StaySafeOnline.org
National Cyber Security Alliance

August 1, 2011
Department of Commerce
International Trade Administration
Office of the Secretary
National Institute of Standards and Technology
National Telecommunications and Information Administration
Internet Policy Task Force
SecurityGreenPaper@nist.gov
Bureau Drive, Mail Stop 893, Gaithersburg, MD 20819

RE: Comments on Department of Commerce Cybersecurity Green Paper: *Cybersecurity, Innovation, and the Internet Economy*
Docket No. 110527305-1303-02

Michael Kaiser
Executive Director
Michael@staysafeonline.org
202-570-7430
1010 Vermont Ave NW, Suite 821
Washington, D.C. 20005

Aimee Larsen Kirkpatrick
Communication & Outreach Director
aimee@staysafeonline.org
202-550-7431
1010 Vermont Ave NW, Suite 821
Washington, D.C. 20005

National Cyber Security Alliance (NCSA) submits these comments in response to the Department of Commerce's call for comment's on the report "Cybersecurity, Innovation and the Internet Economy," published in June 2011.

NCSA Background
Founded in 2001 the National Cyber Security Alliance ("NCSA") (www.staysafeonline.org) is a public/private partnership created to advance cybersecurity awareness and education for home users, businesses, and the formal education community (elementary education through college). As a partnership, NCSA works collaboratively with industry and government. The companies that currently comprise NCSA Board of Directors and financially support activities are: ADP, AT&T, Bank of America, Cisco, EMC, ESET, Facebook, General Dynamics Advanced Information Systems, Google, Intel, Lockheed Martin, McAfee, Microsoft, PayPal, SAIC, Symantec, Verizon and VISA. NCSA's mission is to educate and empower a digital society to use the Internet safely and securely at home, work, and school, protecting the technology individuals' use, the networks they connect to, and our shared digital assets.

National Cybersecurity Awareness Month
National Cybersecurity Awareness Month has been held since 2003 each October in the United States and is a multi-faceted effort to disseminate security messages and information through grassroots, traditional and social media channels. NSCA partners on awareness activities for this campaign with the U. S Department of Homeland Security and the Multi-

State Information and Sharing and Analysis Center (www.msisac.org). In 2010, NCSA's efforts alone (not including partner activities) reached an estimated 175,000,000 people through media and other activities. More than 180 companies, organizations and government agencies endorsed the month.

STOP. THINK. CONNECT.
In 2009 NCSA in collaboration with the Anti-Phishing Working Group (www.APWG.org), initiated an effort to develop a uniform safety and security message across industry and government. Many companies, government entities, and NGOs in the United States had taken up the cause of cybersecurity awareness and online safety. While these efforts were all well intentioned, there was not one message or set of tips and advice that computer users could use to guide behavior online and learn to protect the technology.

Following the model of other successful public messaging campaigns that led to broad scale cultural adoption of safety messages in the United States, such as those around forest fires and seat belts, NCSA and APWG convened a group of over 20 companies and seven federal agencies to explore the creation and dissemination of a unified message.

By unifying and sharing a message that campaign can be accelerated by the reach of the participating companies and agencies as trusted networks for message dissemination. Working together for a little over a year, the group:

- Conducted research about consumers knowledge and practices to keep themselves and family safe and secure online, their major issues of concern and messages that resonate;
- Selected STOP. THINK. CONNECT. as the message;
- Created a website for the campaign www.stopthinkconnect.org;
- Began implementation of the message for their own audiences and supported a national campaign as well; and
- Formed a new entity to hold and protect the intellectual property.

Founding members of the STOP. THINK. CONNECT. Messaging Convention include: ADP, AT&T, Costco, ESET, Experian, Facebook, Good Research, Google, Intuit, Intel, McAfee, Inc., Microsoft, PayPal, RSA The Security Division of EMC, Science Applications International Corporation, Sallie Mae, Symantec, TrendMicro, VeriSign, Verizon, Visa, Walmart, Webroot and Yahoo! Participating federal agencies include: the Department of Homeland Security, The Internal Revenue Service, The Department of Justice, the Social Security Administration, and the Federal Trade Commission.

Many of the participants in the private and public sectors have expressed interest in expanding the campaign globally and translation of some materials is already underway.

