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

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.

<u>Awareness</u>

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.