*Introduction:*

First and foremost, I congratulate you in taking leadership in this effort. It is much needed, not only by the US Federal Government, but by Privacy Offices in general.

Naturally many institutions look to NIST for guidance as the NIST work products are used by many organizations outside of the US Federal Government. This makes this work even more important.

Also, in reading through the introduction, it is clear that the Federal Government does not have a model and methodology that successfuly assists the Systems Designers and Engineers in translating requirements and regulations, though an analaysis process into controls and on into services and mechanisms.

As I read this risk framework, it not only focuses on a risk framework, but the information required to perform the risk assessment and then the processes following the risk assessment that ensure that the risks are able to be remediated.

My comments focus primarily on the input and the following processes, as I expect that you have many individuals that are weighing in on the risk assessment component.

*State of Rigourous Privacy Implementation in general:*

In my reading of recent privacy implementation benchmark studies regarding the maturity of privacy programs in general I find the results disappointing. Few entities have been able to embed privacy as a rigorous discipline into IT engineering. This makes it ever so important that NIST take a strong lead.

Certainly there are a number of disciplined models and methodologies, however most all of them are proprietary. They have been used quite successfully at the high level to inventory systems and personal information flows, apply requirements and regulations, assess risks and make high level recommendations.

Very few, if any have these models and methodologies been implemented at a more granular level to effectivley assist Systems Designers and Engineers.

*The need for the Privacy Engineer:*

Very few Privacy Offices have the band width and the skill sets to to span the entire gammet from high level privacy regulations and policies to working closely with IT professionals to engineer privacy into an IT design to develop detailed controls and translate them into services and mechanisms at the same level of detail those in the security profession do.

In my opinion, there is a need for a Privacy Engineer.

Such a Privacy Engineer would:

* join an IT project team with a comprehensive list of high level privacy controls that meet the privacy requirements and regulations set forth by the Privacy Office, legal, et al
* work with the Systems Designers and Engineers to translate those controls into specific privacy controls (much like the Security Engineer does today) which in turn can be translated into required services and on into mechanisms for that IT system, naturally taking into account the specific technologies employed
* in return, embellish the comprehensive high level privacy controls for use in the next IT project

*There are public models and methodologies available and they have been applied sucessfully since 1999/2000:*

The OASIS work is publically available in the form of the PMRM and PbD works. These works provide the models and methodology for making a Privacy Program and infosystems development processes more predictable and manageable and form the basis for demonstrating accountability.

They fill in the gap that exists in forming a comprehensive Privacy Program and applying a model and methodology to translate high-level requirements to high-level controls to risk assessment and on to detailed controls and services and then on into implementation the implementation of mechanisms.

I contend that if one does not have such rigors in place that it will be impossible to perform a risk assessment.

*Privacy Risk Management for Federal Information Systems Observations:*

In reading the NISTER 8062 Draft, I have the following high level observations:

* I recomment that the the worksheets in Appendix D be revised to include more rigorouse steps prior to the ‘Identify Data Actions” step using the OASIS PMRM and PbD works
* I recommend that these worksheets track, for example which privacy regulatory and business requirements apply to which personal information and system process (aka ‘data action’ and how these are translated into high level controls, detailed controls, services and mechanisms using the PMRM and PbD Oasis work products. This may be accomplished by creating lists for example of requirements, personal information, system processes and high level controls and then using series of matrices, identify which requirments apply to personal information, et al. When completing each list or matrix, capture the more detailed controls required, the risks and the summary issues, such that when you get to the risk step, you will have a much more comprehensive set of all three, building as you go along
* I applaude the development of the “Data Actions” and would recommend that you make the diagram more complete, by considering the components of the Oasis PMRM and PbD works
* I like the first two Privacy Engineering Objectives of Perdictability and Manageability. I would recommend that you consider Regulatory Compliane and Accountability as an objectives. I question the ‘Disassociabiilty’ objective. I was suprized that it achieved this level of objective. Perhaps if it was ‘Data Minimization’ that might work better. I understand that does not achieve the same results
* I would recommend updating the appendices to follow a more rigorous process, ensuring that there is a conncetion from one Appendix to the next, creating traceability from requirements to implemented controls via services and mechanisms

*Privacy Risk Management Framework Questions:*

It is with this supposition that I answer the NIST questions and annotate the NIST draft document. Certainly the OASIS Committees may take my observations and make a more formal response to the NIST effort, which I sincerely support.

1.       Does the framework provide a process that will help organizations make more informed system development decisions with respect to privacy?:

With a more rigorous identification of scope, privacy policy and regulatory conformance criteria, participants, systems, domain and domain owners, roles and responsibilities, touch points, personal data, business processes, media (e.g. internet, mobile, IOT) data flows and subsequent control statements, only then is it possible to take the next step of risk assessment and the design of detailed controls, services and mechanisms.

The ‘data actions’ could be more formally defined to include all of the PMRM elements defined above. The level of detail the ‘data actions’ could be clarified.

**2.       Does the framework seem likely to help bridge the communication gap between technical and non-technical personnel?**

If there were to be a direct mapping of requirements and regulations to controls along with a more comprehensive ‘data actions’, it does. This would allow a non—technical individual to understand how a requirement has been implemented

**3.       Are there any gaps in the framework?**

Yes, the framework does not take into account the elements of the PMRM and document requirements and maturity model of the Oasis PbD works.

*Privacy Engineering Objectives:*

**1.       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?**

System Designers and Engineers need very specific control statements and a rigorous process to translate those control statements into PMRM services and on into mechanisms. Certainly the risk management results inform the Systems Designers and Engineers in where they are to prioritize their work, given that implementing privacy is risk based.

**2.       Are there properties or capabilities that systems should have that these objectives do not cover?**

Yes, see above. Also, it is critical to develop the job description and rigorouse methodology for the Privacy Engineer.

*Privacy Risk Model:*

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

Obstain

**2.       Can data actions be evaluated as the document proposes?**

Yes, with major additions to the ‘data actions’ model. See above.

**3.       Is the approach of identifying and assessing problematic data actions usable and actionable?**

Yes, if the overall Federal Government is applying a risk based model. While a risk based approach will help prioritize implementations of privacy, it is often the outlier surprise that catches the Privacy Office off guard. My approach to implementing a Privacy Program has been to be more wholistic in my implementations.

**4.       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?**

Certainly, if the context were made more comprehensive and rigorous, yes. Without context is is impossible to assess risk.

**5.       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?**

It was interesting that some members on the call interpreted the risk assessment to be only for the organization

Certainly remediating certain high risk problematic data actions might prove difficult for the organization, i.e. too costly, not practical or not even feasible. A step might be added to identify the impact to the organization might be beneficial.