businesses is greater than it has ever been. If they are to maximize all of the capabilities and efficiencies offered by emerging technology while minimizing risk to their systems and information, more must be done. Training efforts must be increased and more must be done in the areas of secure configuration settings, product benchmarks, outreach and research. Today, systems in homes and small businesses are part of a larger infrastructure. Those who have motivation to do harm normally will seek out the weakest link. Certainly, there is a high potential for malicious activity against these non-secured or poorly secured systems. As troubling as this is, of equal concern is the potential for accidental unauthorized disclosure of sensitive information or breach of privacy due to weak security controls on these systems.

We believe that some of the initiatives we've shared with you today, demonstrate our commitment to better national cybersecurity and recognize that more must be done by home users and small businesses to protect their information security.

Thank you, Mr. Chairman for the opportunity to present our views today regarding security challenges facing home users and small businesses. I will be pleased to answer any questions that you and the other members of the Committee may have.

Mr. PUTNAM. Thank you very much.

I want to thank all of our witnesses. I again apologize for the extended delay due to votes. I want to thank the gentleman from Pennsylvania for joining us, our distinguished member of the subcommittee. I will allow him to go first if he would prefer.

Mr. MURPHY. Thank you, Mr. Chairman. I appreciate that. I want to thank the committee, too. I know that this may not seem that exciting an issue to the general public but anybody who owns a computer in their home and anybody who has a business has more than once pounded that computer, saying "What is wrong with this thing?" We know that there could be some things to be taken care of. So your testimony is extremely important for business and for the home user.

I would like to ask about the role and response of the private sector here, including hardware and software vendors, PC makers, ISPs, etc., in contributing to its improve security profile of home users and small businesses. I think of it particularly here because, like anybody else, sometimes I will turn on my computer. Another family member may have been using it, or I will open up what I thought was an e-mail from a friend which may have something else attached to it.

I often times feel, like many other home users, "Why do I have to be the one always to pay the money here to prevent what the system is allowing through?" The software can add up over time, all the editions and updates. What can the private sector do to help everybody who is a small business person or just a home user of computers? I will take an answer from anybody here.

Mr. BEALES. Well, I think one thing that the private sector can do—and I think we are seeing this increasingly—is to build in some of the basic security features so that they are there for users who need them. When you get a broadband or "always on" connection of some sort, it comes with the basic security precautions installed that ought to accompany that kind of application. I think we are seeing more and more of that. It would be good to see more. But I think that is a very useful role for the private sector to play.

Mr. MURPHY. Does anyone else have any comments? Mr. Roback?

Mr. ROBACK. I think we also have to look at the power of the market place in terms of distinguishing the benefits folks can get from security and the ability and the willingness for people to pay for it. Right now people, of course, want security, but they are not necessarily willing to pay more per month for a service that provides a higher level of security. So we need to work.

Mr. MURPHY. I guess this relates also to small businesses and commerce. But there is a symbiotic relationship between, for example, people who want to be able to monitor what you are going to in terms of Web sites so they can target e-mail to you or spam, or pop-ups. I understand that everybody would like to be able to trace things. But it crosses over into privacy issues, too, and opens up where people are downloading things or are constantly spying on your computer, too.

But whose responsibility does this become? This goes to the next question: What is the most appropriate role for Congress here in dealing with this? Do we just assume that it is up to every computer owner to take care of their own problems? Or should we be

outlining some things on our level to say that there has to be certain rules to be followed nationwide?

Mr. Roback.

Mr. ROBACK. Well, from my perspective, the challenge is, of course, that the network is worldwide. So, it does not stop at the borders of this country. You are connecting all the time to Web sites around the world. Whatever rules we might put in place geographically here may well be completely ignored overseas. So there needs to be a really global understanding of what the role should be, on which I do not think you are ever going to attain perfection. I think you are then bound to have reliance on user responsibility that they have to do some due diligence to protect their assets.

Mr. MURPHY. Mr. Beales.

Mr. BEALES. Congressman Murphy, I think some of what we see out there—and it is clearly a role for us and at this point I do not know that it is a role for the Congress—but there are law enforcement problems in the way some bad software ends up on consumers' systems.

If there is deception in tricking people into downloading stuff that they do not know that they are getting, or if software takes over a person's computer and resets settings and then cannot be set back, and consumers do not know that they are getting into that kind of a mess when they download it, those things probably do violate our statute as unfair or deceptive practices. We are actively looking for cases against that kind of conduct.

Mr. MURPHY. I hope so. I think it is important for consumers to be able to join together and have those kinds of protections. I think it does get to be harmful. Certainly a small business costs a massive amount of money when all the computers slow down.

I see my time is almost up. Hopefully I will have some time for questions later.

Mr. Chairman, I yield back.

Mr. PUTNAM. Thank you very much, Mr. Murphy.

What would all of you describe as the single greatest cyber threat facing home users and small businesses today? We will begin with Mr. Yoran.

Mr. YORAN. The largest threat to home users and small businesses is the sheer complexity of effectively protecting one's computer systems, a small business, or a home user. Security is far too complex. I think some of the efforts which we have talked about here in terms of outreach and in terms of awareness, educating the consumer markets, and educating the small business markets, will help drive the market to producing higher quality products.

Much of the efforts underway are geared specifically to making cyber security an easier issue for the home users to deal with. Those efforts fall into a number of different categories, including delivering computer and computer systems and configurations which are better secured than they had been historically. They include the software vendors, delivering software which is capable of patching itself without a tremendous amount of intervention from the home user, and investment in the private sector to producing higher quality code within the security community of making their products easier to use to cover some of the flaws and vulnerabilities which are discovered in the products which are less security aware.

And ultimately, it is in the service providers delivering Internet connectivity in a fashion that is more secure out-of-the-box that defends against "phishing" scams, that defends against viruses and other network-based attacks. It is really a complex issue. When you look at action on the part of Congress or other folks to provide regulation for the software industry to encourage or force higher-quality code or practices. I think we need to very carefully evaluate the effectiveness of that approach versus the effectiveness of investment into the research and development of tools which will empower them, or enable them, to produce higher quality code.

I know, in fact, of no cases where software vendors or software developers are interested in producing code with flaws in it. So the more research we can conduct, the better the quality of the tools to foster higher quality software, the better off we are and the more likely that those tools will result in meaningful progress in the private sector.

Mr. PUTNAM. Mr. Beales.

Mr. BEALES. I think the biggest problem is the lack of attention on the part of both businesses and the home users—attention to the fact that there is a problem and attention to the fact that the nature of the problem is continuously changing. The threats that we face evolve because the tactics of those who would do bad are evolving in response to the last set of changes.

I think even when people try to take steps, too often they say, "I put in place this piece of software. I am done. I do not need to worry about security anymore." That is not true. People need to pay attention to new threats as they emerge, and particularly companies need to pay attention to new threats as they emerge, and try to address those over time.

Mr. PUTNAM. Ms. Mills.

Ms. MILLS. Thank you, Mr. Chairman. This goes to Congressman Murphy's question as well. No. 1, I think the very key is to raise the visibility. Second, it is the education and the impact on how to protect one's self. I know recently I, myself, was receiving undeliverable e-mail messages on my home computer from people I never sent a message to. I took it into a service tech. I thought I had a virus. He said, "No, your e-mail address was grabbed somewhere in cyber space and they are now sending messages to various individuals using your address.

So, I think the consumer, the small business, is definitely not aware of the capabilities that are out there right now in this whole world of viruses. I think raising that visibility, engaging the private sector to help in the education, just as my Association of Small Business Developmental Centers did with Microsoft. I think that is the No. 1 step we need to take.

Mr. PUTNAM. Mr. Roback.

Mr. ROBACK. In addition to all the insightful comments by my colleagues, I guess I would point out this. The current situation to me seems untenable of the degree of exploitation of known vulnerabilities we have now with commercial products. One of the Web-based resources we have at our site at NIST has over 6,600 vulnerabilities in commercial products. Of course, with these vulnerabilities come kiddy scripts and other things that exploit them and can be used to attack systems.

So we are chasing our own tail in terms of trying to stay up-to-date, in terms of installing patches and also trying to stay knowledgeable and taking advantage of what security features are in commercial products, in terms of having to turn on the right level of security, but not too much so you do not break everything.

What are some of the solutions? Well, I usually talk in terms of four steps of solutions. The first is the need for better specifications. I am not talking Government-mandated standards here, necessarily, but better commercial industry consensus-based sets of specifications, and better testing to know that those specifications are correctly implemented by products, that is: Are they implementing and using sound security technologies and techniques?

Third, is taking advantage of those techniques that are appropriate for your environments, so turning on and turning off the right security settings. Fourth, is trying to ensure through these scanning tools and so forth that those settings are maintained and not inadvertently or maliciously turned off.

It probably will not surprise you, since I come from a research institution, that all of these areas need research so that we can improve the ways to do that.

Mr. PUTNAM. Mr. Yoran, from a national security standpoint, how does the computer security of home users and small businesses impact the overall security profile of the Nation's information network?

Mr. YORAN. Chairman Putnam, in a number of recent incidents and events, we have seen cases where large numbers of home computers always-on, high bandwidth systems, have been used to attack components of the Nation's, and really the world's, cyber infrastructure. In many cases those efforts have been thwarted and in some cases they have been effective.

To the extent that home systems are on-line, are always on and are connected through high-speed access points, they can serve in the role of zombie or participate in large Botnet activities and really make the incidence response process a lot more complex and increase the likelihood that our Nation's cyber infrastructure or that other critical infrastructures may be adversely impacted in the near future.

Mr. PUTNAM. How have the partnerships and the initiatives that your Department have taken benefited home users and small businesses?

Mr. YORAN. Well, sir, they have benefited home users and small businesses in a number of ways. The efforts of the cyber alert system to help increase awareness of cyber events and help to increase the actionable items which home users and small businesses can take to protect their own computers has been well received. We have had over a quarter of a million subscribers to that cyber alert system in just the few months that it has been made available to the public.

But all of these efforts again are tactile and operational in nature and need to be pursued in conjunction with development programs for the technology industry and for the cyber security industry, to help assure that the next generation of products are more resilient and more immune to these types of attacks.

Mr. PUTNAM. As you know, yesterday an attack caused failures at Acami; are you aware of that, the world's biggest host. They handle 15 percent of the net's traffic. What was your office's role and response to that attack?

Mr. YORAN. Chairman Putnam, in many instances the Department of Homeland Security and the U.S. CERT play a lead role in helping organizations respond to cyber incidents and very importantly, help coordinate those organizations in their interaction with other private sector entities and with public support mechanisms, such as law enforcement and other Federal resources which may be brought to bear during the time of a crisis.

In instances like the attacks which we saw yesterday, the lead role, if you will, was played by the private sector in protecting their systems and developing and enhancing their protective measures to bring their systems back on line. The role of the U.S. CERT and the Department of Homeland Security in that particular case was more focused around understanding events as they were unfolding, and helping to share, as appropriate, information with other private sector and public sector entities to determine what effect those events may have on other critical infrastructures.

Mr. PUTNAM. This appears to have been a denial of service attack. Are we seeing an increase in those types of attacks?

Mr. YORAN. Sir, we are seeing a number of denial——

Mr. PUTNAM. We will take a recess due to the power failure.

[Recess.]

Mr. PUTNAM. The subcommittee will adjourn due to power failure.

[Whereupon, at 4:26 p.m., the subcommittee was adjourned, to reconvene at the call of the Chair.]

[The prepared statements of Philip Reitinger, Avadis Tevanian, Don Frischmann, Thomas M. Dailey, and Paul Kurtz, submitted for the record but not presented due to the power outage, follow:]

Statement of Philip Reitinger

Senior Security Strategist, Microsoft Corporation

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

Hearing on "Locking Your Cyber Front Door – The Challenges Facing Home Users and Small Businesses"

June 16, 2004

Chairman Putnam, Ranking Member Clay, and Members of the Subcommittee: My name is Philip Reitinger, and I am a Senior Security Strategist for Microsoft. Thank you for the opportunity to appear today. I would like to discuss the ways in which Microsoft is working with its customers and its partners to help make computing more secure for both small businesses and individual consumers. Before joining Microsoft, I was a Deputy Chief of the Computer Crime and Intellectual Property Section of the Criminal Division of the Department of Justice, the Executive Director of the Department of Defense Cyber Crime Center, and the Chair of the G8 Subgroup on High Tech Crime. For some time I have been concerned with criminal threats, and with the challenges posed in preventing, detecting, deterring, and responding to cyber crime.

At Microsoft, security is a top priority. There are fundamental challenges that we and the industry as a whole must address in order to enhance security for small businesses and individual consumers. First, software – regardless of vendor and development model – is highly complex and will always have vulnerabilities. Second, while we see increasing security awareness among our customers, some small businesses and many individuals do not understand the threat or how to defend against it. As a result, many do not enable firewalls, run anti-virus software, or regularly update their systems. Our response to these challenges is rigorous and extensive: We are working with our customers and partners to enhance software security and to make it easier to use security technology, to reach more small businesses and individuals, and, recognizing that security is a process and not a destination, to innovate and work with government to protect public safety.

I. Enhancing Security: A Top Priority

We launched our Trustworthy Computing initiative in January 2002. Within Microsoft, this initiative fuels technological innovation and yields security tools that help our customers enhance the security of their computers.

Many of our technological innovations were discussed in my colleague Scott Culp's testimony before this Subcommittee on June 2, 2004. In brief, we are building more secure software through the following four-part strategy:

- Streamlining updating processes and enhancing updating tools to make it easier for consumers and small businesses to install security updates;
- Pursuing "Engineering Excellence" to reduce vulnerabilities by using state-of-the-art engineering practices, standards, and processes throughout the entire software development cycle;
- Increasing isolation and resiliency so that systems are protected against entire vectors of attack even in the absence of necessary updates; and
- Improving authentication and access controls that govern who gets access to networks and computers, and how they establish access privileges.

We are producing new and useful tools for our small business and individual customers, giving them flexible but simple systems to obtain and install updates. We have introduced a feature called "Automatic Update" for our recent operating systems. This tool presents a user with options ranging from automatic downloads of updates and scheduled installation to declining all updates. Similarly, on Microsoft.com we provide Windows Update, a web-based service which can identify missing patches for the Windows operating system and install them automatically if the user elects to do so. Later this year we plan to introduce Microsoft Update, which will provide the same service, but will also include other major Microsoft software as well as Windows.

At the same time, we improved the updating process by:

- Standardizing the operation of our security updates and installation technologies;
- Releasing updates once a month on a consistent schedule, to enable small businesses to plan update installations systematically and efficiently; and
- Reducing the update size where possible to make obtaining updates less burdensome.

One of the significant steps in the Trustworthy Computing initiative will take place later this year with our release of Service Pack 2 for Windows XP ("XP SP2") which will include significant security upgrades – many of which are aimed directly at home and small-business customers. First, the Windows Firewall will be made easier to use, enhanced and turned on by default to help stop attacks even if a system is not updated. Second, XP SP2 will have a "Security Center" which will centralize security management and recommend guidance when action needs to be taken. Third, file attachment handling will be improved for email and instant messaging programs to help prevent the spread of attachment-based viruses. XP SP2 will also reduce the threat posed by malicious code on web sites by enhancing customers' ability to prevent this code from running on their PCs.

Finally, and especially for customers with dial-up connections to the Internet, we have made available the Windows Security Update CD which we ship on request to customers free of charge. This CD includes Microsoft critical updates released through October 2003 and information on how customers can help protect their PCs. This CD is available for Windows XP, Windows Me, Windows 2000, Windows 98, and Windows 98 Second Edition.

II. Reaching Customers

While we pursue our Trustworthy Computing initiative, we also continue to reach out to customers directly and through partnerships with our industry peers and government.

