ACM US Public Policy Council

Association for Computing Machinery
US Public Policy Council
usacm.acm.org

July 31, 2015

National Institute of Standards and Technology
100 Bureau Drive, Stop 1070
Gaithersburg, MD 20899-1070

Re: Public comment on the draft report NISTIR 8062, *Privacy Risk Management for Federal Information Systems*

Dear NIST:

Thank you for the opportunity to comment on the draft report NISTIR 8062, *Privacy Risk Management for Federal Information Systems*. The ACM U.S. Public Policy Council supports NIST's efforts to define a framework to help manage growing privacy risk in the processing of personal information in federal information technology systems. Introducing the privacy risk management framework (PRMF) can provide continuity across the government sector, its service providers, and those in the private sector who may consider adopting the framework.

With more than 100,000 members, ACM (Association for Computing Machinery) is the world's largest educational and scientific computing society, uniting computing educators, researchers, and professionals to inspire dialogue, share resources, and address the field's challenges. The ACM U.S. Public Policy Council (USACM) serves as the focal point for ACM's interaction with the U.S. government in all matters of U.S. public policy related to information technology. The comments in this letter represent the views of the ACM U.S. Public Policy Council only.

***Privacy Risk Management Framework:* Does the framework provide a process that will help organizations make more informed system development decisions with respect to privacy? Does the framework seem likely to help bridge the communication gap between technical and non-technical personnel?**

The PRMF could benefit from further description of the interrelationship of privacy risk management with the other risks that federal agencies manage. Although the report focuses on privacy risk, many privacy risks are interdependent with other types of risks, data actions, and processes. Ideally, the framework would better detail how these work in tandem so as to address risk comprehensively (i.e., enterprise risk management).

While the NIST goals of repeatable and measurable processes are understandable, the PRMF does not embody objective measurement. Measurement of some objective property has an entirely different epistemological status than the arbitrary assignment of numbers to subjective properties. The latter does not make a process measurable and undermines its repeatability. For example, the Privacy Risk Assessment Model (PRAM) Example, Appendix D - Worksheet 3, assigns various likelihood values with no insight on their basis. Total Business Impact uses up to five data attributes ("Business Impact Factors") in its calculation. Providing additional guidance on how these should be derived from objective properties will enhance consistency within agencies and across industry.

***Privacy Engineering Objectives:* Do these objectives seem likely to assist system designers and engineers in building information systems that are capable of supporting agencies' privacy goals and requirements? Are there properties or capabilities that systems should have that these objectives do not cover?**

There is no clear linkage with or back to the privacy engineering objectives. It is unclear what role, if any, these objectives play in what follows. Explicating the relationship between the privacy engineering objectives, the privacy risk model, and the privacy risk assessment methodology would enhance the coherence of the PRMF and clarify NIST's larger vision.

Privacy Risk Model: **Does the equation seem likely to be effective in helping agencies to distinguish between cybersecurity and privacy risks?**

The report should more clearly identify specific privacy concepts where there are elements unique to privacy as compared to when federal agencies might need to meet the dual imperatives of protecting privacy and security. For example, the report could better distinguish the privacy approaches of minimizing the data collected, reducing retention periods, and de-identifying data, where possible. This is not to confuse controls with problems within the equation. Industry generally confuses privacy and security. Clearly differentiating privacy from security will improve the effectiveness of the model and its adoption, as well as improve the suitability of privacy-centric controls for offsetting inherent privacy risks. Neither the "Catalog of Problematic Data Actions" in Appendix E nor the "Catalog of Problems for Individuals" in Appendix F addresses these concepts. As such, federal agencies and other organizations using existing methodologies (e.g., FAIR, OCTAVE, ISO, NIST) may not achieve the incremental benefit of adopting the PRMF.

The PRMF also defines several new terms or redefines terms already broadly used. The PRMF should strive to use already accepted terminology rather than introduce new terminology. The PRMF should have linkages with enterprise risk management. Common terminology will ease this integration. For example, threats are an accepted element of risk analysis generally and are not restricted to external factors. The term vulnerability is also a general risk analysis concept that relates to relative resistance to adverse events. These terms, taken in the context of general risk analysis, are similarly appropriate for use in privacy risk analysis.

Privacy Risk Model**: Can data actions be evaluated as the document proposes? Is the approach of identifying and assessing problematic data actions usable and actionable? Should context be a key input to the privacy risk model? If not, why not? If so, does this model incorporate context appropriately? Would more guidance on the consideration of context be helpful?**

In striving for ease of use and understanding, the equation could result in misperceptions of privacy risks. For example, a high impact but low probability data action could be inappropriately calculated as a moderate privacy risk. Thus, a mission-critical data action with a low probability could be low in the priorities. As such, an agency might improperly allocate resources to remediate immaterial risk, allowing higher risk priorities to go unresolved.

We support the proposed integration of worksheets and illustrative maps within the privacy risk assessment methodology as a means to provide useful tools for privacy managers. For example, the "Prioritized Heat Map" given in Appendix D provides a user-friendly visual depiction for management teams aiming to focus an agency's remediation efforts (e.g., capital expenditures). The worksheets in the appendices requiring various factors to be scored could be more useful if they would provide example criteria of what to use for scoring each factor and how to score against the criteria.

Conclusion

Thank you again for the opportunity to comment on this draft report and to participate in the open and transparent process to develop and refine the framework. We appreciate NIST's ongoing attention to privacy issues and efforts to help federal agencies better manage their privacy risks through sound privacy policies and practices. With some refinements, the report could provide a useful and meaningful privacy risk framework and serve as a strong foundation for the creation of tools and guidance for federal agencies. As part of NIST's ongoing support to help agencies manage privacy risks, we encourage you to consider providing ongoing updates on best practices, case studies, reference examples of successful implementations, and training opportunities.

The staff and members of the ACM U.S. Public Policy Council are available if you have questions or would like additional information about the issues raised in this public comment.

Sincerely,

Brian Dean

Eugene H. Spafford, Ph.D.
Chair, U.S. Public Policy Council (USACM)
Association for Computing Machinery

Brian Dean, PCI QSA, CIPP, CISA, PCIP
Chair, Privacy Committee
U.S. Public Policy Council (USACM)