October 15, 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

Re: Intel Comment on NIST Privacy Engineering Objectives and Risk Model

Dear Ms. Honeycutt:

Intel Corporation submits this response to the National Institute for Standards and Technology's request for comment on its Privacy Engineering Objectives and Risk Model. Intel commends the agency for issuing this request and takes this opportunity to urge NIST to bear in mind the following concerns as it considers standard setting for privacy engineering, and not to act prematurely to develop a standard in an area where policy is not yet settled.

I. Introduction

Intel is the leading manufacturer of computer, networking and communications products and has over 100,000 employees operating in 300 facilities in 50 countries. Intel develops semiconductor and software products for a broad range of computing applications. These platforms and technology advances are some of the most innovative and complex developments in history, and are now essential to the way we work and live. It is Intel's stated mission to create and extend computing technology to connect and enrich the lives of every person on earth. We envision the role of technology to improve education, energy distribution, government responsiveness and the delivery of health care. To support this mission, Intel works with policymakers, regulators, experts, advocates and industry to resolve policy questions related to security and intellectual property. Intel actively pursues creative, workable ways to protect individuals' privacy. In doing so, it seeks to establish a trusted digital environment in which data and technology can be used robustly, and in which individuals confidently can engage in commerce, conduct research, connect with friends and family, and participate in public life.

Intel appreciates the interest that NIST has taken in privacy engineering. In hosting the April and September workshops, NIST has provided an opportunity for dialogue among policymakers, non-governmental organizations, industry and technical experts.

Intel has long recognized the value and importance of privacy engineering. As companies evolve their privacy governance to incorporate accountability programs and privacy-by-design, privacy engineering fosters the consideration of privacy and the "building in" of necessary privacy protecting controls and measures into all phases of the life cycle of technology, software, or data applications – from inception to retirement and data deletion. In its public policy advocacy, and in its own engineering processes, Intel promotes dialog and collaboration between privacy policy, compliance and technical personnel so that products and services further optimal privacy outcomes. We believe that as a matter of policy, entities that process personal information (or create tools, applications, products or systems that process personal information) should incorporate privacy engineering into their own development models and, when appropriate, require it of their vendors.

II. The policy related to privacy engineering is not ripe for standards work.

Intel believes that any work on a standard should be based on policy that has been developed and agreed upon in the appropriate forums and with the participation of all interested stakeholders. The policy that would be the subject of a privacy engineering standard is not yet settled. Policymakers, experts, advocates and industry are investing tremendous resources and effort to understand how traditional concepts of privacy and data protection, articulated in longstanding notions of fair information practices, can be applied in the current data environment. Moreover, approaches to privacy protection have placed greater emphasis on safeguarding individuals and mitigating the risk of harm that may result from the misuse, loss, or misappropriation of data. Stakeholders are working to understand and articulate the scope and nature of the harms companies must assess and mitigate. These and other questions about privacy are not yet resolved, and standards development in these areas would be premature.

III. Work on privacy engineering standards should only be undertaken when it is determined that a standard would benefit stakeholders and if so, what its appropriate scope should be.

Once privacy policy has been determined, and before standard setting work is undertaken, it will be important to evaluate whether and to what extent businesses, computer and data scientists and consumers would benefit from a standard. It will also be important to understand what the appropriate nature and scope of that standard may be.

As NIST considers work on a privacy engineering standard, it is important to bear in mind that such a standard, if developed, could take many forms. It could include a common taxonomy for privacy that would facilitate productive collaboration between technical, compliance and policy personnel. It could identify points in the development process at which collaboration may be most beneficial. It could also articulate a set of questions to be answered by participants in the privacy engineering process. While these are only a few examples, they highlight the importance of understanding what kind of standard, should it be developed, would best serve the industry.

While concepts of security and the metrics by which it is measured are more generally accepted across nations and regions, notions of privacy are highly subjective. Among the greatest challenges to developing public policy in this area is how personally and culturally specific our concepts of privacy are. Moreover, one of the most important goals – and challenges – in developing privacy governance has been to foster the unimpeded flow of data across national and regional borders. Before embarking on a standard setting process, it will be critical to understand the impact a standard may have on the ability to move data across networks and on efforts to design privacy governance that is interoperable.

IV. Any standard-setting should result from a "bottom up" rather than "top down" process.

These concerns highlight how necessary it is that NIST's work reflects the "bottom up" approach that has characterized the development of successful standards. We cannot emphasize enough the importance of a process that benefits from the insight of all interested stakeholders – industry, government, the technical community and non-governmental organizations – whose collective experience and expertise can inform decisions about the relative merits of developing a standard and its appropriate scope.

V. Conclusion

In the area of privacy engineering, Intel believes that at this time NIST's most effective role is to serve as a convener, encouraging dialog about technical matters pertaining to privacy. These could include discussions about how to promote productive, clear communication between technologists, policy staff and compliance officers, and the integration of privacy analysis in the development process.

Intel appreciates the opportunity to comment on the NIST privacy engineering initiative, and looks forward to serving as a resource as the agency considers this work.

Respectfully submitted,

Peter Cleveland
Vice President, Legal and Corporate Affairs
Director, Global Public Policy
Intel Corporation