Last fall we launched our "Protect Your PC" campaign (www.microsoft.com/protect) through a broad print and online campaign to encourage customers to take three essential steps to safeguard their systems:

1. Use a properly configured Internet firewall;
2. Regularly install security updates in their computers; and
3. Run up-to-date anti-virus software.

We also reach our customers on cyber-security issues in other ways. For instance, we will soon complete a series of security summits that have reached a broad array of customers, including one summit that occurred here in Washington, D.C. on April 8, 2004. Further, we provide security web sites for small businesses (www.microsoft.com/smallbusiness/gtm/securityguidance/hub.mspx) and individuals (www.microsoft.com/security/home and http://security.msn.com). These web sites provide our customers with basic knowledge on how to maintain an appropriate level of security and to avoid common internet-based frauds, such as "phishing" scams.

We have many partnerships to increase security awareness among small businesses and individuals. We are a member of the National Cyber Security Alliance, a partnership between the federal government and industry members with the goal of educating Americans on the need for computer security. The Alliance's web site, www.staysafeonline.info, is a clearinghouse of security-related information designed to encourage small business and home users to protect their systems. In order to make this information even more accessible and understandable to consumers, we are partnering with the Alliance to produce an Internet security and safety booklet that will soon be made available to policymakers and others for distribution to citizens. In addition, we participate in the information technology industry's Information Sharing and Analysis Center, the IT-ISAC, which issues bulletins on significant cyber security events. We also work with US-CERT to share information. And we helped found the Global Infrastructure Alliance for Internet Safety, a collection of global ISPs with the goal of helping to educate and protect consumers against the threat of malicious code attacks as well as emerging Internet threats.

III. Security as an Ongoing Challenge: Innovating and Working with Government

Secure computing is a process and a journey, not a final destination that can be reached. Threat models change over time, and we must change and innovate with them. Just as burglars find ways to defeat home security systems, cyber-criminals find new ways to attack computer systems. As a result, our industry must innovate continually while working with our customers to improve the security of their systems. These are difficult challenges, and they will be with us as long as we have connected computers and criminal attackers.

The government has an important role as well. It must increase the security of its computer systems and provide law enforcement officials with the tools, resources, and training they need to deter and investigate criminal attacks. Our government's hard-

working officials – including those within the Departments of Justice, Homeland Security, and Defense, as well as state and local investigators – are often short-staffed, under-funded, under-trained, and lack state-of-the-art technology used by cyber criminals. Also, cyber attacks are an international problem requiring cross-jurisdictional cooperation – to that end, we urge the Senate to ratify the Council of Europe Cybercrime Convention to help streamline international criminal investigations.

Finally, we are constantly searching for new and better ways for industry and law enforcement to partner to protect public safety in this dynamic environment. One example is our Anti-Virus rewards program, which offers rewards for information leading to the arrest and conviction of cyber criminals in certain cases. This program recently encouraged individuals with information on the author of the Sasser worm to step forward, leading to an arrest of the alleged hacker. We also assist and support the National Cyber Forensics Training Alliance ("NCFTA"), a joint government-industry organization, on investigations, online fraud, and online safety. In fact, to help protect the public from computer crime, Microsoft has placed an analyst on site at NCFTA who performs trend analysis and evaluates and forwards complaints received from users of Microsoft software and services. Microsoft is also in the process of donating software to the NCFTA to support its on-going mission.

Conclusion

Through our Trustworthy Computing initiative, we continue to develop innovative technologies and tools that enhance the security of our software, and to communicate with our customers about the importance of updating and securing their systems. We are working with our partners in industry and government to help consumers and small businesses enjoy safe, efficient, and productive on-line experiences.

I thank you for the opportunity to address the committee, commend your work on this issue, and look forward to your questions.

Written Testimony of
Avadis "Avie" Tevanian, Jr. Ph.D.
on behalf of
Apple Computer, Inc.
before the
House Subcommittee on Technology, Information Policy,
Intergovernmental Relations and the Census
June 16, 2004

Chairman Putnam and members of the Subcommittee, I am very pleased to be here today on behalf of Apple to participate in this hearing titled "*Locking Your Cyber Front Door – The Challenges Facing Home Users and Small Businesses.*" I am Avie Tevanian, the Chief Software Technology Officer for Apple, responsible for setting company-wide software technology direction. I joined Apple in 1997 as the leader of the team of software engineers that designed and developed Apple's brand new operating system, Mac OS X. Mac OS X was first released to the public in 2001. Since its release, I am proud to say the migration of Mac users to Mac OS X has been viewed as one of the most successful operating system transitions in history. Mac OS X, with approximately 10 million active users and more than 10,000 native applications, is widely recognized as having been implemented with an effective, comprehensive approach to security for all users. Apple has an unwavering commitment to security based on our belief that effective, pro-active cyber security is essential to protect the economic health and welfare of our nation. I commend the Subcommittee for holding this series of hearings and appreciate the opportunity to contribute today.

Mr. Chairman, I can appreciate first hand the concerns of Congress in regard to the myriad of threats and challenges individuals face every day as they cope with attempting to manage computer security on their own. From computer companies and software developers, to government agencies, major corporations and small business owners, as well as to individual home users, we all must work together to thwart the growing threat of cyber attacks. Without a doubt, computer security begins with the design and development of secure hardware and software products from companies like Apple. However, it doesn't stop there. Security is everyone's responsibility. While all stakeholders are responsible in varying degrees for ensuring the security of their systems, home users and small business owners must remain vigilant by taking their own security seriously every day. Just as we are expected to lock our own front doors ourselves, we must also take basic steps to protect ourselves from unwarranted cyber intruders. An especially critical challenge for companies like Apple is making security tools as accessible, transparent and easy to use as locking your own front door.

Security Challenges and Threat

It seems that not a week goes by without news of another major software virus or computer worm having infected a host of computer systems. These attacks turn unknowing computer users into victims, sometimes with devastating effects. These victims are not only government agencies and major corporations running mission critical systems, but also include the many small businesses and home users with limited technology backgrounds.

Further, some very serious computer security attacks often come with much less public fanfare than a major virus outbreak, but the results are no less devastating – maybe even more so. For example, often we hear stories of a computer hacker that has commandeered another's computer stealthily, initiating further attacks remotely, stealing important data and/or even that computer victim's identity. Some of these victims never even knew they were being attacked until it was too late.

Why are small businesses and home users so vulnerable today? First, more and more small business owners and home users are accessing the Internet using always-on broadband connections. With these always-on high-speed connections, individuals are increasingly becoming prime targets from external cyber attacks. Second, the majority of individual computer users today are using one operating system, which makes it much easier for global cyber criminals to exploit. Third, just as common criminals tend to prey on the easiest targets, individual computer users are particularly at risk because they often lack the computer expertise, not to mention the information technology (IT) staff, necessary to monitor, assess and react to the constant bombardment of Internet threats. To make matters worse, these threats are constantly changing, morphing into new and increasingly sophisticated attacks, challenging even the most experienced IT professionals. Further compounding the problem, a number of security features available on many computer systems today were developed primarily for IT professionals working for large businesses. As a result, managing security effectively often remains beyond the ability of many average home users and small business owners.

It is important to keep in mind that just as is the case with physical security, information security is not always automatic. Individuals must remain security conscious and alert. At the same time however, we also believe that in order to make computer security more manageable for individual users, security software must be intuitive, easy to administer, and wherever possible, automatic. Otherwise, average computer users will either not know how to protect themselves appropriately or may implement security ineffectively. In the end, many inexperienced computer users often do too little to protect themselves, or worse – do nothing.

Apple's Approach to meeting the Security Challenge

Just as building a computer securely in the first place is a priority for Apple, ensuring that security is easy to manage and maintain by the end user is equally critical. Since implementing the first commercial graphical user interface with the introduction of the Macintosh in 1984, Apple has prided itself on its "ease-of-use" operating system and software targeted originally for home users, small businesses and educators. As a result, Apple's approach to security starts from the vantage point of the individual computer user. This overarching ease-of-use perspective still permeates the Apple culture today, and was the guiding force for me and my team of engineers as we set about to develop Mac OS X, including its built-in security features.

From the beginning, Apple implemented a security strategy approach that was central to designing Mac OS X. First, we developed an extremely robust security architectural plan. Then we applied that plan to securing the very core foundation of the operating system itself. Because security is built into the core, it remains integral to every part of the operating system. Further, understanding that security often would not be administered by a team of IT professionals but by average home users, we made it very easy to administer. This comprehensive approach to integrating security into every aspect of the operating system has also been given very positive

reviews from NSA's own security researchers. It is essential for operating system security to provide a solid, virtually impermeable security foundation for all computer systems, whether intended for use in family rooms across the country or for hosting mission critical government systems. With a secure core in place appropriate layers of additional security can be added.

Let me explain this approach in a little more technical detail. First, at its foundation, Mac OS X is open sourced, based on UNIX, which has had its core components subjected to peer review for decades. We have found this approach has led to potential security problems being identified early and fixed before any vulnerability was exploited. Second, security is integrated directly into all software layers starting with the core foundation, using state-of-the-art standards based technologies (e.g., SSH, SSL, Kerberos, CDSA, AES Encryption). I would like to emphasize this point. We have built security directly into our operating system as an integral component, not simply added it on after the fact. Third, we placed administrative access to all of our security features inside a number of very intuitive applications that the average user can quickly grasp.

Knowing that new vulnerabilities can arise at any time, we built-in a software update tool that automatically alerts users when security updates are ready for download and installation. This feature is critically important. Simply building a secure system and then releasing periodic patches is of limited value if installing, or even finding those patches is confusing, complicated or simply inconvenient. At Apple, we believe that our software update approach ensures consistent secure software configurations, tested by Apple engineers, are readily available to our users. For the home user and small business owner, this approach makes keeping up-to-date as simple as clicking your mouse and authenticating a download – not to mention fast and effective.

We believe that an individual's computer experience can and should be protected from the start. Therefore, we ship all of our hardware and software products such that they are secure right out of the box. By starting out with a computer in a secure state, individuals are better protected when they first connect to a network or venture off onto the Internet. Later, they may choose for themselves those features and functions they want to implement on-the-fly without having security compromised unknowingly.

Knowing that more and more home users have always-on broadband connections, which increases vulnerability, is a significant reason why we built-in the capability of creating multiple user accounts on every computer. This feature enables the owner of a computer to designate himself as an "administrator" of that machine. An administrator is allowed to change important security and system settings. The administrator can also create additional user accounts and limit the degree to which other users of that computer can change important settings. Even those individuals with administrator privileges are required to re-authenticate before important system updates and changes are made, providing additional protection. As a further precaution, the administrator is kept from directly accessing the core of the operating system by default. In addition, to protect an unattended computer from unwarranted and unauthorized access, we configure our entire system to sleep when not being used and then to rapidly wake-up when the owner returns. When the system is asleep it is not accessible from the network nor is it susceptible to Internet attacks. We believe our implementation of these sleep and wake features is very robust and fast, reducing the desire of the user to disable them.

These highlighted security features are by no means intended to be exhaustive. In fact, although not the direct focus of today's hearing, Apple also provides advanced tools and technologies that

allow system administrators to secure their enterprise desktops, servers and networks. As is our approach to every software application we build, all of these security features and system controls are very configurable, extremely flexible, and highly intuitive, whether they are used by IT professionals protecting a cluster of 1,000 or more computers on a university campus, or by a home user managing an iMac with basic technical skills.

Providing security tools alone is not enough. To make educating our users about security convenient, Apple has created a public web page for customers to learn about all of the various Mac OS X security technologies and features (http://www.apple.com/macosx/features/security/). We also provide additional security resources and useful common sense security tips right on their desktop under a number of convenient help menus. Even with security settings easily managed on a Mac, we believe it is important to continually remind all home computer users and small business owners of the types of common sense steps they should be taking as they routinely go about working, communicating and surfing online. A sample of some basic security tips would include the following:

- Choose a password that is difficult to guess and change it often,
- Make sure your system software and security applications are up-to-date,
- Create multiple user accounts on your computer and limit those who are authorized to change system preferences and security settings,
- Be wary of unusual email attachments – even from friends,
- Only download applications and files from legitimate sources, and
- Backup your files regularly

Although these steps listed above seem very obvious, continuing to remind users of their importance can go a long way toward lessening the impact of a spreading virus or a malicious cyber attack.

Mac OS X Security Record

As we are all so well aware, tens of thousands of viruses and worms have been unleashed on the Internet in recent years. These attacks are unrelenting, interrupting Internet access, crippling large company networks, and even bringing down government agencies. The global costs from these disruptions to businesses alone were estimated by Trend Micro to be $55 billion in 2003, up from $30 billion in 2002, and $13 billion in 2001. Not surprisingly, this steep upward trend is projected by Trend Micro to continue this year. Notwithstanding all of our collective efforts to mitigate this threat, it must be made clear that no company or its software can ever claim to be fully immune from viruses or guaranteed impenetrable from a cyber attack.

That said, since the debut of Mac OS X in 2001, and after three major updates, I am not aware of a single virus that has affected our operating system. Furthermore, we have been able to respond rapidly to any potential vulnerability in our operating system through 44 security updates delivered through our software update tool. Of those potential security problems, none were ever known to be exploited.

While Apple is very proud of our approach to security, we recognize the importance of being pro-active in anticipating new threats or security problems so that even potential risks are quickly mitigated and threats reduced. We all know that no security is 100% perfect. If managed improperly, or not at all, no amount of security can withstand a cyber attack. While we can provide secure systems and the tools to manage that security, we need to work with our

customers and partners, in government, industry and the consumer market to ensure preparedness and to ensure the use of best practices in protecting our information systems.

Beyond the Individual User – Employing Cyber-Diversity
Individuals within larger organizations often worry less about cyber security because they believe their internal IT/ Cyber Security departments will protect them. Although implementation of security updates can be administered at the network level, there is still an important role to be played by the individual user in understanding what security features should be enabled on their own desktop.

Moreover, I would urge the Committee to consider the significant vulnerability within many enterprises, including most government agencies, that results from having essentially a homogeneous operating environment. When security has been breached at the enterprise level, or a malicious virus has been unleashed inside an organization, it often propagates itself very rapidly because the organization is configured using one operating system and platform for many systems and applications. This homogenous configuration means that one worm could bring down an entire organization very rapidly, costing millions of dollars and hours, if not days, in productivity. While, with the strong leadership of this Subcommittee, most agencies have implemented redundant systems, disaster recovery plans and other forms of back up, if all the systems are the same, there is significant risk none will survive, even though they may be geographically isolated or have substantial external layers of security.

The Congress should approach this very real security vulnerability by encouraging agencies to achieve cyber-diversity. Organizations should consider adding a mix of interoperable computer systems to their networks such that when one system is attacked, another system will remain up and functioning within the organization on its network. Unfortunately, many organizations hold on to an obsolete belief that differing computer systems, such as Windows PCs and Macs cannot interoperate or are costly to administer when used together. Our implementation of Mac OS X has focused on open industry standards and formats. When possible, we provide direct compatibility with Windows-based PCs and servers. As a result, a Macintosh fits in quite easily with Windows and UNIX networks. We firmly believe that any perceived short term administrative efficiencies and/or cost savings identified by standardizing on one platform is more than offset by the security risk and productivity losses associated with having a thoroughly homogeneous environment that is vulnerable to attack.

Summary
Mr. Chairman, as I said at the beginning of my testimony, computer security is everyone's responsibility. For our part, Apple is committed not only to providing all users with a secure operating system, but also with the easy to use security tools they need to protect themselves, their businesses, and their families, while enjoying all the benefits from surfing online or connecting to others on a network. We remain committed to a computer security approach that is robust and effective, while at the same time easy to use and administer.

We appreciate the Subcommittee's interest in the computer security of small business owners and home users. We look forward to working with you on this very important issue. I'm prepared to answer any questions you may have at this time.

