April 29, 2013

VIA EMAIL - cyberincentives@nist.doc.gov

Mr. Alfred Lee
Office of Policy Analysis and Development
National Telecommunications and Information Administration
U.S. Department of Commerce
1401 Constitution Avenue, NW, Room 4725
Washington, D.C. 20230

Re: Incentives to Adopt Improved Cybersecurity Practices

Dear Mr. Lee:

BSA | The Software Alliance (BSA) appreciates this opportunity to provide comments to the National Telecommunications and Information Administration (NTIA) on the potential benefits and relative effectiveness of incentives for encouraging participation in developing the Critical Infrastructure Cybersecurity Program (the Program). BSA is the leading advocate for the global software industry before governments and in the international marketplace.[1] It is an association of world-class companies that invest billions of dollars annually to create software solutions that spark the economy and improve modern life.

BSA has long worked to support improved cybersecurity and continued innovation. This work has been driven by two fundamental principles: First, cyberspace is global, and no single country or company can succeed alone—all must work together. Second, the networked world is diverse and dynamic. No one-size solution will ever fit all, either at a static moment in time or as threats, vulnerabilities, consequences, or probabilities inevitably change.

These core principles also are at the heart of BSA's response to the Department of Commerce's July 2010 Notice of Inquiry that examined, in part, questions around incentives for noncritical infrastructure.[2] As BSA noted then:

[1] *BSA | The Software Alliance (www.bsa.org) is the leading global advocate for the software industry. It is an association of world-class companies that invest billions of dollars annually to create software solutions that spark the economy and improve modern life. Through international government relations, intellectual property enforcement and educational activities, BSA expands the horizons of the digital world and builds trust and confidence in the new technologies driving it forward.*

BSA's members include: Adobe, Apple, Autodesk, Bentley Systems, CA Technologies, CNC/Mastercam, Dell, IBM, Intel, Intuit, McAfee, Microsoft, Minitab, Oracle, PTC, Rosetta Stone, Siemens PLM, Symantec, and The MathWorks.

[2] Available at http://www.nist.gov/itl/upload/BSA-Comments-9-20-10.pdf

Robert W. Holleyman, II
President and CEO

20 F Street, NW, Suite 800
Washington, DC 20001

P 202-872-5500
W bsa.org

> Every business has strong incentives to protect its high value assets and those of its customers. This includes the value of its brand, and supply chains. These incentives are affected by the particular product or service they offer, geographic markets, competition, innovation, regulatory structure, and other incentives. There is no single answer to a question on incentives.

This remains equally true today. Accordingly, BSA believes the most suitable way to assess and implement appropriate incentives for encouraging participation in the Program will vary based on the sector in question.

At the same time, NTIA should examine efforts and incentives that cut across multiple sectors. For example, the best incentive for driving participation in any voluntary program likely would involve finding ways to reduce or offset the costs of participation.

For example, BSA believes that liability limitations can be a very effective tool to promote increased cybersecurity without requiring the expenditures of scarce fiscal resources. Importantly, liability limitations are a sliding scale of measures: Without granting a complete safe harbor from any and all liability, the threat of certain types of liability can be reduced or removed without affecting others (*e.g.*, punitive damages, actual damages, compensatory damages, economic or non-economic damages). This also can be accomplished by raising the burden of proof that rests on a plaintiff (*e.g.*, preponderance of the evidence vs. clear and convincing evidence).

Furthermore, NTIA should consider finding ways to restrict standing to bring suit to certain parties (*e.g.*, by clarifying that only law enforcement agencies such as the Federal Trade Commission or State Attorneys General can bring suit, rather than private parties). Finally, NTIA should consider whether an incentive would be to pre-empt state laws in favor of a unified federal liability regime, where appropriate.

Changing the liability scheme under which companies participating in the voluntary framework operate is just one example of how to offset the costs for investing in greater cybersecurity. BSA believes that individual sectors will have additional suggestions, and we encourage the Administration to consider them seriously.

BSA commends NTIA on its ongoing efforts to shape the Program and urges continued outreach to the private sector through all available means. BSA looks forward to continuing to work with NTIA on this critical endeavor.

Sincerely,

Robert Holleyman

Robert W. Holleyman, II
President and CEO

20 F Street, NW, Suite 800
Washington, DC 20001

P 202-872-5500
W bsa.org