

<p>S. Joe Bhatia President and CEO American National Standards Institute</p>	<p>InterCEP Roundtable Introductory Remarks <i>Identifying what works and doesn't work in public-private collaboration: structures and strategic for partnering on information, resources, and joint action</i> June 16, 2010 – New York, NY</p>
---	--

Good afternoon, everyone.

My name is Joe Bhatia, and I am the president and CEO of the American National Standards Institute, often referred to as ANSI. I am pleased to be here today to discuss how standards and conformity assessment activities developed in an open, consensus-based process can result in the strongest possible solutions for national priorities.

For those not familiar with us, ANSI is a private, non-profit organization that administers and coordinates the U.S. voluntary standards and conformity assessment system. This system was established more than a century ago to support manufacturing and mechanical processes. Today, there are as many different kinds of standards and accompanying compliance activities as there are different industries, products, and services. But no matter the subject matter, ANSI works in close collaboration with stakeholders from both industry and government to identify interoperable and consensus-based solutions that address national needs and global priorities.

It is important to note that ANSI does not develop standards. Rather, we oversee the creation, promulgation, and use of tens of thousands of standards, guidelines, and conformity assessment activities that directly impact businesses and consumers in nearly every industry. Through our diverse membership, ANSI represents the interests of more than 125,000 companies and 3.5 million professionals worldwide.

In ANSI's role as a neutral forum, the Institute has helped to forge the robust public-private partnerships that bring about effective standards-based solutions.

One recent example is cybersecurity. Some of you may have heard Karen Hughes, ANSI's director of homeland security standards, discuss the Institute's cyber activities in a roundtable discussion yesterday. Since 2008, we have been working in partnership with the Internet Security Alliance as project leaders on initiatives that assess and address the critical cybersecurity issues affecting organizations. Earlier this year that partnership resulted in the publication of *The Financial Management of Cyber Risk: An*

Implementation Framework for CFOs. Authored by more than sixty volunteer experts from government and industry, this document provides a terrific example of how the public and private sectors can work together to provide concrete solutions quickly and effectively.

In the May 2009 White House *Cyberspace Policy Review*, the President asked for a program that would help assign monetary value to cyber risks and consequences. This would give organizations greater ability and incentive to address cybersecurity, and in turn help protect our national security. Our publication responds directly to the President's request by examining cyber risk from a financial perspective. And ANSI's unique position as facilitator of public-private partnerships enabled us to bring together crucial knowledge and expertise from across industry sectors and government agencies. The result is a concrete, robust, and best of all, free action guide that can be implemented by all organizations, large and small.

Beyond cybersecurity, ANSI and our Federation of members are working in partnership on a wide range of current and emerging priorities. The ANSI Homeland Security Standards Panel works in partnership with the Department of Homeland Security to coordinate standardization needs that respond quickly and effectively to DHS priorities. ANSI and the Department of Commerce's National Institute of Standards and Technology (NIST) worked together to launch the Nuclear Energy Standards Coordination Collaboration, a cross-stakeholder forum that works to facilitate the timely identification, development, and revision of standards related to nuclear power plants. And the ANSI Identity Theft Prevention and Identity Management Standards Panel brings together the private sector, government, and consumers to help with the progress of standards solutions for minimizing the scope and scale of identity theft and fraud.

These are just a few of ANSI's areas of activity, and the challenges associated with each of these priorities are very different – but they all have one thing in common . . . the most robust solutions cannot be developed in a vacuum.

Our national standards system is based on collaboration, cooperation, and consensus building. Rather than mandating a “one-size fits all” solution, our system allows players to find the tools and solutions that best fit their needs – whether we are talking about regulatory issues or marketplace demands.

The growth of global business makes a cooperative system even more critical, particularly in regard to supply chain issues. Many manufacturing bases are moving into newly industrialized regions. But national authority ends at the border, and nations protective of their own sovereignty will not accept in-

country enforcement activities by other nations. Destination countries cannot use their enforcement agencies to follow the supply trail back to countries of origin, and very few imports are inspected.

But by relying upon private sector-led standards and conformity assessment programs that can cross borders, the entire global supply chain sees increased quality and safety. That spells benefits for industry, for government, and for consumers.

Within our own borders, legislators often need a neutral source of information on standards and conformance activities. Additionally, government agencies use standards both directly and indirectly in their work: in regulations and laws, in procurement, and in internal operations.

ANSI's role in this process is as an information provider, bridging the gap between standards developers and the governmental agencies that create legislation.

In addition, ANSI monitors legislative activity to determine whether standards and conformance-based solutions exist or may overlap where legislation is being considered. And where we see that new or revised standards are needed, we can focus the attention of the standardization community and facilitate cross-sector partnerships.

Private sector-led solutions can offer tremendous advantages over traditional legislation. Developed by a collaborative group of stakeholders, voluntary consensus standards respond quickly, directly, and effectively to marketplace changes and technological advancement. Recognizing this, many legislators will mandate compliance to consensus-based standards rather than reinventing the wheel with a regulation.

Cybersecurity again provides the timeliest of examples, as federal legislators continue their efforts to create meaningful policies that will strengthen our nation's cyber infrastructure. As just one example, the Cyber Security Act of 2010, or the Rockefeller-Snowe bill, is intended to "address our nation's vulnerability to cybercrime, global cyber espionage, and cyber attacks." I am pleased to see that there are a number of aspects of the latest version of this bill that align with ANSI's cybersecurity activities.

- First, the bill creates a market-driven process that encourages businesses to adopt good cybersecurity practices and innovative security measures.

- And second, Rockefeller-Snowe encourages government agencies and private businesses to work together in partnership to protect our civil liberties, intellectual property rights, and classified information.

No matter the challenge, ANSI will continue to promote standards-based activities that capitalize on the collaboration of all stakeholder groups. I look forward to hearing all of your perspectives on how the public and private sectors can develop viable, effective solutions to address current and emerging issues. Together, we can identify the areas that require the greatest attention, assess what is working in other areas, capture those successes, and build upon them.

Thank you for your attention.

[END]