To: The Department of Commerce Internet Policy Task Force
From: The Coalition Against Unsolicited Commercial Email (CAUCE)
Date: August 1st, 2011
Subject: CAUCE Comments on "Cybersecurity, Innovation and the Internet Economy" http://www.nist.gov/itl/upload/Cybersecurity_Green-Paper_FinalVersion.pdf

Thank you for the opportunity to comment on your recent green paper.

Who We Are:

CAUCE North America, an all-volunteer consumer advocacy organization former in March 2007, has moved beyond its original mission of encouraging the creation and adoption of anti-spam laws to a broader stance of defending the interests of the average Internet user. CAUCE NA is led by a combined Board with a cumulative century of experience in the field of Internet advocacy.

Our Position On The Department of Commerce Green Paper:

Given our focus on defending the interests of the average Internet user, we appreciate any attempt to improve cybersecurity. However, after reading your green paper, we're left wondering:

Will the work you propose to undertake actually improve the cybersecurity of small businessmen and businesswomen -- the entrepreneurs who have historically created and driven the "Internet Economy"? And if so, how soon, and how?

While the Department might naturally be most concerned about helping improve the cybersecurity of large American corporations, we worry that sole proprietorships and small partnerships may be overlooked.

Many of those sole proprietorships and small partnerships are precisely the sort of average Internet users CAUCE is meant to represent, and which we hope are also important to the Department of Commerce.

Page 3 of the green paper states "*Where sectors (such as those with a large number of small businesses) lack the capacity to establish their own voluntary codes of conduct, new and existing National Institute of Standards Technology (NIST) guidelines would be available to bridge gaps in security protection.*"

Except for that one reference to small businesses, the green paper is silent on that important economic sector.

As noted by the Small Business Administration,[1] small firms:

- Represent 99.7 percent of all employer firms.
- Employ half of all private sector employees.
- Pay 44 percent of total U.S. private payroll.
- Generated 65 percent of net new jobs over the past 17 years.
- Create more than half of the nonfarm private GDP.
- Hire 43 percent of high tech workers (scientists, engineers, computer programmers, and others).
- Are 52 percent home-based and 2 percent franchises.
- Made up 97.5 percent of all identified exporters and produced 31 percent of export value in FY 2008.
- Produce 13 times more patents per employee than large patenting firms.

It was those sort of entrepreneurs -- American small businessmen and businesswomen -- who created many of

[1] http://web.sba.gov/faqs/faqIndexAll.cfm?areaid=24

today's Internet giants, and whom we will likely be looking to in the future to create our next Apple or Facebook or Google.

So why does this large and important sector merit only one reference in your entire green paper?

We think you may have accidentally overlooked this critical group.

Small businesses should be an integral part of your investigations and your planning moving forward.

We also ask you to look hard at your timeline for executing the work you have planned. If you will be helping small businessmen and small businesswomen improve their cyber security, when will that happen? Small businesses can't wait decades or even years for the help they really needed yesterday.

We will also say that small businesses don't want NIST *guidelines* imposed upon them, small businesses already have more than enough paperwork and compliance requirements to try to meet.

What small businesses want and need are real usable technical cyber security solutions that will help to keep them -- and their customers -- safe online.

Will your program of work result in the creation of those products and services, and at a price that small businesses can afford to purchase?

Frankly, based on what we currently see, we're skeptical. We hope you can reassure us moving forward.

One concrete opportunity for the Department to consider would be to work to advance cyber security for small businesses via creation of a Small Business Innovation Research (SBIR)[2] program dedicated to the short-term commercialization of cyber security research into market-ready products *for* small businesses, *by* small businesses. If the Department of Commerce doesn't have the existing research base to drive a traditional SBIR process, it should consider partnering and helping to fund such a program with a more traditional research funding agency such as the NSF, NIH, or Department of Energy.

In providing this response, we hope you will forgive us for being blunt. We don't have time to be coy. Small businessmen and businesswomen are "floundering" in "rough cybersecurity seas," and we need to yell loudly for help on their behalf if the true core of America's business sector is to have any hope of not going under once and for all, swamped by relentless cyber attacks.

Thank you for considering these comments, and as always, we'd be happy to elaborate on our position further if you have any questions. Please don't hesitate to get in touch.

Sincerely,

Neil Schwartzman, Executive Director
CAUCE North America
Email: neil@cauce.org

[2] http://www.sbir.gov/index.html