Testimony of Don Frischmann
Senior Vice President, Communications and Brand Management,
Symantec Corporation
Sponsor, National Cyber Security Alliance (NCSA)

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

"Locking Your Cyber Front Door - The Challenges Facing Home Users and Small Businesses."

June 16, 2004

Chairman Putnam, Vice Chairwoman Miller, Ranking Member Clay, members of the Subcommittee, thank you for inviting me to testify today on the important topic of cyber security for consumers and small business. My name is Don Frischmann, and I am the Senior Vice President for Communications and Brand Management at Symantec Corporation. I am also here representing Symantec as a sponsor of the National Cyber Security Alliance, a nonprofit organization whose mission is to educate home users, children, young adults and small business owners on the importance of cyber security best practices. I am honored to be here today, and I look forward to joining my distinguished colleagues from government and industry to discuss this important topic Today I would like to address some of the challenges that consumers and small businesses face, as well as offer some recommendations on how we can overcome these challenges.

Challenges:

We are at an important cyber security crossroads. On one hand American Internet usage has grown to more than 144 million active users according to Nielson ratings. Today, the Internet is being used to do everything from monitoring baby's sleeping to banking, to commanding the combination refrigerator/oven to start cooking dinner before we leave the office. As our society and economy becomes more dependent on Internet connectivity, unfortunately Internet threats are growing just as fast.

The threats we are seeing today are more sophisticated, more aggressive and are able to spread more rapidly than ever before. Equally important, the time from the discovery of a new vulnerability to the release of an exploit targeting that vulnerability is shrinking rapidly. I make the analogy of the vulnerability being an "unlocked door" of a home and the exploit being a break-in by someone who knows about the unlocked door. These two phenomena have made the Internet increasingly vulnerable to attack.

We are beginning to see the early stages of what are called flash threats, threats that are near instantaneous in their dissemination. These are threats in which human reaction time is probably not fast enough. A good example is the Slammer worm, which, at its

peak rate, infected 90 percent of the vulnerable systems around the world in just 15 minutesThis speed of propagation, combined with the reduction of the time to exploitation, raises serious issues about the approach our nation is taking to protect our networks. More information about these trends can be found in our semi-annual Internet Security Threat Report, available on the Symantec website. I would also like to submit a copy of the report for the record.

Some of the specific challenges that consumers and small businesses face include: eliminating viruses, blocking hackers, safeguarding personal information, fighting spam, increasing online productivity, recovering lost or damaged files and safely removing confidential data that small businesses no longer need.

Consumers are storing more valuable, private information on their computers – from personal financial information, digital photos and confidential data and documents brought home from the office for evening or weekend work. Additionally, they are using the Internet to conduct e-commerce on a regular basis. Consumers' increasing reliance on their computers and the Internet allows people to be more efficient and innovative. However, the reliance also makes protecting sensitive data and mitigating Internet threats important issues. Internet threats that affect consumers include viruses, worms, Trojan horses, blended threats, privacy invasions, hackers, spam, cyber predators and inappropriate Web content. Threats such as spam are a hot button among consumers as they not only pose an annoyance, but they also usher-in the possibility of individuals falling prey to online fraud through phishing emails, which are messages that appear to come from trusted sources, but are instead used to scam individuals into disclosing personal information, including credit card numbers, and social security numbers.

The recently enacted Can-Spam Act is a positive step in the fight to control unsolicited commercial email. In addition, we believe that stronger enforcement, greater international cooperation and the use of anti-spam technology should complement legislative action.

According to a March 2004 survey conducted by Symantec and Applied Research, one in three users between the ages of 18-64 has clicked on a spam link. In the case of senior citizens, only 23 percent of such have clicked on a spam link, but 47 percent of those senior citizens who responded did not employ a spam fighting solution. Children also fall prey to Internet threats, including spam. A June 2003 survey conducted by Symantec and Applied Research found that more than 80 percent of children surveyed who use email receive inappropriate spam on a daily basis.

Small Business Challenges

The challenge for many small businesses is that they lack the resources to employ a full-time IT manager. Computer related issues are often handled by the small business owner or the most technologically knowledgeable employee. Many times, the person responsible for computer issues does not have sufficient understanding of Internet security threats or knowledge of how to protect the small business against malicious code, hackers and privacy invasions.

Spam continues to be a hot issue among small businesses due to its annoyance and its negative impact on productivity. A December 2003 survey conducted by Symantec and InsightExpress found that 64 percent of small business owners who responded to the survey reported an increase in spam over the past six months, with 33 percent noting dramatic increases. Symantec's small business spam survey found that 42 percent of small business owners responding would consider abandoning email for business correspondence if the spam situation worsens.

Small businesses have been exposed and will continue to be exposed to Internet threats such as malicious code and unwanted intrusions. According to Access Markets International (AMI) Partners, Inc., small businesses do see the need to protect their critical assets. Thus, AMI expects that total spending on security solutions among small businesses is expected to grow 25 - 30 percent annually in developed countries worldwide (April 1, 2004).

Recommendations:

In light of these trends, the consumer and small business segment is a critical component for improving safe and secure computing and one that would benefit from continued awareness and education initiatives. The President's National Strategy to Secure Cyberspace acknowledges that awareness is a key component to ensuring our overall cyber security.

Everyone who relies on the Internet has an interest in promoting its security. Users, whether at home or at work, need to know the simple things that they can do to help block intrusions, cyber attacks, or other security threats. Security is an evolving process and we must continue to be aggressive, especially in educating the individual user about good cyber security practices. Implementing cyber security best practices enables users to be less reactive when a cyber attack occurs, and become more proactive in the protection of personal data and property, promoting the country's economic stability, and ultimately our national security. A recent study by the National Cyber Security Alliance confirms the need for this broad-based education. That study showed that nearly 67 percent of high speed Internet users do not use firewalls and more than 60 percent do not regularly update their anti-virus software to protect against new threats.

When it comes to Internet security, the first challenge with consumers and small business users is to get past the "it can't happen to me" mentality. The second challenge is to help them understand how these online threats can affect them and the simple steps they need to take to protect their computers and their value data. These steps include a combination of technology tools and best practice processes.

The National Cyber Security Alliance is developing a three-year national cyber security awareness campaign beginning this fall. This awareness campaign targeted at home users and small businesses, will use various vehicles to raise awareness of the cyber-security issue and provide actionable steps people can take to protect themselves. In conjunction with the "StaySafe Online" awareness efforts, the campaign will include dissemination of cyber security tips, which are already available through the NCSA's main website: www.staysafeonline.info. On this site, visitors can also find self-tests, tool-kits for each

audience, helpful links and more. One of the NCSA's top ten tips is to remind computer users to keep their anti-virus and other security software up-to-date by regularly downloading anti-virus definitions, intrusion signatures, and vulnerability patches.

As a provider of products and services to consumers, Symantec has found that home users also want easy-to-use integrated solutions to protect their computers against Internet threats. These bundled packages are easy to install, user-friendly, and protect against malicious code, hackers, privacy infringements, spam and inappropriate web content. We believe it is essential to make it easy for non-technical customers to use technology that will protect them and the systems they rely upon.

Small business owners, are beginning to realize the need to move beyond just anti-virus solutions to integrated security solutions that include intrusion detection, VPN, firewall, remote network security management and spam control. To address this need, security companies such as Symantec are offering appliances that provide affordable, high performance, all-in-one technology for small businesses. These appliances are easy to install and requires minimal maintenance.

Some small businesses have just a couple of computers, and their IT infrastructures more closely resemble a consumer profile than that of an enterprise. Regardless of size, though, small businesses need to protect the critical data from Internet threats. For small offices that employ ten or fewer people, an integrated security suite can protect small businesses from online threats by eliminating viruses, blocking hackers, safeguarding personal information, fighting spam, increasing online productivity, recovering lost or damaged files and thoroughly deleting confidential data that small businesses no longer need.

There are also many small businesses that have a more sophisticated IT infrastructure that includes desktops, network servers and remote computers. These businesses need multi-layered security at every tier, offering one easy-to-manage solution that includes firewall protection, intrusion detection and interacts seamlessly with anti-virus software to keep

systems safeguarded against viruses, worms, Trojan horses, blended threats, and other technology used for malicious activity.

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. Most users (though not all) know it is critical to have anti-virus software. Some users (but certainly not all) also understand the importance of personal firewalls. As I pointed out at the beginning of my remarks, we are at a cyber security crossroads, and we still have a long way to go to raise the level of cyber security awareness with the general public. But, I do believe that we are taking the initial steps and that we can succeed in better securing our infrastructure.

Thank you for the opportunity to speak to you today. I would be happy to take any questions.

Testimony of Thomas M. Dailey
Chair and President U.S. Internet Service Provider Association
General Counsel, Verizon Online

Before the Subcommittee on Technology, Information Policy, Intergovernmental Relations and the Census
June 16, 2004

Thank you Mr. Chairman and members of the Subcommittee for this opportunity to testify about the security challenges facing home and small businesses users on the Internet. The U.S. Internet Service Provider Association (US ISPA) is a leading Internet industry group, representing some of the nation's largest Internet service providers, portal companies and network providers (collectively "ISPs") on important policy issues with a focus on security related matters.[1] The US ISPA is pleased to present testimony before this Subcommittee.

Internet security for home users and businesses is an important and complex issue. While the tools to help protect computers and data from intrusion are commercially available from multiple sources, and public and private educational initiatives have made online materials readily available, educating users in the proper use of such tools and raising their level of cyber security awareness is a significant challenge. For varying reasons, many consumers have not been able to keep up with the technology or information necessary to protect themselves from Internet threats. Although ISPs can and do play an important and helpful role in the education process, ISPs do not make security software or hardware products, or control the end user's activities on the Internet, or the ability or desire of end users to learn and stay current about security issues. In the end, no single group or industry can dictate the behavioral change

[1] US ISPA's members include AOL, Bell South, EarthLink, eBay, MCI, Microsoft, SAVVIS, SBC, and Verizon.

necessary to significantly improve the security awareness of Internet users. Such change requires a joint public-private sector education effort targeted to enhancing the cyber security awareness of the Internet-using public.

A. Understanding the challenges that home and small business users face in protecting their computers that are connected to the Internet.

Home and small business users face a number of challenges in safeguarding their computers and personal information from hackers and scam-artists on the Internet. Here are a few of the more significant challenges from the ISP perspective: 1) recognizing the need for anti-virus and firewall software; 2) getting past the "barriers" to keeping software up-to-date; and 3) staying current on threats and how to spot, avoid and remedy them.

1) Recognizing the need for security. To stay safe online, the home or small business user must first understand that running anti-virus *and* firewall software is essential to securing any computer connected to the Internet, and that such software needs to be frequently used *and* updated. Security software solutions are widely available to consumers today. Many computers come with anti-virus software preloaded or available free for a trial period. Most major ISPs, including US ISPA's ISP member companies, offer security services as part of their portal services or as standalone services that customers can purchase, often at a discount. Firewall software and hardware are also widely available, and some companies offer free firewall software programs that work well for home and small business users. Small business users can purchase security services from their ISP or from third party consultants. Thus, the challenge is not in the availability of security solutions, it is in helping home and small business users to recognize the need for and to install, use and update security hardware and software.

2) The "barriers" to use of security software. Despite the availability and relative ease of use security software, not all users run or update their software on a regular basis. A lack of time may be one cause. Another may be discomfort with technology – in a mass-market environment the technical knowledge of end users varies widely. Regardless of the reason, consumers need help to get past whatever barrier is keeping them from recognizing and using the security tools available. Doing so may require education in the proper use of security software and messaging about the risks of leaving a computer open to security threats. Such efforts should include helping consumers to understand the cost of not taking security precautions to fully gauge the risks of inaction.

3) Staying current on threats and how to spot and avoid them. Even if an end user installs and regularly runs his or her security software, he or she is not free of risk from intrusions, hacks and privacy loss. Software is just a tool – understanding the threats, how to spot them and therefore how to avoid and remedy them, is critical. Equally important is staying current on threats, whether in the form of the latest worm or identity theft scam. Knowing where to look for help – and who is a trusted source of information – can be a challenge for many users. The tools are there, if consumers know where to look.

Government agencies like the Federal Trade Commission (FTC) and the Department of Homeland Security (DHS), and organizations like the U.S. Chamber of Commerce, the National Cyber Security Partnership (NCSP),[2] and the National Cyber Security Alliance (NCSA), are committed to the education effort and are providing key leadership in this area. The NCSA

[2] The National Cyber Security Partnership is a coalition of trade associations, including the U.S Chamber of Commerce, the Information Technology Association of America, TechNet and the Business Software Alliance. *See* http://www.cyberpartnership.org.

website, www.staysafeonline.info, is a good example of the benefits of public-private partnership to address the security issues confronting Internet users today. Another is the U.S. Computer Emergency Readiness Team (CERT) website, www.us-cert.gov, sponsored through a partnership between DHS and the public and private sectors. Industry, too, is working to provide education and self-help sites to assist consumers in finding information about current threats and ways to avoid them. Personalfirewallday.org and Getnetwise.org are two good examples.[3] The websites and resources US ISPA members make available to their customers (*see* Exhibit A to this testimony for a sampling of such sites) is a further example of the private sector's commitment to helping consumers to protect themselves from Internet threats.

With all the government and private resources available, however, the ultimate responsibility for maintaining security rests with the end user. A critical challenge facing consumers, industry and policy-makers alike, therefore, is educating millions of end users not only about the tools and strategies available in the market, but also about threats and threat-avoidance.

B. Some of the Internet threats facing home and small business users, including phishing, zombies, spyware, worms, spackers and denial of service attacks.

There is a multitude of threats facing all Internet users, including home and small business users. Many bear imposing or even slightly comical names, like "Slammer," "MyDoom," "Bagel," "phishing" and "distributed denial of service" (DDoS) attacks. The risks these threats bring to bear are real and fall into several categories. The first includes "worms,"

---

[3] *See* http://www.personalfirewallday.org; http://www.getnetwise.org. Personal Firewall Day is a website sponsored by security software firms Microsoft, McAfee, ICSA Labs, Sygate and TruSecure that provides general advice and encouragement to novice Internet users about anti-virus and firewall software and the importance of upgrades. Getnetwise is a public service website sponsored by a broad group of Internet companies and public interest organizations, including several US ISPA members.

Trojans" and viruses, which typically infect a user's computer and either affect its operation or serve as a tool to accomplish some other end, such as a DDoS attack or spam propagation. "Spackers" represent a new and problematic union between hackers and spammers. Spammers pay hackers for compromised computer ID's or to hack into systems to install "zombie" software for later use as an e-mail relay. Once the software is triggered, the compromised "zombie drone" computer sends volumes of e-mail or other messages to a pre-determined set of e-mail addresses or addresses taken from the host computer's address book.[4]

"Spyware" is another security issue that has attracted attention of late. Arriving at a widely accepted and correct definition for "spyware" has proven problematic for the industry and policy-makers alike. Defining the term too broadly runs the risk of ensnaring legitimate and even beneficial forms of software. The most intrusive forms of "spyware," however, are programs installed on a user's computer that monitor the user's keystrokes or Internet activity and can secretly collect personal information or enable a computer to be hijacked. Anti-spyware software is now available in both free and fee-based forms. It removes many unwanted programs, but some spyware can be difficult to find and uninstall, especially where it is bundled with other software.

---

[4] The Committee expressed specific interest in recent news reports that hackers could purchase computers infected with worms or viruses (10,000 infected computers for just $500.00 in one news story) and use those computers to launch DDoS attacks, to send spam (spacking referred to above) or engage in other unlawful activities. *See Phatbot arrest throws open trade in zombie PCs*, theregister.com, http://www.theregister.co.uk/2004/05/12/phatbot_zombie_trade.html (05/12/04). The particular instance described in the story is a form of "spacking." The fact that the Internet underground has attached a value to compromised or zombie machines is a sobering but not necessarily surprising development. With the millions of dollars spammers make through the distribution of unsolicited e-mail, it is little wonder that a market for zombie machines, which are difficult to trace and provide a degree of anonymity to the spammer, has evolved.

