December 12, 2013

Information Technology Laboratory
ATTN: Adam Sedgewick
National Institute of Standards and Technology
100 Bureau Drive, Stop 8930
Gaithersburg, MD 20899-8930

Dear Mr. Sedgewick:

The American Institute of Certified Public Accountants (AICPA) is pleased to comment on the National Institutes of Standards and Technology's (NIST's) *Preliminary Cybersecurity Framework* (Preliminary Framework) pursuant to the President's Executive Order 13636 on Improving Critical Infrastructure Cybersecurity. With a 126-year heritage of serving the public interest, the AICPA is the world's largest association representing the accounting profession, with nearly 394,000 members in 128 countries. AICPA members represent many areas of practice, including business and industry, public practice, government, education, and consulting; membership is also available to accounting students and CPA candidates. The AICPA sets ethical standards for the profession and U.S. auditing standards for audits of private companies, nonprofit organizations, and federal, state, and local governments. The AICPA also develops and grades the Uniform CPA Examination.

Since the introduction of computers into the business environment the AICPA has provided technology related risk management thought leadership guidance to business ranging from Fortune 10 corporations to sole proprietors on Main Street. As trusted advisers to business, our members have obtained a unique perspective of the impact of technology and its threats on business viability and security. Our members have designed controls to help businesses manage these threats, and when a threat is realized, provide financial and technical guidance that enables businesses to recover.

The AICPA has also been involved in developing various frameworks and standards that businesses rely on to help ensure the confidentiality, integrity and availability of critical business data.In 2000 the AICPA developed Trust Services Principles and Criteria (TSP&C) to respond to the business need of providing independent assurance on confidentiality, integrity and availability on information trusted to third parties. We also provide information security related guidance that facilitates public company compliance with various laws and regulations such as Sarbanes-Oxley (SOX) as well as required disclosures related to Security and Exchange Commission (SEC) filings.

One of the AICPA's largest contributions to the economic environment with publicly registered companies is through our active involvement with partners, audit committees and boards of directors. The CPA, acting as the trusted business advisor, provides insight and support into how shareholder concerns related to information security are addressed through various corporate governance initiatives.

We recognize the considerable work NIST has undertaken in establishing this Preliminary Framework to strengthen the resilience of critical infrastructure. Through NIST's inclusive approach, use of best practices, existing standards and guidance, and collaboration with industry and professional organizations, we look forward to a final framework that retains flexibility. Namely, a fluid framework which overtime will adapt to evolving cyber and business risks. Further, we applaud NIST for placing a high value on extra-governmental recommendations as NIST finalizes the framework.

Our review and comments focus on two of NIST's questions for reviewers found on page i of the Preliminary Framework:

> ***Does the preliminary framework appropriately integrate cybersecurity risk into business risk? Does the preliminary framework provide the tools for senior executives and boards of directors to understand risks and mitigations at the appropriate level of detail?***

The framework should provide additional background around cybersecurity threats and their impact to an organization's objectives. By providing clarity on the level at which cybersecurity objectives integrate into an organizations' Enterprise Risk Management (ERM) framework, the relationship between cybersecurity and business objectives can be better understood. For example, many organizations use the Committee of Sponsoring Organizations of the Treadway Commission (COSO) *Enterprise Risk Management – Integrated Framework* (COSO Risk Management Framework) or similar framework.

Issued in 2004, the COSO Risk Management Framework's principles-based guidance aids organizations with an approach to risk management that is enterprise-wide. The COSO Risk Management Framework provides clear direction and guidance on ERM including identifying essential components, principles, concepts and common language. We recommend NIST use the COSO Risk Management Framework in part or whole to provide adequate enterprise-wide risk management to better facilitate the relationship between cybersecurity and business.

Additionally, we remain concerned that the Preliminary Framework may not sufficiently provide the necessary tools for senior executives and boards of directors to understand risks and mitigations at an appropriate level of detail. Further, it may not provide senior executives with appropriate governance or tools at the senior level to enable effective execution of their responsibilities in the realm of ERM. Namely, the Preliminary Framework does not include a summary addressing the expected impact to critical issues on which business executives and boards of directors often focus. Among these would include reputation, consumer trust, investor or stakeholder responsibilities, required Securities and Exchange Commission disclosures outlining discussion of risks and breach costs, calculating and evaluating security metrics, operation leadership related to customer service delivery, and business opportunity. The framework should translate the issues identified to a senior management level perspective so as to facilitate executive understanding of the issues to be addressed.

Further, because cybersecurity risks vary significantly by industry and organization, it would be useful to provide background on how cybersecurity risks affect the security objectives of a

system, such as the Security Objectives established in the Federal Information Processing Standards (FIPS) Publication 199: information confidentiality, integrity, and availability. This information would help users evaluate cybersecurity risks relative to their own operations.

Does the preliminary framework provide the right level of specificity and guidance for mitigating the impact of cybersecurity measures on privacy and civil liberties?

The Preliminary Framework is helpful in aligning a government organization's cybersecurity and privacy capabilities with its enterprise risk goals. However, it does not demonstrate to users of the guide how to tie the governmental control capabilities back to the user's ERM goals and objectives or provide senior executives and boards of directors with the performance results data that drives further risk management activities. We recommend adding an example to *Table 1: Framework Core* that would provide guidance to users on how specific control capabilities placed into operation are aligned with enterprise risks and are working to mitigate or reduce actual loss events. The example should incorporate experiential loss event, outage statistics, data breach attempts and related threat reduction data.

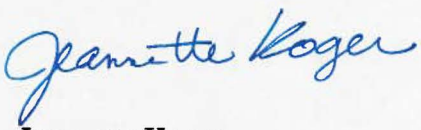
Moreover, references throughout Appendix B single out manual auditing controls as the best means of ensuring Personally Identifiable Information (PII) data remains protected (see under Protect, Protective Technology). However, the Preliminary Framework is silent on other privacy data protective technologies such as Data Loss Prevention (DLP) and Data Masking tools. DLP tools identify and prevent PII type data from being sent to or taken from hosts, servers, and other network connected devices, and data masking tools prevent developers from actually seeing PII data as they test changes to software that need to be checked against copies of production data. Data masking can also prevent regular users who deal with PII data from seeing all the data parts comprising an identifiable data element (e.g. revealing only last 4 digits of customer's Social Security Number rather than all 9 of them). We suggest updating the guidance to include references to protective technology tools that can reduce the overall cost of compliance and protection by preventing PII data from being removed from a system or otherwise viewed by users.

As sharing relates to notification on PII data, we see potential gaps in relevant and timely notification in a shared community for response to threats. For example, in the global information sharing community, when a threat comes forth that incorporates an e-mail address or IP address constituted as PII, will that cause a delay in notification? What considerations are being worked through in this area? Without slowing the process of notification, we would be concerned to see PII data removed from the system inappropriately. We recommend the framework clarify what constitutes PII and identify how information-sharing will appropriately incorporate threats as they may relate to PII.

Finally, there is little mention of the risks users face if their actions violate the Privacy Act of 1974's mandates to protect government information including PII data. With growing citizen concerns over eroding individual liberties through data theft and intelligence gathering, we suggest Appendix B include reference to existing Federal statutory and regulatory data privacy guidelines and the impact these have on users in government and industry.

We appreciate the opportunity to comment and welcome the opportunity to serve as a resource to NIST on cybersecurity issues. If we can be of further assistance, please contact Susan Pierce at 919-402-4805 or SPierce@aicpa.org.

Sincerely,



Jeannette Koger
Vice President, AICPA
CPA Advisory Services and Credentialing