Comments

III. Facing the Challenges of Cybersecurity: Developing Policy Recommendations for the Future.

   a. *Creating a nationally recognized approach to minimize vulnerabilities for the I3S*
      1. *Developing and Promoting I3S-Specific Voluntary Codes of Conduct*

- *Are there existing overarching security principles on which to base codes of conduct?*

The STOP. THINK. CONNECT. Messaging convention developed voluntary basic principles to guide consumer behavior around security (and privacy). The guidelines were developed based upon the consumer research and the best practices put forth by industry, government and academia in a consensus-based fashion. Members of the STOP. THINK. CONNECT. Messaging Convention have asked that we begin looking at how to develop this campaign and modify/expand the principles for small and medium business. The principles are:

Keep a Clean Machine.

- Keep security software current: Having the latest security software, web browser, and operating system are the best defenses against viruses, malware, and other online threats.
- Automate software updates: Many software programs will automatically connect and update to defend against known risks. Turn on automatic updates if that's an available option.
- Protect all devices that connect to the Internet: Along with computers, smart phones, gaming systems, and other web-enabled devices also need protection from viruses and malware.
- Plug & scan: "USBs" and other external devices can be infected by viruses and malware. Use your security software to scan them.

Tip: Protect Your Personal Information.

- Secure your accounts: Ask for protection beyond passwords. Many account providers now offer additional ways for you to verify who you are before you conduct business on that site.
- Make passwords long and strong: Combine capital and lowercase letters with numbers and symbols to create a more secure password.
- Unique account, unique password: Separate passwords for every account helps to thwart cybercriminals.
- Write it down and keep it safe: Everyone can forget a password. Keep a list that's stored in a safe, secure place away from your computer.
- Own your online presence: When available, set the privacy and security settings on websites to your comfort level for information sharing. It's ok to limit who you share information with.

Connect with Care.

- When in doubt, throw it out: Links in email, tweets, posts, and online advertising are often the way cybercriminals compromise your computer. If it looks suspicious, even if you know the source, it's best to delete or if appropriate, mark as junk email.
- Get savvy about Wi-Fi hotspots: Limit the type of business you conduct and adjust the security settings on your device to limit who can access your machine.
- Protect your $$: When banking and shopping, check to be sure the sites is security enabled. Look for web addresses with "https://" or "shttp://", which means the site takes extra measures to help secure your information. "Http://" is not secure.

Be Web Wise.

- Stay current. Keep pace with new ways to stay safe online. Check trusted websites for the latest information, and share with friends, family, and colleagues and encourage them to be web wise.

- Think before you act: Be wary of communications that implores you to act immediately, offers something that sounds too good to be true, or asks for personal information.
- Back it up: Protect your valuable work, music, photos, and other digital information by making an electronic copy and storing it safely.

Be a Good Online Citizen.

- Safer for me more secure for all: What you do online has the potential to affect everyone – at home, at work and around the world. Practicing good online habits benefits the global digital community.
- Post only about others as you have them post about you.

  Help the authorities fight cyber crime: Report stolen finances or identities and other cybercrime to www.ic3.gov (Internet Crime Complaint Center), the Federal Trade Commission at http://www.onguardonline.gov/file-complaint.aspx (if it's fraud), and to your local law enforcement or state attorney general as appropriate

- *What is the best way to solicit and incorporate the views of small and medium businesses into the process to develop codes?*

NCSA research indicates that nearly 60% of small businesses report dependence on the Internet, using it to store customer data (65%), financial record and reports (43%) and to process and store credit card information (33%), personal information (30%), employee data (28%) and intellectual property (22%) (2010 NCSA/Visa Inc. Small Business Study: http://www.staysafeonline.org/sites/default/files/resource_documents/2010_Full_Small_Business_Study_FINAL11%2023.pdf). According to the U. S Census ecommerce has risen steadily from less than 1% of the total retail sales in 2001 to nearly 4.5% by the end of 2010 (U.S. Census Bureau News, Quarterly Ecommerce Sales, 4th Quarter 2010: http://www.census.gov/retail/mrts/www/data/pdf/ec_current.pdf). Employers of all sizes will need their employees, from intern to CEO, to be cybersecurity capable as part of the normal course of business.