Identity theft is yet another category of threat facing home and small business users. Identity theft has been around in different forms for many years. For example, in the past credit card users worried that a credit card receipt left behind with a merchant might allow an unscrupulous person to copy the credit card number and use the credit card to run up charges. The Internet version of this type of fraud is known as "phishing".[5] The term phishing applies to hackers who imitate legitimate companies in e-mails or create fake websites designed to look like a legitimate website to entice users to share their passwords, credit card numbers and other personal information. The hacker then uses the information to steal the target's identity or to sell that identity to others.

Over the years, phishing attacks have grown from stealing dialup Internet accounts into more sinister criminal enterprises. Phishing attacks have risen sharply and now target users of online banking, payment services such as PayPal, and online e-commerce sites, among others, and the attacks represent a significant threat to the branding and reputation of the legitimate companies whose brands are spoofed. Many phishing sites operate either from off-shore locations or from hijacked servers with exposed vulnerabilities. The sophistication of phishing schemes is increasing and it has become more and more difficult to determine if phishing e-mails are real or not. Phishing scams threaten to erode customer confidence and decrease use of online systems and brands.

---

5 The word "phishing" refers to Internet scam artists who use e-mail lures to "fish" for passwords and financial data from the "sea" of Internet users. The term was coined in the mid-1990s by hackers who were stealing ISP accounts by scamming passwords from unsuspecting users. By 1996, hacked accounts were called "phish", and by 1997 phish were actually being traded between hackers as a form of currency where hackers would routinely trade 10 working "phish" for a piece of hacking software.

The variety of threats on the Internet underscores the reason home and small business users must remain vigilant in using and maintaining their anti-virus and firewall software. While desktop software solutions can effectively limit exposure to many forms of viruses and worms or even spyware that captures personal information, there is no substitute for consumer awareness of Internet scams and schemes and knowledge about the ways to spot and avoid them.

C. The tools and strategies available to home and small business users to help mitigate their exposure to malicious attacks and scams over the Internet

The key to mitigating risk from exposure to security threats on the Internet is a combination of the effective use of software and hardware tools, and an awareness of cyber threats and how to avoid them. Home and small business users have an array of tools available to them through the major ISPs, such as US ISPA's members. ISPs not only provide a host of security products directly to their customers or through third party relationships, they play an important role in the education effort by providing useful resources about a variety of online safety and security issues. But ISPs can only provide a part of the solution. Software and hardware manufacturers as well as government organizations, such as the FTC, CERT and DHS, and consumers themselves all have a critical role to play in the education and awareness effort.

The members of the US ISPA fully support online security and safety education. For example, AOL, Bell South, EarthLink, Microsoft, SBC and Verizon Online, and each provides its customers with access to extensive Internet security websites (and other online help areas) that include child protection, anti-spam, anti-spyware and firewall software and other security services. ISPs also provide advice on password use, threat alerts and links to security software and government informational resources and websites. Attached as Exhibit A to this testimony are sample screen shots from some of our member's security-oriented websites. As these

website screenshots show, ISPs take very seriously the role of educating their customers about Internet security and helping consumers to help themselves in this important area. USISPA members realize that Internet security is no longer an add-on feature, but must be part of the basic service offering. Taking advantage of these services is an important part of any home or small business user's cyber security strategy.

Software and hardware manufacturers also offer an array of tools commercially. Many such tools are bundled with portal client software or computers sold by major computer makers. As described above, this software includes anti-virus, firewall, anti-spyware and anti-spam applications that can effectively limit the functioning and distribution of viruses, worms, spyware and Trojans. Government agencies like the FTC, CERT and DHS, and public-private partnerships like the NCSA and the NCSP, also provide valuable information on threat alerts and cyber tips for limiting exposure to security risks. While no security solution provides absolute protection against Internet threats, the combination of security software tools and access to online resources should be a major part of any user's cyber security strategy.

D. **What responsibility do hardware and software vendors have to ensure that their products are secure "out of the box"?**

Hackers and others bent on exploiting the Internet and Internet users are constantly coming up with new threats and scams. Keeping up with the changing nature of the threats and ensuring that software and hardware is secure "out of the box" is undoubtedly a difficult task. Software vendors and hardware manufacturers have strong incentives to make their products secure and to find ways to simplify the automatic update process. It is also critical that users understand the importance of making sure they are using the appropriate security software and that their software is properly updated, and the consequences of not doing so. Thus, the

responsibilities of software and hardware manufacturers cannot be entirely separated from the responsibilities of users -- or from the overall need for better education.

E. Education is the key to improving the security of home and small business users

Educating the mass market of consumers and small businesses, who have widely differing levels of technical and Internet knowledge, is essential to reducing security risks on the Internet. But this education effort requires a concerted effort from all stakeholder groups, including the information and technology industry, government and the schools. Raising consumer awareness of technical issues, like anti-virus protection, password protection and firewall usage, takes time to work itself into the fabric of the average user's experience. For this reason, it is important to develop a multi-pronged education and awareness campaign that targets all segments of the Internet using public, including the schools, starting with K-12 programs.

Significant effort should be focused on educating our children in the safe and lawful use of the Internet. Our schools need to build Internet security and online safety into their curricula. Parents need to take time to learn about proper cyber security techniques to protect their computers and their children from Internet threats. Kids often learn technology faster than their parents, but without training and direction they are just as likely to engage in activity that could open a computer to attack or allow privacy to be compromised (file sharing is a quick and often painful way to learn that your anti-virus software is not up-to-date). Moreover, kids need to learn at an early age how to protect themselves from online predators and scam artists. We teach kids to be wary of strangers when walking home; we should do no less to teach kids how to avoid threats on the Internet.

The education effort does not end with our children, however. Consumer awareness must also be built through advertising, public-service messaging (as others have testified, a Smoky the Bear campaign for online security) and through other key touch points, like contact with software and hardware manufacturers and ISPs. While the messaging need not be identical, there should be continuity on the basic messaging points. The Top Ten Cyber Security Tips on the NCSA website[6] is a good place to start. Companies can take those portions of the Top 10 tips and reinforce the messaging through their own websites and programs. Many if not all US ISPA members are already doing so.

Awareness building is not just a private sector responsibility. The efforts of the FTC, CERT and DHS (and others) and their various public-private sector partnerships should be encouraged and supported. Policy-makers should also look to new and creative ways to generate interest in cyber security, such as through federal training grants and scholarships and national public service advertising campaigns targeted to enhancing security awareness.

Closing Remarks:

The timing of this Subcommittee's inquiry into information and Internet security is right. Now is the time to explore the issue of enhancing the education and awareness of Internet users. But the task ahead is large and complex. Consumers come with all levels of technical knowledge and commitment to protecting their security and privacy. To continue the advancements in security attained to date, a multi-pronged approach that encourages each element of the Internet community, including the public and private sectors, to participate separately and collectively, is necessary.

---

[6] *See* http://www.staysafeonline.info.

On the public sector side, government should continue the outstanding work it has begun to enhance consumer awareness. Public-private partnerships should be supported. On the private sector side, market-based solutions should continue to drive innovation among software and hardware manufacturers, ISPs and others in the online security industry. The impact of competition is already apparent. Software is smarter, easier to use and more powerful than ever before. Updates are now broadcast automatically to millions of anti-virus and operating system users. Security specialists and network companies provide a wide array of services to help protect home and small business users. These advancements in online security have taken place in a cooperative environment with government agencies, driven by concern for consumers and protection of the network. The incentives are in place for continued development; government mandates are not the answer.

Finally, home and business users must step up their efforts to educate and protect themselves, with the help of the public and private sectors. The key to home and small business user acceptance and use of Internet security tools is to identify more effective ways to alert the public to the security solutions that are available, to make them simple to use, and that the consequences of not maintaining adequate cyber security awareness can be severe. At the end of the day, even the most effective tools will be of limited utility unless end users are aware of and choose to use them.

The US ISPA and its member companies are working hard to protect consumers and to make their online experience as safe and satisfying as possible. The US ISPA thanks the Subcommittee for this opportunity to testify today.

Exhibit A to the Testimony of

Thomas M. Dailey
Chair and President U.S. Internet Service Providers Association
General Counsel, Verizon Online

Before the Subcommittee on Technology, Information Policy, Intergovernmental Relations and the Census
June 16, 2004

Sample Internet Security Websites of
U.S. Internet Service Provider Association Members

AOL, Inc.
EarthLink, Inc.
SBC Communications
Verizon Online

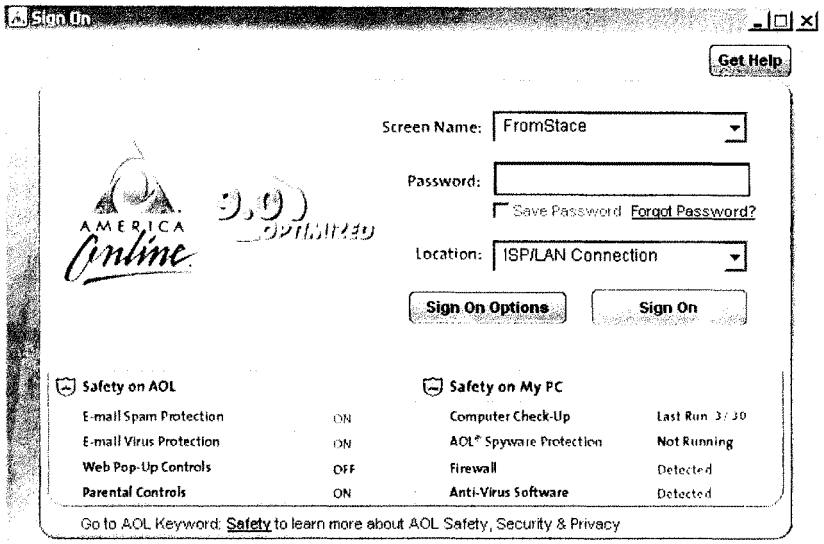
Sample Internet Security Websites of

AOL, Inc.

Security and AOL Features and Programming

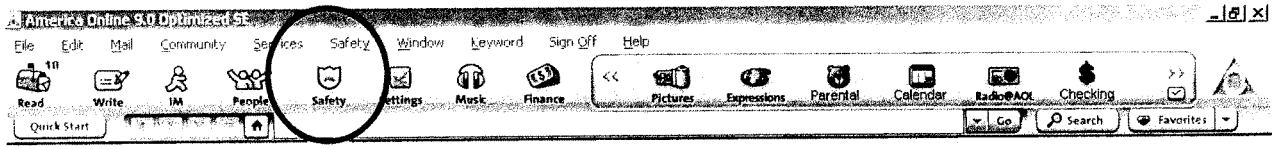
New Sign-on Screen

Provides Members with Relevant Information about their computers



Security Information is Highlighted

Providing a quick link to security information . . .



Security Information is Highlighted

Providing a quick link to security information . . .

AOL Safety, Security and Privacy

Safety, Security & Privacy

Helping you have a more safe and secure online experience.

Featuring VOLVO AOL's Safety Partner

Spam emails blocked today since sign-up jan 01

243,263,115

Safety on AOL:

E-mail Spam Protection	ON
E-mail Virus Protection	ON
Web Pop-Up Controls	ON
Parental Controls	ON

Safety on My PC:

Computer Check-Up	Last Run 3/30
AOL® Spyware Protection	Not Running
Firewall	Detected
Anti-Virus Software	Detected

Review AOL's Privacy Policy

What Are Your Kids Seeing Online?

AOL Guardian lets you receive regular e-mail updates on your child's online activities. Set it up now.

- AOL Parental Controls

Resources:

General Online Safety
Get tips for protecting your privacy, passwords and personal information.

Communication Safety
Stay more secure while using e-mail, IM and chat, and find out more about fighting spam.

Tip of the Week:

Did you know that AOL Bill Pay has special security features?

- **More Tips**
- **Suggest a Tip**

Virus Alert:

Get the latest information on new variants of the Mydoom, Netsky and Bagle worms.

McAfee VirusScan Online
Brought to you by AOL

Get Automated Updates Whenever You Sign On
With over 250 new computer viruses each month, protecting your PC is important!

Try It For Free!

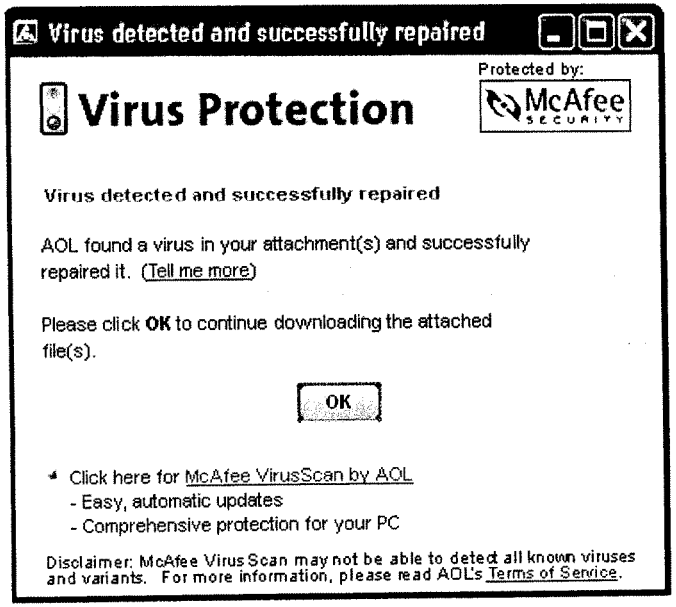
Coming Soon:

Help Protect Your Files!
AOL File Backup helps keep files safe if your PC crashes.

AOL Privacy Wall
Fight hackers with a firewall between the Web and your PC.

AOL Keyword: Safety & Security

Free Virus Scanning of E-mail Attachments. . .



Free Firewall for Broadband

Firewall

AOL Safety, Security & Privacy

Protecting Your PC With a Firewall

Connecting to the Internet without a firewall is like leaving the front door of your home unlocked when you leave.

What is a Firewall?
The first line of defense against harmful computer attacks, a firewall is a piece of software or hardware that provides a barrier between your computer and the Internet, making your PC invisible to hackers and helping prevent some viruses and worms from reaching your computer.

Do I Need a Firewall?
A firewall is essential with a high-speed connection because you are always connected to the Internet.

Coming Soon...
AOL PRIVACY WALL.
Powered by McAfee Security

The smart, effortless firewall that helps protect your files and information from unwanted intruders.

For More Information

- AOL Anti-Virus Center
- AOL Computer Check-Up
- AOL Safety, Security and Privacy
- AOL Computers + Electronics
- Firewall Information on AOL Help

Frequently Asked Questions
If you are a home network user, learn more about routers and firewalls.

AOL Keyword: Firewall

Advanced Parental Controls

AOL Parental Controls

AOL Parental Controls

Featuring VOLVO AOL's Safety Partner

Help

Create Your Child's Screen Name

Give each family member a separate screen name with its own level of online access.

Edit Parental Controls

Change the age category or edit existing controls for your child by clicking on your child's screen name below.

	Screen Name	Category	Requests	Master?
1.	StaceySmith1	General		Yes
2.	Soccerstryt	Young Teen		No
3.	KidzandTeens	General		No
4.	FromStace	Mature Teen		No
5.	MissStaceySmith	General		No
6.	StaceySmithWorks	General		No
7.	StaceyOHora	Kids Only	Web	No

Internet Access Controls

Internet Access Controls will help prevent your child from using external browsers to surf the Internet.

