Karen Hughes Director, Homeland Security Standards American National Standards Institute	**Roundtable Remarks** ***Cyber Threats: Challenges and strategies*** June 15, 2010 – New York, NY

Good afternoon, everyone.

My name is Karen Hughes, and I am director of homeland security standards at the American National Standards Institute, also known as ANSI.

For those of you who are not familiar with ANSI, we are the coordinator of the U.S. private-sector led and public sector-supported voluntary consensus standards and conformity assessment system. We speak as the U.S. voice in standardization forums around the globe. And we offer a neutral forum where business, industry, government, and consumers can come together to address key national priorities. Cybersecurity is without a doubt up high on that list.

Since 2008, ANSI has been working in partnership with the Internet Security Alliance as project leaders on initiatives that investigate, asses, and address the increasingly vital cybersecurity issues affecting organizations. We distributed one successful cybersecurity-related publication in 2008, and earlier this year our continued partnership resulted in the publication of *The Financial Management of Cyber Risk: An Implementation Framework for CFOs.*

This new document provides organizations of every kind with a customizable action guide to help them bolster information security and reduce vulnerability to cyber attacks. And it is a terrific example of the public-private partnership at work in developing timely, concrete solutions.

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 would help protect our national security, which is dependent upon a robust and secure information infrastructure.

Our publication responds directly to the President's request by examining cyber risk from a financial perspective. Our efforts have been endorsed by Melissa Hathaway, former acting senior director for

cyberspace and author of the CSPR report. She described the publication as “an excellent guide for organizations to manage the risk and exposure derived from digital dependence.”

And while it was developed in partnership with many government stakeholders, the entire publication has been managed and funded by the private sector. By making this document freely available for download at no charge to organizations across the country, we are aiming for the broadest dissemination possible, so that a large number of organizations will read and implement the best practices it contains. We’ve presented the document at a meeting of legislative staffers on Capitol Hill, and publicized it extensively to business and industry through press events and news releases. The response has been enthusiastically positive, and so far, more than 3,000 downloads have been counted from our website, in addition to a printed distribution. The document is also reaching students at some of the nation’s leading universities. Melissa Hathaway has made the document required reading for her Kennedy School of Government students at Harvard University. And this fall, the document will be included in an MBA-level cybersecurity course at Loyola University.

In terms of content and development, *The Financial Management of Cyber Risk* was set up as an action guide to help businesses bolster their information security and reduce vulnerability to cyber attacks. But beyond just a framework of IT best practices, this document aims to solve a very serious misunderstanding in today’s business environment.

Many organizations think of cybersecurity as an IT problem. When companies take this approach, individual business units don’t feel accountability for their own data. This limits their own strategic abilities to analyze and communicate about data security, and marginalizes the problem.

But cyber risk is an enormous, financial, organization-wide problem. The CSPR report estimated American business losses due to cyber attacks at more than $1 trillion of intellectual property between 2008 and 2009. By examining the issue from a financial perspective, we are delivering a wake up call to executives nationwide. In other words, we’re telling them: this is a very serious issue, it’s costing you a lot of money, and it needs to be addressed all across your organization.

This enterprise-wide approach is one of the most critical components of this document. It’s not just IT . . . it’s HR, communications, legal, operations, and many more departments that need to get involved and have a hand in crafting a cybersecurity plan that meets the needs of each individual business. It defines the key players within an organization’s C-suite who need to partner to address critical questions. It poses

the questions that need to be asked – and provides recommended tools for the analysis – but does not dictate answers. Each organization will need to conduct its own analysis and make the decisions that are appropriate for that industry sector.

ANSI believes strongly that robust solutions cannot be developed in a vacuum. And that also applies to the approach we took in developing the document. ANSI and ISA gathered together an expansive and open network of more than sixty experts from industry, government, and academia. By engaging this broad group of stakeholders in a series of consensus-based document development workshops, we were able to create an efficient, effective, and scalable document that will work for all organizations, large and small.

ANSI believes firmly in the value of consensus-based problem solving in bringing together all the expert knowledge, perspectives, and resources needed to address cybersecurity. And we believe in the power – and the necessity – of the public-private partnership, where industry and government work together to develop solutions for all of our nation's key priorities.

I look forward to hearing other perspectives on these issues, and than you very much for your attention.

[END]