ISACA®
Trust in, and value from, information systems

3701 Algonquin Road, Suite 1010
Rolling Meadows, Illinois 60008-3105, USA
Web Site: *www.isaca.org*

Telephone: +1.847.253.1545
Facsimile: +1.847.253.1443
E-mail: *info@isaca.org*

13 December 2013

Mr. Adam Sedgewick
National Institute of Standards and Technology
100 Bureau Drive, Stop 8930
Gaithersburg, MD 20899-8930

Re: Preliminary Cybersecurity Framework Comments

Dear Mr. Sedgewick,

Congratulations to NIST for the completion and release of the US Government's cybersecurity Preliminary Cybersecurity Framework. Following the issuance of the Presidential Policy Directive 21, Critical Infrastructure Security and Resilience; and Executive Order 13636 Improving Critical Infrastructure Cybersecurity—we recall the plans and goals of NIST To develop a framework focused on helping to reduce cyberrisks while also helping to align business, policy and technology risks. At the time, we believed this was the right focus and the goal was particularly insightful and NIST has delivered on its intended goals and that the framework will continue to expand the discussion around ensuring a proper focus on an effective cybersecurity approach, which is critical to the economy of the United States and all global economies.

Appendix C of the Framework, *Areas for Improvement for the Cybersecurity Framework* lays out eight considerations and ISACA agrees with all of the items in this appendix. We ask that NIST considers adding the issue of Governance of Cybersecurity efforts to the list of considerations. Although Governance is identified as one of Categories in the Framework Core, Appendix A, by mentioning it earlier in the Framework, it could serve to catch the proper attention of board directors and senior management.

The following are ISACA responses to the questions posed by NIST in the Preliminary Framework.

Is the Framework presented at the right level specificity?
Overall, yes, we believe the Framework, as presented provides enough detail to provide usage without getting overly prescriptive. At a high level, it provides the topics or considerations and some suggestions on how to approach the topic.

Does the Framework adequately define outcomes that will help to strengthen cybersecurity and support business objectives?
The framework does present the process by which organizations could evaluate defined outcomes –and help strengthen overall cybersecurity.

Is the Framework at a proper level that it will provide the tools necessary for senior management and boards of directors to understand the risks and mitigation appropriately?
Yes. However, it likely would enhance the document understanding and support by boards and senior management if aspects of the "Message to Senior Executives on the Cybersecurity Framework" were modified and added back to the document. This high-level synopsis could also be used on its own for communication about the Framework to these Key decision makers.

Will the Framework help provide the guidance and resources for businesses of all sizes, while maintaining flexibility?
The Preliminary Cybersecurity Framework is presented with risk as a main focal point. It also provides the steps an organization should consider along the way. Although there is no specific content in the Framework that calls out how a small or medium organization would approach implementation, the steps outlining things to consider are appropriate for all sized entities.

Will the Framework, as presented, be inclusive enough yet not disruptive to ongoing business, for effective cybersecurity practices?
Yes. The Preliminary Cybersecurity Framework is presented as a suggested approach to complement existing business and cybersecurity operations.

Is the Framework sufficiently clear on how the Privacy methodology is integrated into the Framework?
Appendix B, presents how Privacy could in integrated into the Preliminary Cybersecurity Framework. While the items presented are clear, they appear more detailed than needed for the purposes laid out by the Framework. We are sure other comments might address this issue as well as NIST's call out in Appendix C for further alignment with industry good practices.

….

Again, we appreciate the opportunity to respond and stand ready to provide additional assistance to ensure that NIST's efforts to support a safe, yet reliable and robust, cybersecurity focus for the United States are successful and lasting.

Respectfully submitted,

Thomas Lamm
Director – Professional Advocacy
ISACA (*www.isaca.org*

About ISACA

With more than 120,000 constituents in 180 countries (40,000 in the US), ISACA members have developed, implemented, managed and assessed security controls in leading critical infrastructure organizations and governments on a global basis. ISACA is a leading global provider of knowledge, certifications, community, advocacy and education on information and systems assurance and security, enterprise governance and management of IT, and IT-related risk and compliance. ISACA continually updates COBIT®, which helps IT professionals and enterprise leaders fulfill their governance and management of IT responsibilities, particularly in the areas of security, risk, assurance and control to deliver value to the enterprise. COBIT is used within many governmental departments and regulatory bodies around the world. ISACA also participates in the development of international security and governance standards through its global liaison status with the International Organization of Standardization (ISO).

Founded in 1969, the nonprofit, independent ISACA hosts international conferences, publishes the *ISACA® Journal*, and develops international IS auditing and control standards, which help its constituents ensure trust in, and value from, information systems. It also advances and attests IT skills and knowledge through the globally respected Certified Information Systems Auditor® (CISA®), Certified Information Security Manager® (CISM®), Certified in the Governance of Enterprise IT® (CGEIT®) and Certified in Risk and Information Systems Control™ (CRISC™) designations.