Internet Access Controls

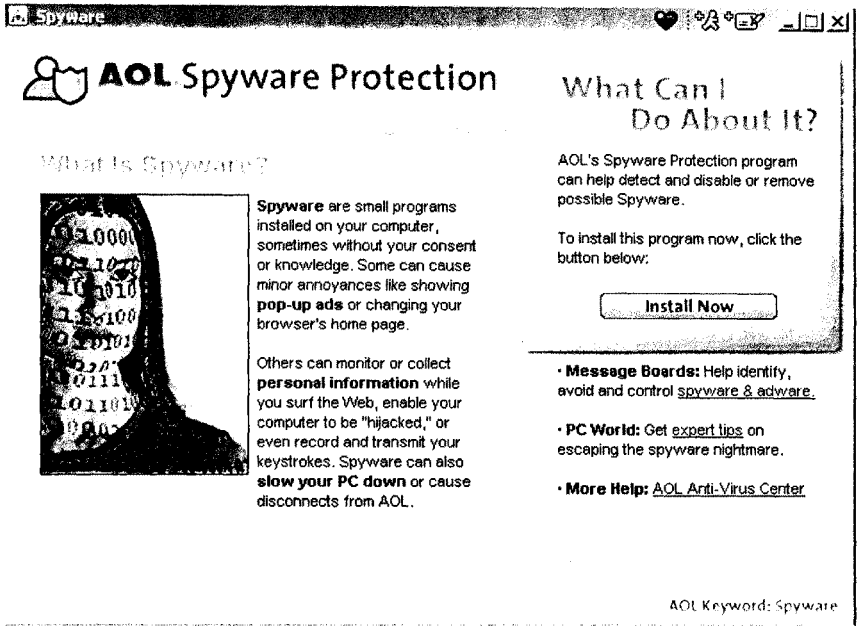
Tools to Give Your Child the Best Online Experience

Get in Control
Learn more about the Online Timer and AOL Guardian.

- Visit the CyberTipline and find out how to help protect kids online.
- Control who can sign onto your AOL account. Disable Guest Sign On.

AOL Keyword: Parental Controls

Removal and Protection Against Spyware

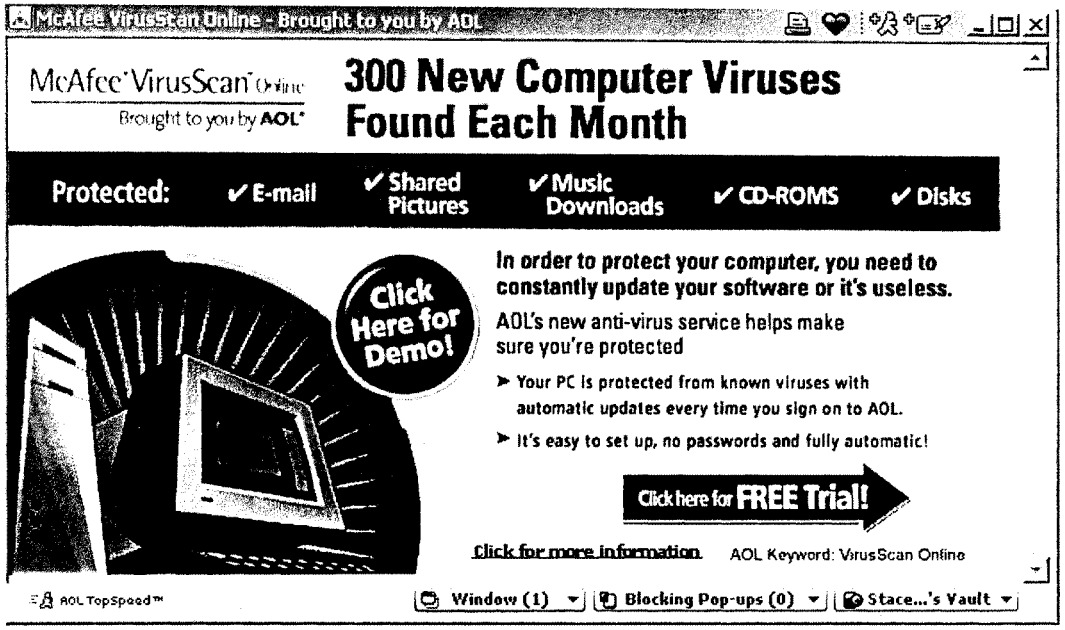


New Features of AOL Coming Soon. . .

- Safety and Security Center, which will bring all a computer's security settings to be set from one interface

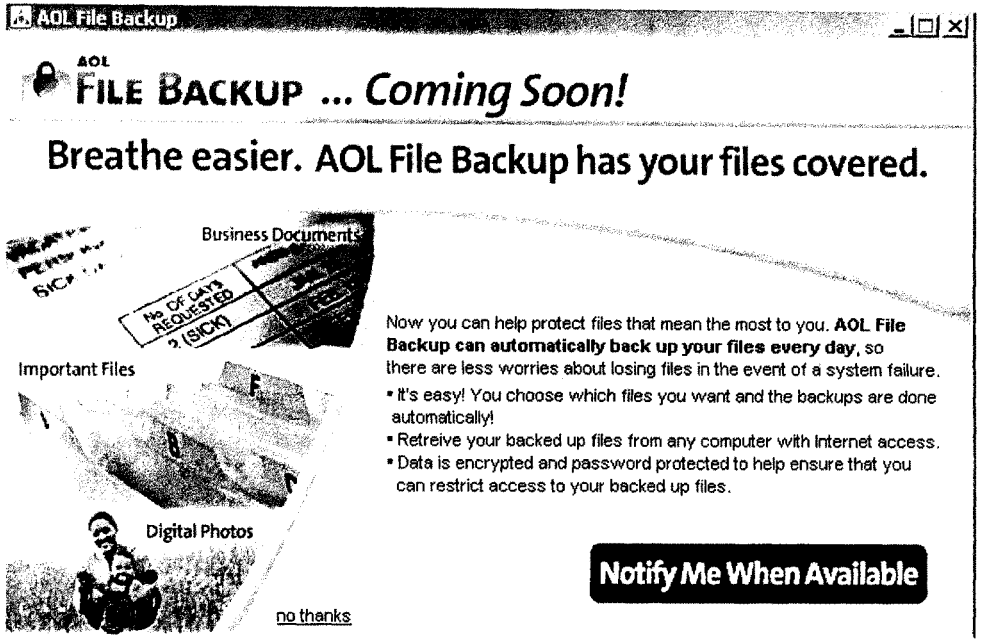
New Security Products

New security products that are easy to use. . .



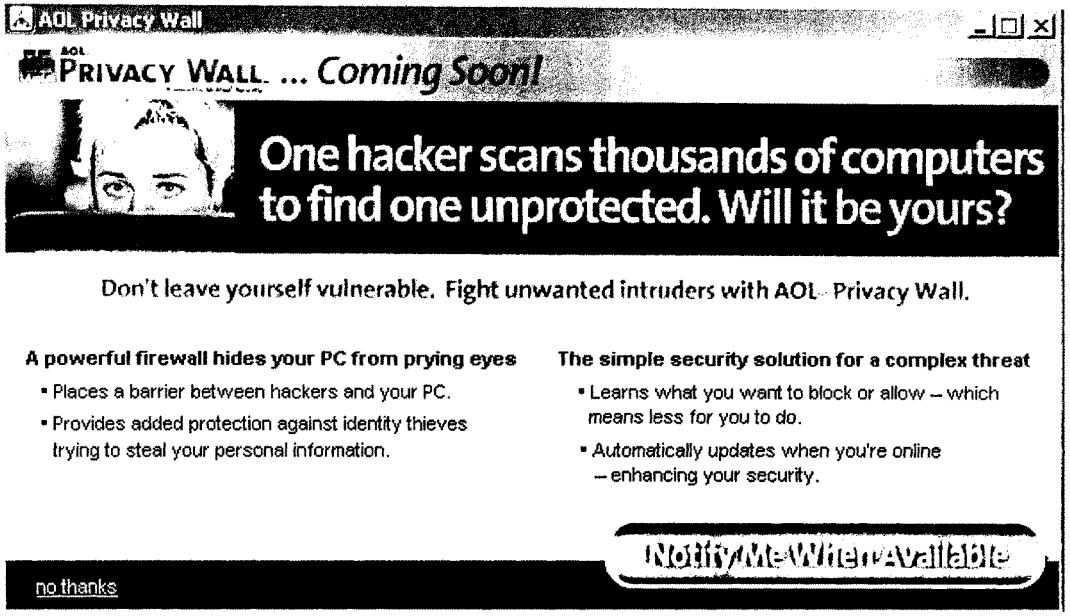
New Security Products

New security products that are coming soon. . .



New Security Products

New security products that are coming soon. . .



New Security Products

New security products that are coming soon. . .

- PassCode, SecurID support for AOL accounts
- NetKey, encryption and digital signature support within AOL using a USB token

Sample Internet Security Websites of

EarthLink, Inc.

EarthLink Protection Center - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Back Search Favorites Media

Address http://www.earthlink.net/protectioncenter/ Go

EarthLink.net | Start Page | Web Mail | Biz Center | My Account | Support

EarthLink revolves around you™

EarthLink powered by Google™

HOME | SWITCH | STORE | EARTHLINK TOOLS | MEMBER CENTER

DIAL-UP | HIGH SPEED | WIRELESS | BUSINESS | EXTRAS

Protect your computer, yourself, and your family. It's simple with EarthLink. You can count on our [illegible] for protection against dangerous email viruses, hidden spyware, Web site tracking, and other privacy and security threats. And for complete PC protection, we also offer powerful tools from Symantec™, the world leader in Internet security technology.

Free Scans for Your PC

[illegible]

Test your computer's exposure to viruses, hackers, and other Internet security threats.

(Note: If you use EarthLink's Pop-Up Blocker℠, please be sure your Pop-Up Blocker preferences are set to Normal Blocking or Off before beginning the Symantec Security Check.)

[illegible]

Detect spyware, Trojan horses, system monitors, and hoaxes on your PC.

Norton™ Security Products, Brought to You by EarthLink

Only EarthLink can offer you award-winning Norton security products on a monthly subscription basis—so your protection is always up to date, and you save money, too!

[illegible]

Enjoy complete, 24/7 PC protection against all virus threats with Symantec's state-of-the-art software. Your monthly subscription includes regular updates to keep you protected against new threats. $3.95 per month.

[illegible]

Prevent hacker intrusions and keep prying eyes out of your PC with this advanced personal firewall. It automatically hides your PC online and blocks suspicious connections. $3.95 per month.

[illegible]

Save more than 20% per year when you choose this complete protection package for your PC. $5.95 per month.

Done | Internet

EarthLink Spy Audit - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Back Search Favorites Media

Address http://www.earthlink.net/spyaudit/ Go

EarthLink.net | Start Page | Web Mail | Biz Center | My Account | Support

EarthLink revolves around you™

EarthLink powered by Google™

HOME SWITCH STORE EARTHLINK TOOLS MEMBER CENTER

EARTHLINK SPY AUDIT

Do you have spyware on your machine?
Find out now—FREE!

When you browse the Web, spyware programs can sneak onto your computer. As a result, Web sites can track your browsing habits, corrupt your data, or even steal your identity.

To scan your PC for spyware, just run a quick EarthLink Spy Audit.* This **free** service examines your computer and lists spyware results in minutes. It will not change or harm your system in any way.

Learn More

How to scan your computer for spyware

1. Click the **Start EarthLink Spy Audit** button. The **Download Dialog** box will open.
2. Click **Run** or **Open**. The program is a 200K download and will only take a few minutes to run. (If you'd rather save the program to use later, click **Save**.)

START EARTHLINK SPY AUDIT

* EarthLink Spy Audit powered by Webroot is available for Windows 98, 98SE, Me, 2000, and XP (Home and Pro). Spy Audit requires Internet Explorer 5.0 or higher.

Done Internet

EarthLink Spyware Blocker - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Back Search Favorites Media

Address http://www.earthlink.net/home/software/spywareblocker/ Go

EarthLink.net | Start Page | Web Mail | Biz Center | My Account | Support

EarthLink revolves around you™

EarthLink powered by Google™

HOME SWITCH STORE EARTHLINK TOOLS MEMBER CENTER

When you visit Web sites or open your email, spyware programs can infiltrate your computer and track your online activities. These suspicious programs can corrupt your hard drive or even allow strangers to access your PC.

How do I know if I have spyware?
Find out by running a fast, free . You'll get a detailed report in minutes!

FREE SPYWARE SCAN

SPYWARE BLOCKER

Not an EarthLink member?

EarthLink Spyware Blocker disables all common forms of spyware in a flash, including adware, system monitors, keyloggers, and Trojan horses. This powerful tool is **free** for all EarthLink members as part of , our Internet access software.

HOW TO DISABLE SPYWARE

1. Install the latest version of EarthLink TotalAccess 2004. If you're already using TotalAccess*, just run the **Update Manager**.

Internet

EarthLink Parental Controls - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Back Search Favorites Media

Address http://www.earthlink.net/home/software/parentalcontrols/ Go

EarthLink.net | Start Page | Web Mail | Biz Center | My Account | Support

EarthLink revolves around you™

EarthLink powered by Google™

HOME SWITCH STORE EARTHLINK TOOLS

EarthLink Parental Controls

Protect Your Children

Parents, relax! With EarthLink, everything's under control.

Now your 10-year-old can play games independently on the Web, your 8-year-old can email Grandma, and your teenager can chat online with friends—**all** protected by EarthLink's flexible suite of parental controls. Now the Net's as safe as it is fun and educational.

EarthLink Parental Controls are included with your **free** EarthLink **TotalAccess® 2004** software. And it's easy to adjust each child's profile on your **My Account** Web page.

EarthLink Parental Controls let you choose how often, when, where, and even with whom your kids play on the Net. But there's more! A suite of kid-friendly programs—email software, Web surfing, instant messaging, online games—enhances EarthLink Parental Controls for even the youngest children.

EARTHLINK PARENTAL CONTROLS OFFER:

- ***Customizable Parental Features***
  It's easy for you to control what your kids can and can't do, to block access to attachments, or even graduate your children to grownup software or email programs while still keeping them safe.
- ***Kid Patrol Browser***
  Clear child-friendly navigation and colorful special effects let kids go anywhere online,
- ***Kid-Friendly Email***
  Your child can send email to friends and family using a program that's fun, simple, and especially for kids.
- ***Set Online Time Limits***
  How much and when do you want your children to use the Net? As much as they

Done Internet

EarthLink Virus Blocker - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Back Search Favorites Media

Address http://www.earthlink.net/home/benefits/virusblocker/ Go

EarthLink.net | Start Page | Web Mail | Biz Center | My Account | Support

EarthLink revolves around you

EarthLink powered by Google

HOME SWITCH STORE EARTHLINK TOOLS

EARTHLINK VIRUS BLOCKER

powered by symantec.

Email is the most common way that computer viruses, Trojan horses, worms, and other malicious software can infect your PC.

That's why EarthLink members should be sure to activate our free **EarthLink Virus Blocker** email scanning system. Using technology from Symantec™ Corporation, Virus Blocker automatically scans all your incoming email messages for viruses, and removes them before they can cause any trouble.

Virus Blocker will:

- Scan every incoming message
- Clean your messages or attachments to remove any viruses, when possible
- Quarantine your message online if it can't be cleaned*
- Delete the entire message (if it's nothing but a virus)
- Work with both Windows and Mac**

It just takes a minute to activate Virus Blocker. After that, we'll keep our scanning system updated and running on our servers. There's nothing else you need to do!

To protect your entire computer and ensure your personal privacy, learn more about [illegible] or [illegible].

How to Activate Virus Blocker

You can activate Virus Blocker using either **My Account** or **EarthLink Web Mail**.

1. Visit [illegible], our online account management tool.
2. Sign in using your EarthLink email address and password.
3. Click on your email profile
4. Under the **Virus Blocker** section, click **Enable**.

