October 10, 2014

Via cyberframework@nist.gov

Ms. Diane Honeycutt
Secretary
Computer Security Division
National Institute of Standards and Technology
100 Bureau Drive, Stop 8930
Gaithersburg, MD 20899

Dear Ms. Honeycutt:

The Internet Commerce Coalition ("ICC") appreciates the opportunity to respond to the National Institute of Standards and Technology ("NIST") RFI on the level of awareness and initial experiences with the Framework for Improving Critical Infrastructure Cybersecurity (the "Framework"). The ICC is comprised of leading Internet and e-commerce companies and trade associations. We work to promote balanced, reasonable and workable rules and standards governing liability, privacy and security relating to the Internet.

Our Coalition has supported NIST's efforts to develop voluntary cybersecurity guidelines pursuant to Executive Order 13636, "Improving Critical Infrastructure Cybersecurity" drawing on the extensive public and private input during the year long and open process culminating in release of the Framework on February 12, 2014. There is broad awareness of the Framework throughout our Coalition, and a number of member companies are using or are exploring how to use it as a resource to assist them in managing cyber risks they face. ICC members have found the voluntary and flexible nature of the Framework to be of great utility in supplementing existing cybersecurity practices and in communicating with third parties.

By giving companies the discretion and leeway to draw upon and adapt those elements that are best-suited for their particular organizational structure and business operations, NIST's approach is fostering broader and more constructive usage of the Framework. Further, by providing industry with a common frame of reference, the Framework may prove to be particularly useful in facilitating discussions regarding best practices and new risk management tools and techniques both within and across the various elements of the Internet ecosystem.

Additionally, the process oriented approach of the Framework, and the Methodology to Protect Privacy and Civil Liberties (the "Privacy Methodology") in particular, accommodates utilization of privacy practices across diverse sectors using a range of technical implementations and allowing for ongoing innovation. For example, the Framework and the Privacy Methodology have allowed ICC member companies to continue using the extremely successful formula of "privacy by design" in the development and improvement of new products and services and beneficial uses of data.

500 8th Street N.W., Washington, D.C. 20004
tel: 202.799.4000 fax: 202.799.5000

The Privacy Methodology has been a helpful resource for companies in reviewing the manner in which they satisfy their existing privacy obligations in the context of their organization's cyber defense practices and protocols.

The flexibility of the process oriented approach to privacy reflected in the Privacy Methodology is critical to encouraging use of the Framework. The privacy practices of ICC member companies are already subject to a variety of statutory frameworks and agency oversight and enforcement activities. Any movement beyond the Privacy Methodology set forth in Version 1.0 runs the risk of layering an additional and unnecessary set of privacy obligations on top of the existing frameworks that our members already adhere to, thereby imposing more complexity, cost and compliance burdens, with little incremental improvement to privacy or cybersecurity. NIST should continue to offer companies the breathing room to tailor the Framework to their particular business practices and legal and regulatory frameworks, and refrain from moving toward a new privacy methodology that might inhibit use of the Framework and undermine its flexible and voluntary nature.

The ICC supports the risk-based approach of the Framework. The U.S. technology industry has long coalesced around the use of risk-based frameworks, such as ISO 27001, for preparing and adapting to security risks. The Framework's strong risk-based focus has benefited U.S. critical infrastructure sectors in the same way and should now be applied to the U.S. government itself, which still relies on government security compliance processes focused on exhaustive checklists and audits.

The ICC is concerned that NIST's draft Privacy Engineering Objectives and Risk Model, rather than following the successful process of the Framework involving the integration of consensus-based guidelines and industry standards in furtherance of established public policy goals, is deviating from this proven approach and addressing remote and questionable privacy harms. If NIST continues to focus its privacy engineering initiative on ill-defined harms and objectives that are not tied to established public policy, the ICC is concerned that it will create uncertainty that discourages further positive developments under the guidance of the Privacy Methodology and hinder innovation of new products and services. Instead we urge NIST to focus on existing, proven best-practices used to protect the privacy of individuals, drawing especially from industry sectors with existing legal privacy paradigms, in order to create a tool that is instructive for organizations seeking to improve privacy engineering.

Respectfully submitted,

Jim Halpert, General Counsel

EAST\83814281. 12

500 8th Street N.W., Washington, D.C. 20004
tel: 202.799.4000 fax: 202.799.5000