PREPARED TESTIMONY OF THE NATIONAL CYBER SECURITY ALLIANCE
MICHAEL KAISER, EXECUTIVE DIRECTOR

ON THE STATE OF CYBERSECURITY AND SMALL BUSINESS

BEFORE THE
COMMITTEE ON HOUSE SMALL BUSINESS SUBCOMMITTEE ON HEALTHCARE AND TECHNOLOGY

UNITES STATES HOUSE OF REPRESENTATIVES

WASHINGTON D. C.

DECEMBER 1, 2011

Chairwoman Ellmers, Ranking member Richmond, and members of the subcommittee, thank you for the opportunity to testify today on the current state of cybersecurity and small businesses. My name is Michael Kaiser and I am the Executive Director of the National Cyber Security Alliance (NCSA). Thank you for inviting me to discuss the current state of cybersecurity and small businesses.

Since its inception ten years ago, the issue of cybersecurity has been the core area of work for the National Cyber Security Alliance. NCSA is a 501 (C) 3 nonprofit organization. We operate as public private partnership working with industry leaders and government on education and awareness issues in cybersecurity. NCSA's Board of Directors is comprised of representatives from 18 companies: ADP, AT&T, Bank of America, Cisco, EMC^2, ESET, Facebook, General Dynamics Advanced Information Systems, Google, Intel, Lockheed Martin, McAfee, Microsoft, PayPal, SAIC, Symantec, Verizon and VISA. In addition, NCSA works with many other companies, nonprofit organizations, government agencies and education institutions to achieve our mission.

NCSA is the leading education and awareness nonprofit on cybersecurity. NCSA leads critical efforts such as the STOP. THINK. CONNECT., the first ever national cybersecurity awareness campaign (in partnership with the Anti-phishing Working Group) and the

Department of Homeland Security as the lead Federal Partner, National Cyber Security Awareness Month, and Data Privacy Day. NCSA has a long track record in conducting surveys about the practices of individual computer users and small businesses as well as the state of cybersecurity education in U. S. schools. NCSA recently signed a memorandum of understanding with the Department of Education and National Institute of Standards and Technology to establish a public partnership to address the county's approach to cyber education from basic education to career pathways.

This past October, NCSA released the results of a study conducted in conjunction with Symantec about the cybersecurity practices of small businesses. The study was conducted by Zogby International, which polled 1,045 U.S. small business owners.

There is little doubt that small businesses are becoming increasingly dependent on the Internet and the survey bears this out. Businesses still allow a considerable amount of risky behavior and don't have employee policies in place or strategic approaches to cybersecurity. This all leads to a false sense of security on the part of small business operators.

The Internet has become a critical engine for small business. Business operators surveyed reported high integration of the Internet into their daily business:

- Two-thirds (66%) say that their business is dependent on the Internet for day-to-day operations

    - two-fifths (38%) characterize it as very dependent
    - two-thirds (67%) say they have become more dependent on the Internet in the last 12 months.
- Sensitive information businesses report handling:
    - more than two-thirds have customer data (69%)
    - almost half deal in financial records and reports (49%)
    - almost one-quarter (23%) have their own intellectual property
    - nearly one-fifth (18%) handle intellectual property belonging to others outside of the company.

- A majority of small business owners (57%) say that the loss of Internet access for 48 straight hours during a regular business week would be disruptive to their business and two-fifths (38%) say it would be extremely disruptive.

Small businesses have a lack of cyber security policy, planning and practice:

- seventy-seven percent (77%) do not have a formal written Internet security policy for employees.
- of those who don't have a formal policy, almost half do not have an informal policy either (49%)
- a majority (56%) do not have Internet usage polices that clarify what websites and web services employees can use

- almost two-thirds (63%) do not have policies regarding how their employees use social media.
- two in five small businesses (40%) do not have a privacy policy in place that their employees must comply with when they handle customer information
- almost half (48%) do not have a plan or strategic approach in place for keeping their business cyber secure.
- More small business owners say they do not (45%) provide Internet safety training to their employees than those that do (37%).
- Two thirds (67%) allow the use of USB devices in the workplace.

- Six in ten (59%) say they do not require any multifactor authentication for access to any of their networks
- only half (50%) say that all of their machines are completely wiped of data before disposal.

Yet, in spite of the poor practices and the lack of planning and policies and policies, cybersecurity is increasingly important to the value of a business:

- Seven in ten (69%) say that Internet security is critical to their business's success.
- A majority (57%) believes that having a strong cyber security and online safety posture is good for their company's brand.