EarthLink Web Mail:

1. Visit [illegible].
2. Sign in using your EarthLink email address and password.
3. Click on **Preferences** at the bottom left of the page
4. Under **Mail Handling Preferences**, click **Virus Blocker**.
4. Click the **Turn On Virus**

Done Internet

EarthLink Privacy Tools - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Back Search Favorites Media

Address http://www.earthlink.net/home/software/privacytools/ Go

EarthLink.net | Start Page | Web Mail | Biz Center | My Account | Support

EarthLink revolves around you™ EarthLink powered by Google™

HOME SWITCH STORE EARTHLINK TOOLS CUSTOMER CENTER

EarthLink Privacy Tools

EarthLink TotalAccess® 2004 software includes free tools to help guard your privacy while you're online. When you surf the Net, you may not know that some Web sites are keeping track of where you click and storing information on your hard drive while you browse. The purpose for this can be anything from decreasing download time the next time you access the site to marketing specifically to you based on your interests and online shopping habits.

With EarthLink Privacy Tools, you can choose to keep personal information (like your credit card number, home address, and which Web sites you've visited recently) private. Best of all, you can customize these tools to provide as much or as little privacy protection as you'd like.

How to activate EarthLink Privacy Tools: EarthLink Privacy Tools are available for our subscribers only. If you're already using TotalAccess 2004, you can activate these Privacy Tools right away. From the TotalAccess Task Panel, click the **Protection button**, select **Privacy Tools**, and then click **Options**

If you're using an earlier version of TotalAccess, there's no need to reinstall the software. Just use the TotalAccess function to get the latest version with new features like EarthLink Privacy Tools.

PRIVACY TOOL (as it appears in your Options menu)	WHAT DOES THIS TOOL DO
• Delete tracking data from my **Favorites** list	• Erases any extra tracking information a Web site tries to store on your hard drive when you add it to your **Favorites** list. (Your Favorites themselves will not be deleted.)

Done Internet

Sample Internet Security Websites of

SBC Communications

Security Overview Section

Back to My Services

Security Overview

Trust us: you do need security.

Be safe. Always.
People are constantly thinking of new ways to disrupt your computing and gain access to your files and valuable information. This is why ever more than ever, online security is an issue that you need to be addressing.

SECURITY
Overview
Email AntiVirus
Desktop AntiVirus (choice service)
SpamGuard

For example, you must protect yourself against viruses that come to you through email attachments or other methods - destroying your data your computer. You must safeguard yourself from inappropriate content th your email box, as well as block pop-up ads that are offensive and annoyi must stop spyware that you're unsuspectingly downloaded to your compu companies who try to follow your online activity and learn your passwords.

Turn your security on
Fortunately, as an SBC Yahoo! Internet customer, you already have protec these and other online intruders. In fact, you'll find that we've gone to great an environment that's safe and secure. Best of all, most of this protection i no extra charge to SBC Yahoo! subscribers. Simply turn the tools on, set specific needs, and relax.

Get informed. Now.
The first step to being safe is being informed. To get you started, we've me you. Simply read our 10 essential security tips for protecting your persona online. You'll find it at the Yahoo! Security Center, where you can pick up timely security information — including how to pick a secure password.

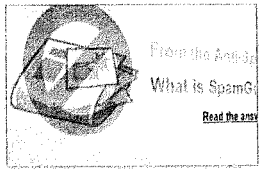
Iron clad security
With your SBC Yahoo! Internet Access you get Parental Controls for watc children, and Firewall Software that watches over your personal data. We the most popular anti-spyware software to help keep people from keeping t you're doing online.

And to make your online experience more enjoyable, we've also built in En

Back to My Services

Using Your SpamGuard

Put spam in its place: your Bulk Folder



SpamGuard help pages Get Started

SpamGuard
Spam is growing concern among Internet users. This is unsolicited junk email from companies pitching everything from get-rich-quick schemes to inappropriate content. With SBC Yahoo! Internet Access, you no longer have to open and sort through long lists of messages from unwanted companies or individuals. We bring you SpamGuard: an advanced line of defense against annoying spammers.

SECURITY
Overview
E-mail AntiVirus
Desktop AntiVirus (choice service)
SpamGuard
Pop-Up Blocker
Parental Controls
Firewall Software
Anti-Spyware

It's already turned on
For your convenience, we have defaulted your account with SpamGuard activated. It automatically detects mail sent in bulk and re-directs it to your Bulk Mail Folder. You can even adjust the filters to redirect messages with certain words or from specific senders into your Bulk Mail Folder. At any time you can open your Bulk Mail Folder and quickly scan for e-mails you do want to see — and delete ones you don't. Or, ignore them all, and we'll delete them after 30 days to save your storage space.

You can turn SpamGuard on and off by simply clicking a button in the settings of your web based email (http://mail.yahoo.com). See the instructions below.

If you're using a pop mail client (e.g. Microsoft Outlook Express), email caught by

Security Help Page

SBC Yahoo! Help - - Microsoft Internet Explorer provided by SBC Services

File Edit View Favorites Tools Help

Back Search Favorites Media

Address C:\Documents and Settings\ms8751\Local Settings\Temporary Internet Files\OLKC\SBC Yahoo! Help -.html

Google Search Web 569 blocked AutoFill Options

SBC YAHOO! DSL HELP

SBC Yahoo! | My Account | Help Home

Current Settings

DSL | sbcglobal.net

Change these settings

Top Security Issues

- Does firewall software come with SBC Yahoo! DSL?
- How does SBC Yahoo! Parental Controls work?
- Why am I getting a blocked page message?
- What can I do to make sure others can't access my account?
- How do I scan files attached to emails I have received with SBC Yahoo! Mail (Web-based)?

Search Advanced Search

Contact Us

Email Us
Get help in 24 hours.

Online Chat
Contact an agent 24x7.

Call Us
Get help over the phone.

Help Home > **Security**

There are 134 articles in:
"All Topics + All Applications + All Operating Systems"

Refine your results

By Security Topic	By Application	By Operating System
All Topics (134)	**All Applications (134)**	**All OS (134)**
Parental Controls (84)	Internet Explorer (3)	Macintosh (all) (1)
Protecting Your Information (35)	SBC Yahoo! Mail (4)	Macintosh OS X (all) (1)
Viruses (25)	SBC Yahoo! Browser (1)	Windows (all) (5)
Spyware (4)	SBC Yahoo! Messenger (1)	

Displaying 1 - 10 of 134 | Next

Show Summaries

How do I install SBC Yahoo! Parental Controls?

Why can't I share files or printers over the Internet? (TCP ports 135, 139, 445 and 1025 are blocked)

I forgot my Parental Controls Override password. Can I get a new one?

Bundled Security Solution

How do I uninstall SBC Yahoo! Parental Controls?

Does firewall software come with SBC Yahoo! DSL?

Sasser (LSASS Error) and Gaebot (Agobot) Worm Removal

Critical Security Update for Macintosh OS X Help Viewer

Internet

Sample Internet Security Websites of

Verizon Online

veri on Search Go Verizc

Welcome to Verizon Online

Home
Verizon Central
E-Mail & More
Help & Support
My Account
My Web Space
Music, Games & Video
Latest Internet Products
Resource Center
- Control Pad
- Perks
- Announcements
- Instant Messaging
- DSL Support Center
- Verizon Wi-Fi
- Contact Us
- DSL Guide
- Switching Tips
- Online White Pages
- Online Yellow Pages
- System Status
- Dial-up Access Numbers
- Policies Section
- Moving Help
- Internet Security Center
- Safeguard Your Computer
- Child Safety Software

More From Verizon

Resource Center

Internet Security Center

Protect, Detect, Connect - Three simple rules for online safety.

Internet & E-mail Threat Alerts!
- Beagle Virus
- Phishing Scam
- More...

Your Internet security is very important to Verizon Online. And we also know that trying to keep up with all the technology and options for staying safe online is sometimes hard to do.

To keep you up to date on the latest software and security information, Verizon Online has created this Internet Security Center website to combine security tools and information in one place - so staying safe online is easier.

Bookmark this site today! We will continually update this site with enhancements to this site you won't want to miss!

Many of the services listed below are available, at no additional cost, to Verizon Online DSL MSN Premium members. If you don't already have Ve DSL with MSN Premium, sign-up at www.verizon.net/betterway today!

Protect

Safeguard your Passwords
Guard your passwords like you would your social security number.
Tips:

- Choose a password that others cannot guess but that you can remember.
- Use a combination of letters and numbers instead of personal information such as birthday or your name.
- Don't share your password with anyone you don't feel comfortable with.
- Don't use the same password for more than one service.

To learn more: Visit GetNetWise
To take action: Visit Online Help & Support for Passwords

Guard Your E-mail
Treat your e-mail address like you do your password. It is personal information that should not be shared carelessly.
Tips:

- Enable a Spam and domain filter.
- Choose an uncommon e-mail address so it cannot be easily guessed.
- Don't publicize your name or e-mail address on the Internet.
- Never reply to Spam or unsubscribe from Spam. That only informs the sender the address is valid.
- Look for and read the privacy statements of any company or website you use.
- Use separate e-mail addresses for public and private communications.

To learn more: Visit GetNetWise.
To take action: Visit Online Help & Support for E-mail.

Use Parental Controls
Parental Control software allows you to shield your children from objectionable material on websites, newsgroups, or chat rooms. The software control the type of information your child can reveal and access. Access can be controlled based on:

- PICS ratings (an independent rating system)
- web address (URL)
- user review's of websites
- keywords based on the context in which keywords appear
- age group.

To learn more: Visit GetNetWise Kids
To take action: If you have MSN Premium, click the safety icon on your Verizon Online DSL with MSN toolbar, select Parental Controls. Verizon offers CyberSitter as an alternative to managing Parental Controls.

Enable Spam Filtering and Blocking
Spam filtering helps you manage junk e-mail by placing suspect messages in a separate folder and deleting them. Spam blocking lets you block addresses and e-mail domains to help keep unwanted e-mail out.

- Pick an address that is hard for Spammers to guess and easy for you to remember.
- Consider creating separate addresses or accounts that can be used for online purchases, chat rooms and other public postings.

To learn more: Visit GetNetWise About Spam

Secure Home Networking
Verizon Online's Home Networking Verizon Online home networking solutions come equipped to support secure communication between all co home. In addition to protecting your computers and data, network security prevents unauthorized access to your Internet connection.

To learn more and take action: GetNetWise WiFi Security and Home Networking FAQs
To sign up: Visit Verizon Online Home Networking.

Backup Important Files and Information
Backing up your data is a good idea regardless of Internet security issues. However, the increasing threat of security breaches makes data back for any Internet user who values the files and photos and other information on their PC. Verizon Online offers a service called My Storage Place the process of backing up your important files.

To learn more and to take action: Visit My Storage Place

Use Caution when Downloading Files
To help reduce the risk of inadvertently downloading a harmful virus, use caution when downloading files from the Internet. File sharing program often used to share music and video files (peer-2-peer programs), may be a source of viruses and other harmful programs that can damage you system or cause your computer to distribute viruses and spam. We urge you to only download from legitimate sites where you know the source is legal, reliable, and safe. And remember, downloading copyrighted music, videos and other software without permission from the copyright ow many popular peer-to-peer sites), can be illegal and expose you to serious civil and criminal liability.

Be careful when you download (or let others download using your computer). There are a wide variety of safe, lawful sites available online, and Online's DSL Live site. Sites like Rhapsody for music and Wild Tangent for games.

Detect

Install Anti-Virus Software
The most important thing you can do to help keep your computer and important data safe from viruses is to install use and update an anti-virus program on your computer. The Internet is constantly monitored for new viruses, and many anti-virus programs can automatically keep your cor date the latest detection software and virus definitions.

To help, Verizon Online DSL with MSN Premium Software offers advanced Anti-virus software.

To learn more: Visit GetNetWise Use Anti Virus Software
To take action: Download MSN Premium to take advantage of its anti-virus protections. If you already have MSN Premium, click the safety icon Verizon Online DSL with MSN toolbar, and select Virus Guard.

Install a Firewall
Another key way to stay safer online is to establish a security border between your computer and the Internet, blocking Internet hackers from ac computer and personal information while you are online.

To learn more: Visit GetNetWise Firewalls
To take action: If you have MSN Premium, click the safety icon on your Verizon Online DSL with MSN toolbar, and select Firewall. Verizon Onlir the ZoneAlarm Pro firewall free for 90 days

Detect Spyware
Spyware, a catch all term for software that tracks what you do online, is used by some Internet companies to gather your personal data without knowledge. Install a Personal Firewall which will detect Spyware and keep your personal data safe. Both the MSN Premium and ZoneAlarm Pro solutions include Spyware protection.

To learn more: Visit GetNetWise Spotlight on Spyware
To take action: If you have MSN Premium, click the safety icon on your Verizon Online DSL with MSN toolbar, and select Firewall. Or download ZoneAlarm Pro firewall free for 90 days.

Use Pop Up Blocker
Detect and block pop-up ads before they launch. Blocking pop ups not only saves you time it can also help thwart security issues by removing tl "mis-click" to load or launch an unwanted program or setting change. Verizon Online DSL with MSN Premium Software include a Pop-up Blocke

To learn more: Visit Popup blocking with MSN Pop-up Guard
To take action: If you already have MSN Premium, click the safety icon on your Verizon Online DSL with MSN toolbar, and select Pop-up Guard

Connect

Staying connected to accurate, relevant information available on the web is time consuming-but not for Verizon Online customers. We've done t you. Below are the sites we recommend you visit regularly. We'll continually monitor the Internet for new sites and provide only those sites we d relevant and accurate.

GetNetWise
http://www.getnetwise.org
This is a great resource site that provides tips, tools and advice on keeping children safe online, stopping unwanted e-mail and Spam and prote computer and your personal information.

Microsoft Security
http://www.microsoft.com/security/
Microsoft's site provides in depth information covering a wide range of security topics including security bulletins and virus alerts as well and link specific product updates and tools.

Stay Safe Online
http://www.staysafeonline.info
Take a self-guided cyber security test that will score how well your doing to protect yourself. This website also provides educational information how to safeguard your system.

MSN Kids
http://kids.msn.com/
Send your children to a kid-friendly site they'll love with no worry about objectionable content. MSN Kids includes games to play and activities to coloring, music, and reading. There are also things to learn, like news, animal facts, and weird stuff that can't even be categorized!

The National Center for Missing and Exploited Children
http://www.missingkids.com/
Access the latest laws and information, report a harmful content you find online, and view tips for keeping your kids safe online and in their daily

veri on Search Go Verizc

Welcome to Verizon Online

- Home
- Verizon Central
- E-Mail & More
- Help & Support
- My Account
- My Web Space
- Music, Games & Video
- Latest Internet Products
- Resource Center
  - Control Pad
  - Perks
  - Announcements
  - Instant Messaging
  - DSL Support Center
  - Verizon Wi-Fi
  - Contact Us
  - DSL Guide
  - Switching Tips
  - Online White Pages
  - Online Yellow Pages
  - System Status
  - Dial-up Access Numbers
  - Policies Section
  - Moving Help
  - Internet Security Center
  - Safeguard Your Computer
  - Child Safety Software
- More From Verizon

Resource Center

Internet Security Center

Learn about the latest Internet-borne threats and get information on safety updates and precautions.*
You would never leave your home unprotected from outside threats, so why leave your computer vulnerable? With the increase in the number of v horses and hackers on the Web, keeping your computer protected is more important than ever. Keep up with the latest viruses, get tips for keepin safe and more. Bookmark this site and check back often for updates.