Research similar to that done for the STOP. THINK. CONNECT. campaign to understand how to best influence behavior change amongst consumers (see below) should be done for small and medium size businesses. To best serve and reach businesses we need to understand where they place the importance of cybersecurity in relation to other issues in running their business, what their attitudes about cybersecurity in general are, the barriers to success, what types of messages would influence them, where they are most likely to turn for information (government, business or trade associations, non-profits, software providers, etc.) and the types of materials and resources that are most useful for them.

- *What is the best way to solicit and incorporate the views of the consumer and civil society?*

The STOP. THINK. CONNECT. Messaging Convention did extensive market research into the attitudes and beliefs of consumers to understand what types of words, messages and ideas would resonate with them and drive them to take action. The research showed that Americans need to hear a positive message that is empowering and action oriented. Some findings from the research (http://www.stopthinkconnect.org/researchSurvey.html):

- 96 percent of Americans feel a personal responsibility to be safer and more secure online.
- 93 percent believe their online actions can protect not only friends and family but also help to make the Web safer for everyone around the world.
- 61 percent believe that much of online safety and security falls under their personal control, and consistent with those feelings, 90 percent said they want to learn more about keeping safer on the Internet.
- 48 percent feel their actions to stay safe and secure can have a positive impact on financial, economic, and national security of the country, indicating Americans are open to making the bridge between their own safety and the nation's security.
- Concern about identity theft rates slightly higher than fears of job and healthcare loss. 54 percent of Americans are extremely concerned about loss of personal or financial information. To place this is in context, 53 percent are concerned about losing their jobs, while 51 percent feared not being able to provide healthcare for their family.
- Nearly two-thirds of the American public have heard, read or seen something about online safety and security issues recently. However, most of what the news they remember is negative: identity theft, privacy loss, and increased frequency of attacks.
- When asked why they don't always do all the things they can or should do to stay safer online, Americans said they simply lacked the information or knowledge (28 percent) – a surprising finding that surpassed other hurdles often cited by the media. Only 12 percent said online safety was too expensive, while just 5 percent said they were too busy to take the extra step.

More of this type of research should be done as technology, messages and threats evolve to understand where consumers are at in their understanding of the issues and the importance they place on cybersecurity in relation to other issues; whether or not they are taking action; and what types of messages, resources and education materials are appealing and useful.

2. *Promoting Existing Keystone Standards and Practices*
    - *What process should the Department of Commerce use to work with industry and other stakeholders to identify best practices, guidelines, and standards in the future?*
    - *Should efforts be taken to better promote and/or support the adoption of these standards, practices, and guidelines?*
    - *In what way should these standards, practices, and guidelines be promoted and through what mechanisms?*
    - *Should the government play an active role in promoting these standards, practices, and guidelines? If so, in which areas should the government play more of a leading role? What should this role be?*

3. *Facilitating Information Sharing and Other Public/Private Partnerships in the I3S to Improve Cybersecurity*
    - *What role can the Department of Commerce play in promoting public-private partnerships?*
    - *How can public-private partnerships be used to foster better incentives within the I3S?*
    - *How can existing public-private partnerships be improved?*

- *What are the barriers to information sharing between the I3S and government agencies with cybersecurity authorities and among I3S entities? How can they be overcome?*

Public private partnership to develop enforceable codes of conduct that are developed by a broad multi-stakeholder process are the mechanism through which government can effectively work with industry and other stakeholders to identify best practices, guidelines and standards. The NCSA serves as the premier organization for government to work with industry in public-partnership to address cybersecurity education and awareness. The STOP. THINK. CONNECT. Messaging Convention, led by NCSA and the APWG is an excellent example of the type of public-private partnership NCSA is able to build to foster consensus-based and constructive engagement to address security and privacy issues.

