31 July 2015

Comments Submitted via Electronic Mail

National Institute of Standards and Technology
Information Technology Laboratory
100 Bureau Drive (Mail Stop 8930)
Gaithersburg, MD 20899-8930
Email: privacyeng@nist.gov

Re: IEEE-USA and IEEE Comments on NISTIR 8062 (DRAFT)
Privacy Risk Management for Federal Information Systems

To Whom It May Concern:

The IEEE-USA and IEEE first want to commend the NIST for undertaking this work. Recent events have clearly shown that the Federal Government needs a better approach to ensuring the privacy and security of data. Privacy requirements must be translated into systems and software in a systematic and repeatable way. NIST is uniquely suited to help the government respond to these increasing risks, and we thank you for rising to the challenge.

The risk management system you have proposed is a strong step in the right direction. It is an admirable attempt to provide a framework for agencies to use when addressing privacy concerns in their unique systems. However, we are concerned that your proposal is in many places vague and lacks certain elements that will be required for it to be effective.

Comments on specific issues, as requested:

- ***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? Are there any gaps in the framework?**

  Any structured process for surfacing and evaluating privacy risks is helpful. The framework might help bridge the communication gap between technical and non-technical personnel to some extent. However, there are remaining issues that need to be addressed.

  - The risk assessment appears to be more objective than it is. The ratings of business impact factors and likelihood of occurrence are subjective. It would be helpful to provide further guidance on how different levels of impact and likelihood can be determined at the level of granularity anticipated by the worksheets.

- The framework provides no linking between risk evaluation and Privacy Engineering Objectives. It is not clear how mitigating risks identified through the framework leads to achievement of objectives.

- ***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?**

  The Predictability and Manageability objectives are helpful, in spite of the remaining questions about how predictability and manageability can be measured. However, while useful for evaluating the effectiveness of a given process, neither predictability nor manageability speaks to the security of a given system. Part of any Privacy Engineering Objectives needs to be clear guidance on how to measure the security of a privacy system, and criteria for determining when a system is secure enough. Simply being predictable and manageable is insufficient to establish that a privacy system is effective.

  The Disassociability objective is essential for any privacy system. However, the term needs to be refined. As currently defined, it doesn't capture the variety of circumstances that might require processing of some, but not all, personal information. E.g., there are some operations that might require name and address, but not SSN. A system should be able to remove or encrypt just those elements that are not required for a particular operation while providing access to the rest, whether or not those elements are classified as personal information.

- ***Privacy Risk Model***

  - **Does the equation seem likely to be effective in helping agencies to distinguish between cybersecurity and privacy risks?**

    The equation does not seem to be helpful. The equation does not distinguish between security risks and resulting problems and privacy risks. In fact, the equation creates an impression that privacy risks and controls are more quantified than they actually are. The equation might be useful in the future when the theory behind privacy risk management becomes more developed.

    Moreover, the Privacy Risk Model places an emphasis on the impact of risks on the organization, while mentioning that risks to individuals need to be part of the calculation. This seems to us to be backwards. Any government risk model needs to emphasize the risks to individuals first, with the risks to government organizations coming second. Your Risk Management System needs to make this clear at all times.

- **Can data actions be evaluated as the document proposes? Is the approach of identifying and assessing problematic data actions usable and actionable?**

  The approach to identifying and assessing privacy risks raises several concerns.

  1. There is no definition of "representative or typical" person. A lack of definition creates the possibility that system designers will skew the definition to minimize potential privacy issues.

  2. Some consideration must always be given to "atypical persons." Systems that adequately protect the privacy of typical people, but systematically fail in certain unusual, but predictable, circumstances still need to be corrected. By focusing on "typical" persons, you have dangerously limited the scope of any system evaluation.

  3. The rating of business impact factors and likelihood of occurrence are subjective. This creates the possibility of skewed risk assessments.

  4. There is no methodology for determining the cutoff in the problem prioritization table.

  5. There is no link between risks and objectives, so there is no way to evaluate which objective is furthered by addressing a particular risk. Organizations may not prioritize all objectives equally for any given system, and this framework does not allow them to tie risks to their most important objectives.

- **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?**

  Privacy scholars (and the White House Consumer Privacy Bill of Rights) identify context as important. It should be incorporated in the risk mitigation model, but the model does not do so appropriately. Appendix G describes contextual factors for consideration, but these factors do not include the context from the point of view of individuals whose data is being collected and processed. There is no mention of considering initial purposes of data collection, initial notices provided to individuals, or whether (and to whom) individuals provide consent. This is a highly significant omission because adverse reactions tied to contextual violations result from the mismatch between individual expectations and what actually happens. The model does not include consideration of expectations that might arise from the information available to individuals whose data is in the system, so it is unclear how it can prevent context violations or adverse reactions to such violations.

- **The NISTIR describes the difficulty of assessing the impact of problematic data actions on individuals alone, and incorporates organizational impact into the risk assessment. Is this appropriate or should impact be assessed for individuals alone? If so, what would be the factors in such an assessment.**

  The question of who bears the consequences of problematic data actions is a difficult one. Both individuals and organizations have legitimate interests in the processing of

personal information and bear the consequences of problematic data actions. The extent of divergence between the perceptions of consequences depends on the relationship between the organization and individual. When there is a direct relationship, the organization may care a great deal about potential loss of trust or reduced willingness to transact with the agency as a result of problematic data actions. When the relationship is indirect or non-existent, i.e., when agencies don't deal directly with individuals in their missions or operations, individual privacy concerns have much less salience to the agency. Thus, limiting privacy risk analysis to the agency's perception of risk might lead to reduced considerations of privacy issues in systems not designed for direct interaction with individuals. Because both individuals and organizations have a legitimate interest in data processing and protection of privacy, impact on individuals should be part of the risk assessment for all systems. In fact, we believe that the impact on individuals needs always to be the primary concern of any such system.

Authors of NISTIR 8062 are tackling a difficult and complicated subject. The proposal, as written, is helpful and a good step towards your goal. IEEE and IEEE-USA recognize the pressing need for this project and look forward to working with you as further steps are taken.

Thank you for giving us the opportunity to provide this information. We would welcome any further discussions with NIST on these matters.

Respectfully submitted,

James A. Jefferies
President, IEEE-USA