**General remarks on NISTIR**

* Risk orientation is good
* Should include more the design pillar

**Remarks on NISTIR definition of privacy engineering**

* Definition of privacy engineering by NISTIR-8062:
  + Current: collection of methods to support the mitigation of risks to individuals arising from the processing of their personal information within information systems.
  + Proposed: collection of methods to support the engineering of systems that mitigate risks to individuals arising from the processing of their personal information within information systems.
* Definition of privacy engineering by Ann Cavoukian
  + privacy engineering is the discipline of understanding how to include privacy as a non-functional requirement in systems engineering
  + privacy engineering is the discipline of integrating privacy as a non-functional requirement in systems engineering
  + privacy engineering is the discipline of integrating privacy as a transversal requirement in systems engineering

**Answers to NISTIR8062 questions**

*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?*

* Very good start
* Miss design phase (how to design mitigation measures)
* Does not show the iterative approach (e.g. PMRM)
* We will know of there are gaps by applying a trial approach (e.g. 2 year trial approach of the smart grid DPIA template in Europe)

*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?*

* Generally speaking I prefer the protection goals defined by Marit Hansen, Meiko Jensen, Martin Rost (http://ieee-security.org/TC/SPW2015/IWPE/2.pdf):
  + **Unlinkability:** property that privacy-relevant data cannot be linked across domains that are constituted by a common purpose and context.
  + **Transparency**: property that all privacy-relevant data processing −including the legal, technical, and organizational setting− can be understood and reconstructed at any time
  + **Intervenability**: property that intervention is possible concerning all ongoing or planned privacy-relevant data processing.
* I also prefer the order: first unlinkability, transparency, intervenability
* If we maintain the terms predictability, manageability, dissassociability I would change the order to dissassociability, predictability, manageability. I would also change the definition of predictability:
  + Predictability is the enabling of reliable assumptions by individuals, owners, and operators about personal information and its processing by an information system.
  + Predictability is the enabling and verifiability of reliable assumptions by individuals, owners, and operators about personal information and its processing by an information system.

*Privacy Risk Model:*

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

*As stated before we would recommend a trial approach.*