NCSA leads, in partnership with the APWG, the STOP. THINK. CONNECT. Messaging Convention and is the public-private partnership through which the National Initiative for Cybersecurity Education (NICE) has engaged for the National Cyber Security Awareness campaign, as called for in the President's 2009 Cyber Space Policy review. STOP. THINK. CONNECT. is the National Campaign for cybersecurity awareness and is the mechanism through which consumers are reached with a branded, action-oriented message for how to be safe and secure online. The STOP. THINK. CONNECT. Messaging Convention has more than 30 companies, organizations and government agencies (ADP, AT&T, Costco Wholesale Corporation, ESET, Experian, Facebook, Good Research, Google Inc., Intuit Inc., Intel Corporation, Lockheed Martin Information Systems and Global Services, McAfee Inc., Microsoft Corporation, PayPal, RSA, The Security Division of EMC, Science Applications International Corporation (SAIC), Symantec Corporation, TrendMicro Inc., VeriSign Inc., Verizon Communications Inc., Visa Inc., Walmart Stores Inc., Webroot Software, Inc. and Yahoo! Inc., FTC, IRS, SSA, DHS, FBI, Department of Commerce, NIST, InfraGard, D.A.R.E. America, MS-ISAC, Public Safety Canada, Securing Our eCity) that participate on a regular basis and provide oversight for the campaign and serve as part of the distribution mechanism, for the campaign providing tremendous reach and bandwidth to reach consumers. The campaign needs continued support and investment from both industry and government. The role of government should be to adopt the campaign across all agencies, invest in the creation and distribution of campaign materials and to make a long-term commitment to work in partnership with industry and other via the STOP. THINK. CONNECT. Messaging Convention to shape and guide the campaign to bring about a cultural consciousness of cybersecurity.

National Cyber Security Awareness Month is another long-established campaign through which the Department of Commerce can engage in promoting best practices, standards and guidelines for consumers and small and medium business. Founded by the NCSA as a way for industry and government to engage together in an awareness campaign, National Cyber Security Awareness Month has gained brand recognition among business and government agencies (local, state, federal and internationally) as a time during the year in which to come together to educate business, the public and others about the importance of cybersecurity. The NCSA continues to lead National Cyber Security Awareness Month in partnership with DHS and the Multi-State Information Sharing and Analysis Center. This month-long campaign also serves as period for which we can take stock of our progress and set goals for the future. In 2011 NCSA reached an estimated 175 million people through media impressions, had more than 180 companies formally endorse National Cyber Security

Awareness Month and launched with STOP. THINK. CONNECT. campaign in partnership with APWG, DHS and the White House, including a proclamation by President Obama declaring STOP. THINK. CONNECT. as the national message for cybersecurity education and awareness

c. *Education and Research*
   2. *Creating and Measuring I3S Cybersecurity Education Efforts*
      - *What new or increased efforts should the Department of Commerce undertake to facilitate cybersecurity education?*
      - *What are the specific areas on which education and research should focus?*

The Department of Commerce should look to support existing efforts that are looking to address cybersecurity education. In addition to the STOP. THINK. CONNECT. campaign being the effort through which the need for education can raised and basic awareness education delivered, The National Cyber Security Alliance has also responded to the call from the National Initiative for Cyber Security Education (NICE) to form a public private partnership to address formal cybersecurity education (NICE Component Area 2).

Over the past year NCSA has developed an impressive stakeholder group who have agreed to work together, as a public private partnership, to make recommendations to government, industry, foundations and others, about how to best invest in cybersecurity education (whether existing or new programs) so that resources are leveraged to their fullest potential, strategies for how to achieve those recommendations so that we are intentionally developing a cybercapable (those able to use technology safely, securely, responsibly and productively) workforce, starting with primary education, and also supporting the development of a professional cybersecurity workforce through the identification of career pathways and support of the necessary foundational education necessary for success in pursuing cybersecurity jobs. This coalition is comprised of a diverse group of industry, government, education and nonprofit stakeholders working together to find national solutions to cybersecurity education issues. Stakeholders include the NCSA board of director companies (ADP, AT&T, Bank of America, Cisco, EMC, ESET, Facebook, General Dynamics Advanced Information Systems, Google, Intel, Lockheed Martin, McAfee, Microsoft, PayPal, SAIC, Symantec, Verizon and VISA), IBM, Air Patrol, Oracle, Northrup Grunman, Capitol One, MS-ISAC, US Cyber Challenge, SANS Institute, Exxon Mobile, CoSN, ACM, NDIA, AIA, EDUCAUSE, iKeepSafe, Carnegie Mellon University, APWG, FOSI, ISC (2), Bay Area Council, CompTIA, WebWise Kids, Future of Privacy Forum, NSF, DOJ, NIST, Dept. of Ed, DHS, FTC, DOD, DNI and many others.