Threat Watch List

Name	Discovered	Comments
Sasser	4/30/04	Also known as: WORM_SASSER, W32/Sasser.Worm Sasser spreads to Windows 2000 and Windows XP PC's via the Intern nobody is using the PC at the time. The worm infects PCs without any part of the computer user. Learn More
Phishing Scam Alert	4/21/04	A rash of e-mail scams have been identified on the Internet in recent w recent e-mail version claims to represent "Verizon Account Specialist S asks Verizon customers to update their Verizon Online billing informati $7.99 processing fee. The e-mail contains a "click here" link that actual the e-mail recipients to a fraudulent Verizon look-alike site to complete THIS MESSAGE IS NOT AUTHORIZED BY VERIZON. IT IS A SCAM. Learn More
W32.Beagle.J@mm	3/2/04	Also Known As: W32/Bagle.j and W32.Beagle.I This virus contains me that are constructed with several parts to effectively customize the ema appear to be a legitimate E-Mail warning notification from your Internet Provider. Learn More
International Modem Dial Scam	N/A	Verizon Online has been alerted that there is a known Internet scam ta who download software from the Internet, leading users to unknowingl charges – often running to the hundreds of dollars – on their phone bill Learn More
W32.Netsky.B@mm	2/18/04	Also known as: Moodown. W32.Netsky.B is a mass-mailing worm that SMTP engine to send itself to the email addresses it finds when scanni drives and mapped drives. This worm also searches drives C through names containing "Share" or "Sharing," and then copies itself to those Subject, Body, and email attachment vary. Learn More
Mydoom	1/28/04	Also Known As: Mydoom.B [F-Secure], W32/Mydoom.b@MM [McAfee WORM_MYDOOM.B [Trend], Win32.Mydoom.B [Computer Associates Worm.Mydoom.b [Kaspersky], W32/MyDoom-B [Sophos] Learn More
W32.Beagle.A@mm	1/18/04	Also known as: I-Worm.Bagle [Kaspersky], WORM_BAGLE.A [Trend], [Sophos], W32/Bagle@MM [McAfee], Win32.Bagle.A [Computer Assoc
Mimail	1/7/04	Also known as: W32.Mimail.P@mm, W32/Mimail.p@MM [McAfee], Wi [Computer Associates], WORM_MIMAIL.P [Trend], WORM_MIMAIL.A W32/Mimail@MM [McAfee], Win32.Mimail.A [CA], W32/Mimail-A [Sopl Worm.Mimail [KAV], W32/Mimail.c@mm [McAfee], Worm_Mimail.C [Tr W32/Mimail-C [Sophos], Mimail.C [AVP], W32/Mimail.d@mm [McAfee] Worm_Mimail.D [Trend], W32/Mimail-D [Sophos], Mimail.D [AVP], W32/Mimail.e@mm [McAfee], Worm_Mimail.E [Trend], W32/Mimail-E Mimail.E [AVP], W32.Mimail.L@mm [McAfee]

Please note: There are a variety of virus watch companies who monitor, identify, and sometimes name the latest threats. Names and acronyms (such as [KAV], [Sophos], etc.) reference these companies.

How to Safeguard Your Computer

Follow these 3 steps to help protect your computer from potential threats:

Step 1: Activate a Firewall
If you have a personal firewall, make sure that it is enabled. A firewall will

How to Remove a Threat from Your Computer

Follow these 2 steps:

Step 1: Protect Your Computer
It is recommended that you follow the 3 steps outlined in the

help to protect your computer by stopping unknown intrusions and controlling what gets into AND out of it. If you do not have a firewall, you can purchase one like ZoneAlarm(R) Pro. As a Verizon Online subscriber you can try it free for 90 days.

Step 2: Use Your Anti-Virus Software
If you already have anti-virus software on your computer, make sure that you have the latest updates. Please contact your anti-virus software vendor if you are unsure as to whether or not you have the latest updates.

Step 3: Get the Latest Windows Update(s)
If you use Microsoft Windows, make sure you have the most recent updates. To do this:

- Click the Start button in the bottom left corner of your screen.
- Select Windows Update.
- Follow the instructions to install the latest updates.
- If you can't find Windows Update on your computer, go directly to: http://windowsupdate.microsoft.com

Safeguard Your Computer" section. This will help to ensure th computer is protected from any other potential threats.

Step 2: Find & Remove the Threat
Search for the virus on your system using your anti-virus soft not have anti-virus software or feel your software isn't workin search your computer using a web based virus scan, such as Once you have identified the virus, use the removal tool to ge

[illegible]

[illegible]

[illegible] All Rights Reserved
[illegible]

veri on

Search Go

Verizc

Welcome to Verizon Online

- Home
- Verizon Central
- E-Mail & More
- Help & Support
- My Account
- My Web Space
- Music, Games & Video
- Latest Internet Products
- Resource Center
  - Control Pad
  - Perks
  - Announcements
  - Instant Messaging
  - DSL Support Center
  - Verizon Wi-Fi
  - Contact Us
  - DSL Guide
  - Switching Tips
  - Online White Pages
  - Online Yellow Pages
  - System Status
  - Dial-up Access Numbers
  - Policies Section
  - Moving Help
  - Internet Security Center
  - Safeguard Your Computer
  - Child Safety Software
- More From Verizon

Resource Center

Announcements

Recent Announcements

- Important Information on the Sasser Worm - 5/06/04 NEW
- Supplier Federal Universal Service Fund (FUSF) Recovery fee on DSL Service. - 4/22/04 NEW
- Phishing Scam Alert: What It Is and What You Can Do About It - 4/21/04 NEW
- Verizon Online Now Offers Nationwide Dial-up Access – 3/18/04
- Help Keep Your Documents, Videos and Pictures Secure Online - 3/3/04
- INTERNET SCAM ALERT: Use caution when downloading software - 3/1/04
- Important information about Computer Viruses - 2/14/04
- Learn about Verizon Online DSL with MSN Premium services - 2/5/04
- Make your Mark on the Web with a Personal Website - 1/27/04
- Important information regarding Newsgroup Access Change on 12/8/03 - 12/5/03
- Potential password change issue for customers using the Westell 2200 modem - 11/10/03
- Verizon Online Implements Sender Verification - 11/3/03
- Verizon Online Implements Advanced Spam Fighting Measures - 10/31/03
- Announcing the Internet Security Center - 10/28/03
- Introducing the Verizon Business Center - 8/15/03
- Important Update on the "Blaster" Worm/Virus - 8/12/03
- Introducing Verizon Online Enhanced E-Mail & More Features - 6/9/03
- The New Start Page & Verizon Central Are Here! - 4/2/03
- Verizon Online System Enhancement Project - 3/30/03
- E-mailbox Policy Change - Implementation of e-mail inactivity policy - 2/27/03
- Important changes to your e-mail message retention period - 2/21/03
- Attention: NYC Dial-Up Customers - 1/28/03

Announcements

Important Infor
the Sasser Wc
Get more infor

Supplier Feder
Universal Serv
(FUSF) Recov
DSL Service.
Get more infor

Phishing Scan
What It is and
Can Do About
Get more infor

Mor

Today at Verizon

- See mobile ac
- Play your favc
- Send a text m
- Check who's c reverse numb
- See demos at Wireless

verizon

Home | Verizon Central | E-Mail & More | Help & Support | My Account | My Web Space
Music, Games & Video | Latest Internet Products | Resource Center | More From Verizon

veri on

Search Go

Verizc

Welcome to Verizon Online

- Home
- Verizon Central
- E-Mail & More
- Help & Support
- My Account
- My Web Space
- Music, Games & Video
- Latest Internet Products
- Resource Center
  - Control Pad
  - Perks
  - Announcements
  - Instant Messaging
  - DSL Support Center
  - Verizon Wi-Fi
  - Contact Us
  - DSL Guide
  - Switching Tips
  - Online White Pages
  - Online Yellow Pages
  - System Status
  - Dial-up Access Numbers
  - Policies Section
  - Moving Help
  - Internet Security Center
  - Safeguard Your Computer
  - Child Safety Software
- More From Verizon

Resource Center

Announcements

Phishing Scam Alert: What It Is and What You Can Do About It

Phishing scams use fraudulent e-mail addresses and Web sites designed to fool users into providing personal data such as credit card numbers, account user names, passwords, social security number, etc. By impersonating the trusted brands of well-known banks, online retailers, and other established businesses, phishers are able to convince recipients to respond to their inquiries or requests for personal information.

A rash of e-mail scams have been identified on the Internet in recent weeks. One recent e-mail version claims to represent "Verizon Account Specialist Services" and asks Verizon customers to update their Verizon Online billing information to avoid a $7.99 processing fee. The e-mail contains a "click here" link that actually forwards the e-mail recipients to a fraudulent Verizon look-alike site to complete a form.

THIS MESSAGE IS NOT AUTHORIZED BY VERIZON. IT IS A SCAM.
Appropriate action is being taken by Verizon to address this situation.
Be aware that a legitimate e-mail from Verizon will: 1) never ask you for your password, social security number, credit card number, or any other sensitive account information and, 2) never include any attachments. If you receive such an e-mail allegedly written on behalf of Verizon, do not reply to it. Instead Verizon strongly urges you to take the following actions:

1. Do not reply to the e-mail.
2. Delete the message immediately.
3. Do not open any attachments associated with the suspected e-mail.
4. Do not click on any associated links or fill out any information that the e-mail may be requesting.

To Learn More Visit These Additional Links & Resources:

- How Not to Get Hooked by a "Phishing" Scam
- Verizon Online Internet Security Center

Announcements

Important Infor
the Sasser Wc
Get more infor

Supplier Fede
Universal Serv
(FUSF) Recov
DSL Service.
Get more infor

Phishing Scan
What It is and
Can Do About
Get more infor

Mor

Today at Verizon

- See mobile ac
- Play your favc
- Send a text m
- Check who's c reverse numb
- See demos at Wireless

verizon
Make progress every day

Home | Verizon Central | E-Mail & More | Help & Support | My Account | My Web Space
Music, Games & Video | Latest Internet Products | Resource Center | More From Verizon

veri on

Search Go

Verizc

Welcome to Verizon Online

Home
Verizon Central
E-Mail & More
Help & Support
My Account
My Web Space
Music, Games & Video
Latest Internet Products
Resource Center
- Control Pad
- Perks
- Announcements
- Instant Messaging
- DSL Support Center
- Verizon Wi-Fi
- Contact Us
- DSL Guide
- Switching Tips
- Online White Pages
- Online Yellow Pages
- System Status
- Dial-up Access Numbers
- Policies Section
- Moving Help
- Internet Security Center
- Safeguard Your Computer
- Child Safety Software

More From Verizon

Resource Center

Announcements

Important Information on the Sasser Worm

There is a known worm (referred to as W32.Sasser.A and its variants) affecting Internet users worldwide. Sasser spreads to Windows 2000 and Windows XP PC's via the Internet, even if nobody is using the PC at the time. The worm infects PCs without any action on the part of the computer user.

After a machine gets infected, the worm will start to spread to other computers. As a side effect, users might see error messages and experience their computer rebooting repeatedly. Microsoft has a patch available and we urge you to apply the update immediately.

In order to help protect your computer, you should follow the steps below:

1) Activate a Firewall
If you have a personal firewall, make sure that it is enabled. A firewall will help to protect your computer by stopping unknown intrusions and controlling what gets into AND out of your computer. If you do not have a firewall, you can purchase one like ZoneAlarm(R) Pro. As a Verizon Online subscriber you can try ZoneAlarm(R) Pro free for 90 days.

2) Install the Security Patch & the Latest Windows Updates
To install the patch for your operating system, go to Microsoft's Sasser information site and follow the instructions provided.
To ensure that you have the latest Window Update:

- Click the Start button in the bottom left corner of your screen.
- Select Windows Update from the menu.
- Follow the instructions to install the latest updates.
- If you can't find Windows Update on your computer, go directly to: http://windowsupdate.microsoft.com

3) Use Your Anti-Virus Software
If you already have anti-virus software on your computer, make sure that you have the latest updates and run a complete system scan immediately.

4) Run the "Sasser" Worm Removal Tool
If you think that your computer may be infected with the "Sasser" worm go to the Symantec site and follow the instructions to run the Sasser worm removal tool. For detailed information and additional patches go to the "What You Should Know About the Sasser Worm and Its Variants" article on the Microsoft site.

5) Visit the Internet Security Center
Learn about the latest Internet-borne threats and get information on safety updates and precautions on the Verizon Online Internet Security Center. If the problem persists please contact your Operating System vendor or your Computer Manufacturer.

Announcements

Important Infor
the Sasser Wc
Get more infor

Supplier Fede
Universal Serv
(FUSF) Recov
DSL Service.
Get more infor

Phishing Scan
What It is and
Can Do About
Get more infor

Mor

Today at Verizon

- See mobile ac
- Play your favc
- Send a text m
- Check who's c reverse numb
- See demos at Wireless

verizon
Make progress every day

Home | Verizon Central | E-Mail & More | Help & Support | My Account | My Web Space
Music, Games & Video | Latest Internet Products | Resource Center | More From Verizon

© 2004 Verizon Online. Internet access services are free also for subscriber user companies with dial-up. All Rights Reserved.
Use of Verizon Online Internet access services are free also for subscriber user companies with dial-up.

Internet Security Center

Online

Help Fight Hackers with a PC Firewall from Zone Labs

With your Verizon Internet service, you have the tools and freedom to do everything you want online. But it's important to make sure you and your PC are safe.

Hackers, data thieves, and cybercriminals continually develop new methods to break into computers, while malicious programs, such as worms and Trojans, are circulated to unsuspecting computers in an attempt to erase information, spread themselves, or spy on you.

Zone Labs' ZoneAlarm® Pro blocks these and other emerging Internet threats. It also helps protect your privacy and has features that guard your identity from being stolen.

Get ZoneAlarm Pro

Special Verizon Online Offer
$39.95 (Save $10)

ZoneAlarm Pro helps protect you and your computer in these ways:

- **Firewall** blocks known and unknown threats
- **Antivirus Monitoring** helps make sure your antivirus software isn't turned off and is kept up-to-date for complete protection
- **Automatic Program Control** tells you whether to allow or deny programs requesting Internet access to ensure malicious programs can't "phone home"
- **Privacy and ID Theft Prevention** with ID Lock, Cookie Control, and Cache Cleaner features
- **MailSafe** quarantines 47 types of suspicious e-mail attachments and monitors outbound e-mail for virus-like behavior to prevent a rogue e-mail from being sent to everyone in your address book
- **Ad Blocking** blocks pop-ups, pop-unders, and banner ads so you can surf in peace
- **Easy Install & Set Up** allows you to be protected in minutes with "set and forget" security

If you'd like to try out the protection of ZoneAlarm Pro for 90 days free of charge, download the trial version for free.

Software is provided by Zone Labs. Verizon Internet Services Inc. ("VIS") and GTE.Net LLC d/b/a Verizon Internet Solutions ("GTE.Net") (collectively referred to herein as "Verizon Online") do not provide software and/or products offered on this Web site. Verizon Online makes no representations or warranties of any kind, either express or implied, including, without limitation, warranties or conditions of title, or implied warranties of merchantability or fitness for a particular purpose, or non-infringement. Verizon Online is not responsible for examining or evaluating, and we do not guarantee or warranty the product offerings of this Web site. In no event shall Verizon Online be liable for special, indirect, exemplary, or consequential damages or any damages whatsoever,

Back to Verizon Online

Proven PC Protection

With over 25 million PCs protected around the globe, Zone Labs' award-winning personal firewall technology is the world's most trusted Internet security solution.

Find out more

Zone Labs Technical Support

ZoneAlarm Pro Demo
(requires Flash player)

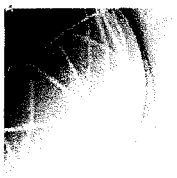
NEW!
See a Demo

Need Flash Player?

including but not limited to loss of use, data, or profits, without regard to the form of any action, including but not limited to contract, negligence, or other tortious actions, all arising out of, or in connection with the use, misuse, copying or display of the products or services presented on this site. Zone Labs is solely responsible for their own obligations to you. If a product offered on this site does not function as described or represented by Zone Labs, your sole remedy is to return it to seek any remedy from Zone Labs.

