ANSI Response to Notice of Inquiry Regarding Cybersecurity, Innovation and the Internet Economy, dated July 28, 2010

The American National Standards Institute (ANSI) is pleased to provide this response to the NIST, ITA, NTIA Notice of Inquiry regarding Cybersecurity, Innovation and the Internet Economy dated July 28, 2010, Docket No.: 100721305–0305–01.

By way of introduction, ANSI serves as the coordinator of the United States' private-sector led and public-sector supported standardization system. The Institute oversees the creation, promulgation and use of tens of thousands of standards, norms, guidelines, and conformance activities that directly impact businesses and consumers in nearly every industry sector. ANSI and its members cooperate with government agencies at the federal, state and local levels to achieve optimum compatibility between government laws and regulations and the voluntary standards of industry and commerce, as well as ensuring that voluntary consensus standards provide for government needs in their procurement of goods and services.

ANSI is the official U.S. representative to the International Organization for Standardization (ISO) and, via the U.S. National Committee, the International Electrotechnical Commission (IEC). ANSI is also a member of the International Accreditation Forum (IAF) and a number of regional standards and conformity assessment bodies.

According to the White House *Cyberspace Policy Review*, between 2008 and 2009, American business losses due to cyber attacks had grown to more than $1 trillion of intellectual property. Members of the ANSI Federation have been working to provide standards and conformity assessment solutions to address cybersecurity issues as a national priority.

The Institute recently partnered with the Internet Security Alliance in the development of an action guide to assist business executives in the analysis, management, and transfer of financial risk related to cyber attack. *The Financial Management of Cyber Risk: An Implementation Framework for CFOs*[1] responds directly to the President's Cyberspace Policy Review which asked for a program that would help assign monetary value to cyber risks and consequences, giving organizations greater ability and incentive to address cybersecurity. A briefing and video presentation were made to Congressional members and staff.[2]

ANSI also has convened the Identity Theft Prevention and Identity Management Standards Panel (IDSP),[3] a cross-sector coordinating body working to identify standards, guidelines and best practices needed to combat identity crime which, over

---

[1] http://www.ansi.org/news_publications/news_story.aspx?menuid=7&articleid=2489

[2] http://www.ansi.org/news_publications/news_story.aspx?menuid=7&articleid=2513

[3] http://www.ansi.org/idsp

the last seven years, has affected 65 million Americans at a cost to U.S. consumers and businesses of close to $400 billion.[4]

In 2009 the IDSP released a workshop report calling for the development of an American National Standard on identity verification as a tool to help combat terrorism and identity theft.[5] The workshop and report were driven by recognized vulnerabilities in the issuance of foundational documents used to prove identity. As a result of this activity, the North American Security Products Organization, an ANSI-accredited standards developing organization, recently convened a consensus body to develop an American National Standard on this subject.[6]

Also in 2009 the IDSP released a report addressing how research companies measure identity theft, which included a review of relevant terminology, research studies and methodologies for studying the problem, as well as recommendations in each of these areas.[7]

In 2008, the IDSP released a comprehensive, two volume report, developed in partnership with the Better Business Bureau and more than 70 leading private and public sector organizations, to help arm businesses and other organizations with the tools and processes they need to prevent the theft of personal and financial information.[8]

In terms of conformity assessment activities, ANSI and the ANSI-ASQ National Accreditation Board (ANAB)/ACLASS brand have launched a formal pilot accreditation program based on the requirements of the ISA Security Compliance Institute (ISCI) *ISASecure*™ Embedded Device Security Assurance (EDSA) certification program. *ISA Secure* recognizes and promotes cyber-secure products and practices for industrial automation suppliers and operational sites. A new agreement between ISCI, ANSI, and ACLASS establishes ANSI/ACLASS as the Accreditation Body for organizations that provide product certifications in accordance with the *ISASecure* EDSA conformance scheme as well as ISO/IEC Guide 65, *General Requirements for Bodies Operating Product Certification Systems.*[9]

ANSI also has accredited personnel certification bodies that certify cybersecurity IT professionals. This was mandated by the Department of Defense (DOD Directive 8570.1 – Information Assurance Training, Certification, and Workforce Management) and is supported by the Department of Homeland Security. Ensuring the competencies

---

[4] https://www.javelinstrategy.com/news/831/92/Javelin-Study-Finds-Identity-Fraud-Reached-New-High-in-2009-but-Consumers-are-Fighting-Back/d,pressRoomDetail

[5] http://www.ansi.org/news_publications/news_story.aspx?menuid=7&articleid=2351

[6] http://www.ansi.org/news_publications/news_story.aspx?menuid=7&articleid=2597

[7] http://www.ansi.org/news_publications/news_story.aspx?menuid=7&articleid=2345

[8] http://www.ansi.org/news_publications/news_story.aspx?menuid=7&articleid=1723

[9] http://www.ansi.org/news_publications/news_story.aspx?menuid=7&articleid=2611

of cybersecurity professionals is important as issues relating to protecting information often are not with the software or systems but involve human error.

In sum, the Institute has considerable experience in this issue area. We would be pleased to facilitate efforts to bring together experts from the private and public sectors to address the need for standards and conformity assessment solutions as envisioned by the Department of Commerce in the notice of inquiry.

For further information on how we might be of service to your efforts, please contact Scott Cooper, VP of government affairs (scooper@ansi.org; 202-331-3610).

Thank you for the opportunity to comment.