We also found a disconnect exists between perceptions of cyber security preparedness and reality among U.S. small businesses:

- Two fifths (40%) say that if their business suffered a data breach or loss such as loss of customer or employee information, credit or debit card information or loss of intellectual property, their business does not have a contingency plan outlining procedures for responding and reporting it.
- Small business owners are most concerned about their employees picking up a computer virus while on the Internet (32%), followed by:
    - spyware/malware (17%)
    - loss of data (10%)
    - ID theft (8%)
    - loss of customer information (8%)
    - loss of intellectual property (4%)
    - seeing objectionable content and loss of employee data (1%)

Small businesses are increasingly using mobile devices, however:

- the majority (72%) do not let employees access company files/data remotely from mobile devices
- More than half (59%) work from home computers/access company information from personal mobile devices
- More than a third (37%) do not have employee policy/guidelines in place for remote use on mobile devices.

Despite all of these security risks and concerns, a very large majority (85%) say that given the measures they have taken, their company is safe from hackers, viruses, malware, and cyber-security breaches.

- Three quarters (72%) say they would know if their computer network was compromised
- nine in ten (91%) say their company has never suffered a security breach in which important information was stolen from a computer or their network.
- Of those who did suffer a breach, the majority says they told their customers about it (57%).

Small businesses need well-trained employees ready to use technology safely, securely, ethically and productively. When employers were asked to rate skills necessary for new hires, U.S. small businesses report the following skills are very relevant or essential:

- Understanding privacy (51%);
- Importance of protecting intellectual property (49%);
- Basic knowledge of using technology ethically (47%);
- Basic knowledge of Internet security practices (passwords, identifying secure websites) (44%).

The complete study can be found at:

http://www.staysafeonline.org/sites/default/files/resource_documents/2011%20SMB%20Study%20.pdf.

This data shows that we need to not only reach individual small businesses and help them build a better-defended environment, but that the entire small business ecosystem is at risk. We need to instill cybersecurity as a basic practice at all small businesses connected to the Internet. Small businesses owners need to see themselves as not only protecting themselves but also protecting their customers, their employees and the Internet. They need to understand that increasingly, cybercriminals see small businesses as targets. Cybercriminals know, as our data suggests, that small businesses are less defended and more vulnerable. And it may be easier or more profitable to steal money or data from a small business then to try and harvest millions of credit card or other records. By compromising a small business, cybercriminals can steal data, for example that of customers, and use the trusted relationship of the small business to prey on their customers, such as sending phishing emails that look like they come from the business and are sent to real customers and appear to be from a person they know.

Small businesses sense of security is especially unwarranted given that 40% of all targeted cyber attacks are directed at companies with less than 500 employees, according to Symantec data (http://bit.ly/njTeMU). In 2010, the average annual cost of cyber attacks to small and medium sized business was $188,242. What's more, statistics

show that roughly 60% of small businesses will shut down within six months of a cyber attack (http://www.businessinsider.com/the-challenges-in-defending-against-malware-2011-9). According to the Norton Cybercrime Report, the total cost of cyber crime to consumers and small business owners alike is greater than $114 billion annually (http://norton.com/cybercrimereport).

Therefore, we must look at cybersecurity more broadly as an economic security issue. We can ill afford to have our small businesses under constant attack. It is difficult enough for small businesses to make it and thrive; we shouldn't be losing them to cybercriminals.

Changing the cybersecurity posture of small businesses is going to take a collaborative effort. Small businesses are difficult to reach on this issue. Generally the owner/operators in charge of IT issues (59% according to the NCSA/Symantec study) as one of the many hats they wear, and may see cybersecurity as either a cost burden (32% in the NCSA/ Symantec study reported lack of funds to invest as an obstacle) or as not critical (23% in NCSA/Symantec study report cybersecurity as just a nice thing to have). To be effective any efforts should include a brad array of stakeholders from industry, government, and nonprofits. There is no single company, government agency, trade association or nonprofit group that can take on this vast issue alone or reach every small business. Working together, leveraging each others resources and engaging networks—trade associations, government agencies, industry leaders and others—that small

businesses already trust, is our best hope for making the wide scale impact that is needed.

Based on the premise of a collaborative approach here are some specific suggestions to address the cybersecurity issues of small businesses.

