October 10, 2014

Submitted by email to privacyeng@nist.gov

Ms. Diane Honeycutt
Secretary
Computer Security Division
National Institute of Standards and Technology
100 Bureau Drive, Stop 8930
Gaithersburg, MD 20899

Dear Ms. Honeycutt:

The undersigned associations appreciate the opportunity to submit this comment to the National Institute of Standards and Technology (NIST) in connection with its Privacy Engineering initiative. We have reviewed the materials released in connection with the workshop held by NIST on September 15-16 in San Jose, CA. In addition, a number of representatives from the signatory associations—and their members—participated in the workshop as well as the related webinar held on October 2, 2014.

Privacy engineering can offer tremendous value to consumers. Many of our member companies utilize privacy engineering solutions as part of their "privacy by design" practices and internal information management programs. Refining and improving privacy engineering processes requires a collaborative effort among resources devoted to information technology, compliance, legal, product development, marketing, customer service and other functional areas. NIST is well positioned to contribute technical expertise to this kind of collaborative multi-stakeholder effort to further the field of privacy engineering.

We write to express our concerns, however, that the current NIST Privacy Engineering initiative will (either explicitly or implicitly) endorse potential public policy goals rather than integrate agreed-upon policies into a framework or standard. Specifically, NIST is proposing objectives and a risk model to address those objectives, with an eye toward developing controls and metrics as part of a privacy engineering framework or standard. In order to develop objectives or a risk model that could ultimately be part of a framework or standard, the underlying policy goals need to be well-defined by a large and varied group of stakeholders. Such goals must take into account the diversity of existing privacy law requirements that span different industry sectors. In addition, policy discussions are currently underway in self-regulatory and governmental policy-making bodies, including Congress, state legislatures, the Federal Trade Commission, and the National Telecommunications and Information Administration (NTIA).

We appreciate that NIST, a technical body, has laudable intentions to avoid policy making. However, the establishment of a technical framework or standard can only follow from predefined policy objectives. Embarking on a project that includes defining privacy harms and choosing among privacy engineering objectives, without the prerequisite policy references, inevitably leads to less transparent policy-making embedded as part of a technical standards development process. Specifically, NIST has identified three objectives: predictability, manageability, and confidentiality; and has identified specified privacy harms. It is inappropriate to populate a framework with objectives and harms until such time that public policy goals are precisely defined through a consensus multi-stakeholder process.

Even in areas for which there is applicable privacy law, moving to define policy objectives and a risk model is premature. In other NIST efforts, existing best practices or standards are in place prior to the development of a framework or standard, and NIST's role is that of convener. The current initiative, however, sets out to define objectives as to which consensus does not yet exist, which is a marked departure from NIST's usual practice.

In addition to the absence of a policy framework to guide NIST's privacy engineering initiative, we are concerned about the lack of a systems engineering approach. We note that standard-setting requires a rigorous systems engineering methodology to fully describe the benefits to be achieved and problems to be solved, including desired and undesired outcomes; the human, technological, economic, and environmental actors and factors that would contribute to the system; and a description of how those actors and factors interact with one another. This proven approach is the discipline of systems engineering, which has been used by many industry sectors, governmental entities and individual companies to address very complex problem sets.

Applying a systems engineering approach to privacy would be a complex and challenging process for three reasons. First, as noted above, policy objectives have not been defined for many sectors and practices. Second, the privacy laws that cover specific regulated sectors and practices vary widely, so engineering practices based on those laws differ. Finally, there are very few, if any, current industry privacy engineering standards from which NIST can draw, unlike in the security context.

We value NIST's interest in contributing its technical expertise in the privacy realm and encourage NIST to leverage that expertise to further the privacy engineering field. We respectfully submit that NIST focus its efforts on cataloguing, in a policy-neutral manner, how privacy engineers accomplish various privacy-by-design or information management processes they are tasked with developing. In other words, the NIST privacy engineering initiative would pivot from what *should* be done in privacy engineering to what *is* being done in the privacy engineering field.

To our knowledge no such catalogue exists, and NIST will be able to make a significant contribution to the field by undertaking such an initiative.

A cataloguing effort will involve input from numerous stakeholders, including privacy engineers, as well as those within organizations that task engineers with achieving certain processes and outcomes. In particular, those in industries governed by established privacy laws would have expertise in contributing to this initiative. To provide inputs for this cataloguing, organizations could share practical examples of how they establish privacy programs and how they use Privacy Impact Assessments or similar tools to identify, assess, and address potential privacy issues.

The cataloguing initiative will provide a better and shared understanding of the use of privacy engineering solutions in corporate data governance structures. In connection with such an initiative, to gain robust participation, it will be useful for NIST to indicate that this cataloguing initiative is designed to index approaches in use, rather than yield specific endorsements or organization commitments. We believe that this cataloguing initiative will yield significant benefits in privacy protection. Such a resource will make it much easier for business and government to understand the universe of privacy protective engineering solutions currently in use, and has potential to drive further innovation in the privacy engineering field. Small and medium sized enterprises, in particular, will benefit from such a resource.

Again, thank you for the opportunity to provide input in connection with NIST's work going forward.

Sincerely,

Application Developers Alliance
CTIA-The Wireless Association
Computer & Communications Industry Association
Electronic Transactions Association
Information Technology Industry Council
Internet Association
Internet Commerce Coalition
National Business Coalition on E-Commerce & Privacy
National Cable & Telecommunications Association
National Retail Federation
Software & Information Industry Association
TechAmerica
U.S. Chamber of Commerce