To support the creation of a cybercapable workforce, we must ensure that every young person receives the basic knowledge needed to use technology safely, securely, responsibly and productively. *The 2011 State of K-12 Cyberethics, Cybersafety and Cybersecurity Curriculum in the United States* (http://www.staysafeonline.org/sites/default/files/resource_documents/2011%20National%20K-12%20Study%20Final_0.pdf), an annual survey produced by NCSA and Microsoft, looks at the perceptions and practices of U.S. teachers, school administrators and technology coordinators in regards to cyberethics, cybersafety and cybersecurity education in the nation's K-12 schools. The study, conducted since 2008, continually finds this type of education lacking, despite the agreement between teachers, administrators and technology coordinators that it should be taught. Teachers are not prepared to teach the topics – 86 % if teachers reported receiving less than 6 hours of training on any cybersecurity, cybersafety or cyberethics topic and 36% received zero hours of training in the 12 months prior to the study – yet nearly all administrators surveyed (97%) agree schools should teach curriculum throughout K-12 that prepares young people to enter the workforce as cyber capable employees.

To support the creation of a strong cybersecurity workforce an area of focus must be on preparing young people to pursue careers in cybersecurity. This means ensuring that students are aware of cybersecurity career options and have the necessary foundational education in Science Technology Engineering and Math (STEM) and Computer Science in K-12 to successfully enter and finish university or technical programs. Computer science education should include cybersecurity as a key component. Other non-traditional programs also need to be supported, for example: cybersecurity challenges (such as the U.S. Cyber Challenge, the Maryland Cybersecurity Challenge, San Diego's Mayor's Cyber Cup and the Air Force Association US Cyber Patriot Challenge), math and computer science camps, and Girl Scout and Boy Scout STEM and career programs.

According to the study, 68% of administrators believe their schools or school districts are doing an adequate job of preparing students to pursue college-level (two- or four-year) education in cybersecurity. Yet research tells a different story. According to the 2001 Organisation for Economic and Co-operative Development (OECD) rankings of math and science performance of 15 year-olds in the 30 OECD countries, the United States ranks 25th in math and 17th in science (OECD Programme for International Student Assessment: Strong Performers and Succesfull Reformers in Education, Lessons from PISA for the United States: http://www.oecd.org/dataoecd/32/50/46623978.pdf. A recent New York Times article states that, according to the Community College Research Center at Teachers College at Columbia University, about 65 percent of all community college students nationwide need some form of remedial education, with students' shortcomings in math outnumbering those in reading by 2 to 1 (New York Times, *CUNY Adjusts Amid Tide of Remedial Students:* www.nytimes.com/2011/03/04/nyregion/04remedial.html).

In a report from the Computer Science Teachers Association (http://csta.acm.org/Research/sub/Projects/ResearchFiles/StateofCSEDHighSchool.pdf) indicates that despite our need for more technical experts in our society basic and advanced high school course work is shrinking. The study found that in 2005, 78% of responding institutions offered what they described as a pre-AP course; only 40% offered an AP Computer Science course. The 2007 data, however, show an alarming drop in the availability of computer science courses at both these levels, with 73% of respondents indicating that their school offered a pre-AP Computer Science course and

32% of respondents indicating that their school offered an AP Computer Science course (an overall decrease of 8% in the two years between surveys).

Furthermore we are failing to produce adequate numbers of graduates with science and engineering degrees. The National Science Foundation (NSF) Science and Engineering Indicators 2008 report (http://www.nsf.gov/statistics/seind08/c2/c2s5.htm) indicates that only about a third of all the bachelor's degrees earned in this country are S&E, with only 5% in engineering and 12% in natural sciences (physical, biological, computer, and agricultural sciences, and mathematics). Other countries are far-outpacing the United States with more than half of first degrees in S&E (Japan 63 %, China 56%, Singapore 59%, Thailand 69%) and across Asia 20% of first degrees are in engineering.

We face the challenge of achieving something multi-disciplinary in nature that requires cooperation from a broad range of stakeholders to be successful. Even at these early stages agencies, groups and institutions have staked out claims to various elements of the solution or focused solutions on a narrow definition of the problem.

Higher education (2 yr, 4 yr, graduate) must lead to skills and competencies that meet the hiring requirements of government and industry to fill the growing need for cybersecurity professionals. The Bureau of Labor Statistics estimated there will be 295,000 new IT jobs between 2008 and 2018, many of which will require cybersecurity expertise. (http://www.bls.gov/oco/pdf/ocos303.pdf)

To address the current workforce and support the developing workforce, a system of in-service training is needed to maintain a skilled workforce in the face of an ever-changing threatscape and continuously evolving technology.