- **Create a harmonized message and campaign that can be deployed by key stakeholders**. Like the STOP. THINK. CONNECT. campaign, a harmonized message used by trusted entities in the small businesses community could go a long way towards clarifying for businesses owners the need to have up-to-date cybersecurity practices and inspire them to action and take responsibility for securing their businesses. This campaign should be built around positive messages about the role of cybersecurity in growing a business and should be built by a diverse partnership of industry, government and nonprofits. The campaign should be based on research to see what messages would resonate with small businesses. Negative or fear based messages are unlikely to be effective. In a study NCSA conducted with VISA in 2010, we found that 85% of small businesses believe they are less of a cybercrime target than large companies (http://www.staysafeonline.org/sites/default/files/resource_documents/2010_NCSA_VISA_SB_Study_Factsheet_FINAL%2011%2023.pdf), which is clearly in opposition to previously stated data. In addition to creating awareness about the need for cybersecurity in small businesses the campaign should include advice

about basic protections—software updates, basic security practices (password management, authentication, etc.)—training materials for employees and best practices. By unifying the messaging across all trusted networks, we have the best chance of reaching every business and strengthening the entire small business ecosystem.

- **Align forces within the Federal government to support small businesses and cybersecurity.** As one of the most important factors in a strong economy, many federal agencies have an interest in helping small businesses grow while protecting their digital assets. By working together, Federal agencies can bring their expertise to the table and assist each other in outreach and education of small businesses. At a minimum, the Small Business Administration, The Department of Commerce (including representation from NIST), the Federal Trade Commission, the Federal Communications Commission and the Department of Homeland Security should participate. Others such as the Department of Defense and Internal Revenue Service, that work with or reach small businesses should also be included. A unified government approach would take advantage of each agency's reach and day-to-day contact with small businesses.
- **Engage local communities in the effort.** Small business owners are perhaps most likely to be influenced by their peers at the local level. These are the people they interact with on a day-to-day basis and they may also belong to local groups—Chamber of Commerce, Rotary or other business/civic association. A few

forward thinking communities such as Washtenaw County, MI, San Diego, California, San Antonio, Texas and Colorado Springs, CO have started efforts to make their communities more cyber secure. In each community, they have prioritized helping small businesses. They recognize the important role small businesses play in their communities and the need to strengthen their community's cybersecurity must include small business if they are going to be successful. Because they are local and the leaders of these efforts are known and trusted community members, they can reach many small businesses others cannot.

- **Support education reform that leads to graduating a more cyber-capable workforce.** In the 21st century, we will need a workforce that understands how to use technology safely. We can assume, given current trends, that a vast majority of jobs will include using Internet connected technology. To be successful, small businesses will need a workforce ready, when they graduate high school and college, be educating young people to be safe and productive employees from day one. We know that in the K-12 education system children are not get getting the basics of a cybersecurity education. Research NCSA conducted with Microsoft found that the topics are not being taught in the classroom, teachers do not feel prepared to teach the topics and teachers are not receiving professional development on the topics. As an example the survey found that, 76% of K-12 teachers had received less than 6 hours professional development on these topics in the last year. More than a third had received 0

hours

(http://www.staysafeonline.org/sites/default/files/resource_documents/K-12%20Study%20Fact%20Sheet%20FINAL_0.pdf). In addition to basic skills of all employees, it is likely that small businesses will also increasingly need the help of trained cybersecurity experts to insure that their business are keeping up with the latest security practices, technology and threats. We face a serious shortage of trained cybersecurity professionals in this country. Right now large industry and government are competing for the graduates that do exist and estimates of the need for new professionals ranges up to more than 700,00 in the Americas and almost 2 million worldwide by 2015 (ISC2: www.isc2.org/uploadedFiles/Landing_Pages/NO_form/2011GISWS.pdf). The needs of small business aren't even considered in these the numbers. NCSA has signed an memorandum of understanding with the Department of Education and the National Institutes of Standards and Technology to lead the National Cybersecurity Education Council (NCEC), a public-private partnership, to collaborate with the National Initiative on Cybersecurity Education, led by NIST, to address cybersecurity education issues at all levels including basic cybersecurity education, the development of the professional cybersecurity workforce and workforce training. Our aim is to build a consensus around the path forward from a large and diverse stakeholder group that can also help with implementation.

- **Highlight and leverage existing resources.** There are many good resources available for small businesses on cyber security such as the U. S. Chamber of Commerce's Internet Essential for Small Business (http://www.uschamber.com/issues/technology/internet-security-essentials-business) and the FCC's new online small business cyber planner (http://www.fcc.gov/cyberplanner) to name just a couple. Industry, including software and hardware manufacturers and Internet Service Providers, have a wealth of information and resources. Getting the word out about materials that can help small businesses today is important.
- **Encourage members of congress to make information available to the small businesses in their district or to hold a cybersecurity for small business town hall.** NCSA believes that if members reached out to the private sector to provide content for the town halls that there would be many companies willing to participate in providing content.

Thank you again for the opportunity to testify on this critical issue. I look forward to your questions.