* - One or two years of access to updates, support, and services included with purchase of Zone Labs security software; annual maintenance contract required for subsequent access.

Copyright ©1999-2004 Zone Labs, Inc.



CYBER SECURITY INDUSTRY ALLIANCE

CYBER SECURITY INDUSTRY ALLIANCE
1201 PENNSYLVANIA AVENUE, NW
SUITE 300
WASHINGTON, DC 20004
PHONE: 202-204-0838

CSIA Testimony
June 16, 2004
Testimony before the House Subcommittee on Technology, Information Policy, Intergovernmental Relations and the Census

EXECUTIVE DIRECTOR
PAUL KURTZ

CHAIRMAN OF THE BOARD
JOHN THOMPSON, CEO
Symantec Corporation

BOARD MEMBERS

ERIC PULASKI, PRESIDENT & CEO
BindView Corporation

JERRY UNGERMAN, CEO
Check Point Software Technologies Inc.

STEVEN SOLOMON, CHAIRMAN & CEO
Citadel Security Software Inc.

RUSSELL ARTZT, EXECUTIVE VICE PRESIDENT, eTRUST SOLUTIONS
Computer Associates International, Inc.

BILL CONNER, CEO
Entrust Inc.

THOMAS NOONAN, CEO
Internet Security Systems Inc.

ROBERT THOMAS, CEO
NetScreen

GEORGE SAMENUK, CEO
Network Associates Inc.

PHIL DUNKELBERGER, CEO
PGP Corporation

PHILIPPE COURTOT, CHAIRMAN & CEO
Qualys Inc.

ARTHUR COVIELLO, CEO
RSA Security, Inc.

JOHN MCNULTY, CEO
Secure Computing Corporation

Mr. Chairman and Ranking Member Clay, thank you for inviting the Cyber Security Industry Alliance (CSIA) to testify before the House Subcommittee on Technology, Information Policy, Intergovernmental Relations and the Census.

This is the first opportunity I have had as the Executive Director of the Cyber Security Industry Alliance to testify before Congress. I am pleased to speak about the cyber security challenges facing home users and small business today.

I will cover three areas in my testimony.

- The purpose of CSIA and how we view the issue of cyber security;
- The importance of securing home and small businesses and the challenges they face today;
- The activities underway to secure home users and small businesses;

Before I begin my remarks, I want to commend Chairman Putnam for his leadership in the area of cyber security. The Corporate Information Security Working Group has made significant contributions to advancing dialogue, understanding, and awareness of cyber security policy issues in both the public and private sector.

CSIA's Approach to Cyber Security

The cyber security industry plays a unique and critical role in enabling the IT revolution. We ensure the confidence, reliability, and trust of information networks. While we are suppliers, we must work closely with both the producers of hardware and software as well as consumers ranging from large enterprises to small businesses and home users. Our member companies partner with suppliers to make products more secure and protect end-users from attack. We must remain agile, responding daily to new threats and vulnerabilities on ever changing systems and devices.

CSIA is dedicated to enhancing cyber security through public policy initiatives, public sector partnerships, corporate outreach, academic programs, alignment behind emerging industry technology standards and public education. Launched in February 2004, the CSIA is the only public policy and advocacy group comprised exclusively of security software, hardware and service vendors addressing key cyber security issues. Our Board members are almost exclusively CEO's and are committed to advancing cyber security policy.

Members include: BindView Corp; Check Point Software Technologies Ltd; Citadel Security Software Inc; Computer Associates International; Entrust, Inc; Internet Security Systems Inc; NetScreen Technologies, Inc.; McAfee formerly Network Associates, Inc.; PGP Corporation; Qualys, Inc.; RSA Security Inc.; Secure Computing Corporation and Symantec Corporation.

We encourage the membership of other firms with substantial business and technology offerings in cyber security. In addition to our Charter and Principal membership categories, I am pleased to announce today that the CSIA Board of Directors has approved two new affiliate membership categories to facilitate the participation of small security firms as well as large IT hardware and software firms. The affiliate memberships will allow firms to participate in CSIA working committees and events.

CSIA's approach to cyber security policy can be defined by four tenets each of which relates to today's topic:

- First, we must not only protect systems against viruses and worms but we must also authorize and authenticate users and encrypt sensitive information wherever appropriate. Cyber security spans the confidentiality, integrity, and availability of information systems.
- Second, CSIA believes cyber security should primarily be seen in terms of business and economic security. In the post 9-11 environment, there are frequent attempts to define an issue in terms of "homeland security" in order to drive action. Cyber security has been no exception. While we do not discount that terrorists will likely launch cyber attacks against critical information infrastructure, they are not behind today's attacks which are costing the U.S. and global economy billions of dollars in lost productivity, personal identity, and intellectual property. By increasing cyber security for economic reasons, we will have the fortuitous byproduct of hardening information infrastructure against potential terrorist attack.

- Third, the private sector is in the best position to improve cyber security. This is consistent with President Bush's *National Strategy to Secure Cyberspace* which states that, "in general, the private sector is best equipped and structured to an evolving cyber threat." It is also consistent with the recently released Business Roundtable (BRT) cyber security framework which states, "traditional regulations directing how companies should configure their information systems and networks could discourage more effective and successful efforts by driving cyber security practices to a lowest common denominator, which evolving technology would

quickly marginalize." The BRT continues that a regulatory approach could result in more homogeneous security architectures that are less secure than those currently deployed. Given the complexity and dynamism of cyberspace, the marketplace will provide in most cases the necessary impetus for improving IT security. Finally, in those instances where existing market forces fail to provide such impetus, incentive programs that rectify market shortfalls and encourage proactive security solutions should be considered and adopted as appropriate.

- Fourth, we look to the Federal government for leadership. The Federal government should foster collaboration, reduce legal barriers, and lead by example.

The Importance of Securing Home Users and Small Business

Security Enabling E-Commerce

Mr. Chairman, home users and small business make up a very large segment of the current and potential computer market. Current and prospective home users encompass some 270 million Americans. According to the House's Small Business Committee the category of "small businesses" in the United States includes over 22 million non-farm firms, making up over 50 percent of private-sector workers. And, small businesses obtain 33 percent of federal prime and subcontract dollars.

It is useful to define the number of home users and small businesses in the terms of the growth of broadband service. According to the Federal Communications Commission, high-speed Internet access in the United States increased by 42 percent last year as some 8.3 million homes and businesses signed up for broadband service,. Driven largely by new residential and small-business customers, broadband use grew to 28.2 million lines by the end of 2003. While not all home users and small business are operating in an "always on" broadband environment, the numbers are expected to continue to grow, particularly in light of President Bush's goal to ensure affordable access to broadband to all Americans by 2007.

Broadband will create a greater potential for e-commerce. The potential for e-commerce is enormous; the next round of innovation and services on the Internet can only grow if home users and small businesses are confident in their information systems. Security is perhaps the greatest obstacle to the expansion of on-line commerce and services.

Security Challenges

Home users and small business face a challenging environment--identity theft, and on- line fraud perpetrated via phishing scams and bad actors using spyware, to name just a few. Home users and small business will be slow to drive on-line commerce given these challenges.

According to a Federal Trade Commission 2003 analysis, identity theft affected nearly ten million Americans and cost almost $53 billion over the previous year. Incidents reported

to the FTC increased 73 percent over the previous year and accounted for 43 percent of the complaints fielded by the FTC.

CSIA member firms report that we have seen an increase in computer viruses designed to steal victims' personal information. One reported in March that the last six months of 2003 showed over a 500 percent rise in the volume of viruses that constituted threats to user privacy and confidentiality compared with the first six months of 2003. Another member firm said reports generated by its VirusScan software of what it calls such "potentially unwanted programs" grew to nearly 2.6 million in March from 643,000 last September.

Phishing attacks use "spoofed" e-mails and fraudulent websites designed to fool recipients into divulging personal financial data such as credit card numbers, account usernames and passwords, social security numbers, etc. By hijacking the trusted brands of well-known banks, online retailers and credit card companies, phishers have been able to convince up to 5 percent of recipients to respond to them. In April there were over 1,000 unique phishing attacks reported to the "Anti-Phishing Working Group"—a 180 percent increase over the number of attacks in March.

Home users and small business also face adware and spyware. Adware constitutes programs that secretly gather personal information through the Internet and relay it back to another computer, generally for advertising purposes. This is often accomplished by tracking information related to Internet browser usage or habits. Adware can be downloaded from Web sites (typically in shareware or freeware), email messages, and instant messengers. A user may unknowingly trigger adware by accepting an End User License Agreement from a software program linked to the adware. Many manufacturers of free programs rely on adware to profit from their no-cost products. In some cases, manufacturers also make ad-free versions of the same freeware and shareware products available for purchase.

Spyware are stand-alone programs that can secretly monitor system activity. These can detect passwords or other confidential information and transmit them to another computer. Spyware can be downloaded from Web sites (typically in shareware or freeware), email messages, and instant messengers. A user may unknowingly trigger spyware by accepting an End User License Agreement from a software program linked to the spyware. Hijacking programs also fall under the spyware label. Hijacking programs often use deceptive dialogue boxes to trick users into installing them. Others exploit vulnerabilities in browsers to integrate into the user's system. Upon installation, these programs might change the user's home or search pages or even use the hijacked system for unauthorized activities.

Activities Underway to Secure Home Users and Small Businesses

Market Solutions

With this in mind Mr. Chairman I would like to offer a few examples of how the private sector—particularly the cyber security industry—is improving security for home users and small businesses.

Two CSIA member firms have established partnerships with leading ISPs to provide security solutions to home users and small businesses. In one case the security vendor-ISP partnership has blocked more than a billion virus attachments from reaching its members since it launched automatic e-mail attachment screening and premium anti-virus protection roughly a year ago. The ISP stated the service has protected each of its members from an average of 30 different virus attacks, or an attack every ten days. Services are expanding as well using more advanced services to scan all incoming and outgoing attachments to members' e-mail each day for known viruses. If a virus is detected, the attachment is automatically cleaned of the virus, or, if the virus cannot be fixed or quarantined, the e-mail is returned without the infected attachment to the original sender with a notice that their attachment contained a virus. The virus definitions are regularly updated.

In another case a CSIA member firm is offering an antivirus and firewall subscription bundled with an ISP's service. Rather than having to pay for a security software package and a year of updates--which must then be renewed a year at a time--this offering lets consumers pay through their ISP billing.

The bundling of antivirus and firewall protection with an ISP is a significant development. I recall several years ago when this was initially proposed and it met with resistance. Now we see partnerships developing between the security community and the IPS's to provide consumers real time protection and support services.

In addition to protecting against viruses, authentication and encryption technologies assist home users and small businesses. This is a challenging environment given that a recent survey revealed that 70 percent of people would reveal their computer password in exchange for a candy bar. Thirty-four percent required no bribe. Family names, pets, football teams were used by many questioned to provide inspiration for a password. A CSIA member firm survey found that many people volunteered important personal information, such as their mother's maiden name or their own date of birth.

Maintaining on-line identities is becoming a burden for many people who, on average, use 20 sites that require them to register and log-on afterwards. To ease the burden, two thirds of the respondents said they use the same password. A third of the respondents said they shared passwords or wrote them down to make it easy to remember which one to use.

These statistics show that home users and small businesses would greatly benefit from greater use of two-factor authentication. With this context, I note another CSIA member firm announced a partnership with a major operating system provider to develop a version of its secure ID token to support the operating system. The system will provide an additional layer of security. Under the plan users will only be asked to remember a single PIN (personal identification number) when the token is used to access the operating system. A rotating password will be supplied via the CSIA member firm.

Other CSIA firms offer other forms of protection for home users and small business in the area of encryption. One such technology enables individuals to protect confidential communications and digitally stored information with an integrated solution based on strong, broadly adopted security technology. The service includes e-mail, file and disk storage encryption. Together, these features provide strong security for an individual's confidential information no matter where it is located—stored on a computer or laptop, at every point in transit through email, or on a recipient's computer. The service integrates with popular email applications and operates on all mainstream operating system platforms.

President Bush's *National Strategy* states that home users and small businesses can help the nation secure cyberspace by securing their own connections to it. It continues, that by installing firewall software and updating it regularly, maintaining current antivirus software, and regularly updating operating systems and major applications with security enhancements are actions that individuals can take to help secure cyberspace. Indeed individuals should take these steps, but what has changed since the *National Strategy* was issued in February 2003 is the partnership between the security industry and the major networking and operating system providers. These partnerships—which are largely market driven--have eased the burden on the consumer while working to secure cyberspace. I am confident that other security vendors will have additional partnerships with ISPs, networking, and operating system providers in the coming year in several areas of information security, making a range of services more easily available to customers.

Mr. Chairman, I want to briefly address legislation currently under consideration by Congress regarding spyware. I would caution against legislation that attempts to address spyware through technology and not behavior. Technologies similar to those used for spyware are used by security companies to secure computers with automatic updates and anti piracy programs. Government should punish those that deceive users while allowing while allowing the development of innovative technologies that will increase security.

Awareness

While partnerships have developed between security firms and networking and operating system providers, awareness still requires attention. Raising awareness is also a key factor in addressing the security challenges home users and small businesses face today. I am pleased to announce today that CSIA has joined the National Cyber Security Alliance (NCSA).

Mr. Doug Sabo, Member of the Board of Directors of the National Cyber Security Alliance and McAfee's Director of Government and Community Relations, testified before this committee on April 21 on NCSA's activities. NCSA is the only 501(c) 3 focused on delivering cyber education to home users and small businesses. NCSA is a true public private partnership. NCSA works closely with the White House, Federal Trade Commission, FBI, the Small Business Administration, the Department of Homeland Security, the Department of Commerce, and other government agencies at the federal, state, and local level.

NCSA understands the important role that home users, small businesses and our youth play in contributing to our overall cyber security. NCSA has developed a number of initiatives; including an awareness campaign targeted at home users and small businesses. Through the NCSA website: www.staysafeonline.info visitors can find self-tests, security tips, and helpful links. NCSA will also produce toolkits for small businesses and subgroups within the home user audience. These toolkits will include materials, guidebooks and training programs. NCSA is also developing a major effort that will focus on educating youth on cyber security practices to make sure the next generation of users is cyber secure.

CSIA will act through the NCSA to raise awareness for home users and small businesses.

Conclusion

Mr. Chairman, before closing I want to highlight an area where CSIA believes the Federal government is demonstrating leadership that relates to home users and small business.

The U.S. government has a strategy centered on the creation of a "citizen-centered E-Government." Central to enabling the implementation of e-government services in the U.S. is the Federal e-Authentication Initiative, which is administered by the General Services Administration (GSA). While this program has struggled in the past, we see new momentum and leadership—the fourth tenet I described earlier. For example, at this year's industry-wide RSA Conference in San Francisco, the GSA hosted the first multi-vendor interoperability lab which included an interactive demonstration of Secure Assertion Markup Language (SAML) v1.1 SSO interoperability. Some of CSIA's member companies have already been approved for use by federal agencies in implementing the government's E-Authentication Initiative, placing CSIA vendors squarely in the U.S. Government "Circle of Trust" for enablement of e-government services. This program will ultimately have a direct impact on the security of home users and small business.

Mr. Chairman, thank you for inviting me to testify today. Home users and small businesses face significant cyber security challenges today. The security of each is critical to the future of e-commerce. The security industry's role is unique and critical. We must partner with suppliers to make the software and hardware more secure as well as protect home users and small businesses from attack. Over the past year the security industry, partnering with ISPs, and networking and operating system providers have begun to

provide solutions to home users and small businesses. These partnerships have eased the burden on both. However, we must be active, engaging with suppliers to establish more partnerships as well increase awareness through organizations like the NCSA. CSIA is committed to doing just that.