**OASIS DRAFT COMMENTS ON NISTIR 8062**

**July 13, 2015**

**Submitted by: the OASIS Privacy Management Reference Model Technical Committee and the Privacy Design Documentation for Software Engineers Technical Committee**

**Major Summary Comments**

The OASIS PMRM and PbD Technical Committees congratulate NIST for undertaking a risk management approach to privacy – leveraging RMF –and focusing on your two pillars – privacy engineering objectives and a privacy risk model. Everything we do should be framed in risk management; thus this approach to improved privacy protection is a much welcomed view and is much needed, not only by U.S. Federal Government agencies, but by private sector organizations as well.

However, because government agencies use COTS products to build internal systems and rely heavily on private contractors and technology companies to help define technical requirements, to develop system architectures, for cloud-based services, for software development, and for technology/product selection, NIST guidance must explicitly reference and make use of existing and emerging global industry privacy-related standards (whether definitional, policy, or technical) in constucting the NISTIR.

Creating new terminology and definitions while ignoring existing standards and specfiications will weaken the NISTIR, its usefulness and its value. The global influence and impact of international privacy regulations, such as the anticipated European General Data Protection Regulation (GDPR), make it essential that NIST guidance consider today’s data protection mandates, and the best practices and standards being developed to address them.

For well over a decade, standards organizations such as OASIS have been looking hard at data privacy/data protection in the light of global privacy regulations and business practices. They have anticipated the growing convergence between technical standards and policy. They have been developing standards and specifications which bridge the abstractions of privacy regulations, organizational policies and privacy control statements with the granular, technical domain of the architect and engineer. These should form part of the foundation for NIST guidance.

These OASIS specifications are particularly important:

Privacy Management Reference Model and Methodology v1.0 (PMRM) - http://docs.oasis-open.org/pmrm/PMRM/v1.0/cs01/PMRM-v1.0-cs01.pdf

Privacy by Design Documentation for Software Engineers (PbD-SE) - <http://docs.oasis-open.org/pbd-se/pbd-se/v1.0/csd01/pbd-se-v1.0-csd01.html>

Additionally, the NISTR should take advantage of other NIST standards and Special Publications, such as SP 800-53A r4, and important privacy engineering and risk management related work, such as the European PRIPARE initiative and other intiatives. PRIPARE, for example is consolidating the concepts of the Privacy Management Reference Model and Methodology and Privacy-by-Design into an initial methodology and process reference model for systematically incorporating the PMRM and PbD into its ICT software engineering approaches.

These documents as well as standards published by other standards bodies (such as ISO and the IETF) and important guidance from the audit community (such as the ISACA “Privacy Principles and Program Management Guide” to be published in November) are important inputs to your efforts. They must be referenced and utilized by NIST in developing NISTIR 8062.

**Privacy Engineering**

The technical community generally has not provided effective design guidance for Privacy Enhancing Technologies (PETs) and for privacy-specific technical standards to help manage privacy risks at the level available for security. While we acknowledge that a major factor in most security data breaches can be traced to ‘operationally’ induced vulnerabilities (e.g., lack of effective security hygiene, weak access control, not using encryption, social engineering attacks, and little to no monitoring (of the cyber suite and data flows)), the fact remains that we don’t have a common, open systems architecture to address all of the key elements of privacy protection, including essential privacy requirements other than security (such as user notice and consent, secondary uses, data quality, etc.).

Although we cannot ‘boil the ocean’ and need to eat the privacy elephant one chunk at a time, we must follow basic systems engineering processes in our quest to minimize our collective privacy risks in a structured, common manner. This means following a few key SysEngr/ software design principles in our collaborative quest for effective, value-added privacy protection:

(1) minimize the data to be collected, processed and stored, hence minimizing the impact of security and privacy breaches and processing failures

(2) use an open systems architecture (OSA) approach (with its loose coupling, etc – like we learned in ‘OOP’ years ago),

(3) take a data-centric architecture view (including security) (which also ‘tends’ to reduce the tight coupling and complexity factors, assessing the data and the specific environment it used in,

(4) building in security, privacy and resiliency (see NIST’s building trustworthy resilient systems - pub SP-800-160), and

(5) most importantly of all, get the requirements ‘right’ upfront (which is exremely challenging in privacy).

**The Need for --- Common, Universal Privacy Specifications**

Focusing on the last statement above, getting the requirements right first, we need to review on how that typically leads to buildable specifications and also explore what are the options if we can’t ever get them at a level of detail to develop buildable specifications that can be utilized in PETs and privacy-compliant systems.

Typically the operational requirements will be based on the business need, legal requirements AND the associated policies surrounding the capability (in many cases the policy aspects are more demanding than the pure business capability needs). These operational requirements then need to be translated into technical requirements, sometimes this process requires a lot of assumptions and interpretations – all filters that can skew what is ultimately defined in the technical views (of which there can be several). Lastly, the technical views / requirements are then translated into specifications to actually build the capability. Therein lies the first issue with providing privacy and PETS buildable specifications - several translations of what we think the business need, legal requirements and policy even are.

This has been an intractable privacy problem: the lack of a common set of (or even harmonized) global privacy policies. Without common policies, requirements are at best developed locally, creating ineroperability issues and serious risk assessment and risk management problems.

**NIST Must Consider and Use Existing Models and Methodologies**

This is a huge missed opportunity in the draft NISTIR: to integrate, leverage and harmonize other NIST publications to facilitate building the foundation for their risk management approach, In doing this, NIST should take an enterprise cyber ecosphere view, first establishing baseline sets of concise “machinable” privacy policies that can later be consumed by standards-based technologies before getting deep into quantifying their privacy engineering objectives and the risk model.

As a starting point to develop reasonably definitive sets of global/industry specific privacy policies, NIST might consider a ‘best of breed” harmonization of existing major ‘requirements’ guidance (inducing what they have in NIST 800-53a R 4 now, as well as PbD, FIPPS,European and OECD elements of course) and defining minimal, working sets from those by which to base their two pillars on. NIST SPs to consider in devloping an integrated privacy EA: Cloud 800-144; PII 800-122, IA controls 800-53, and building trustworthy resilient systems 800-160, and likely several more. These all seem to fit HOW to build data security in (privacy) – thus would seem to be EA elements in any RM effort.

The current draft missed a great opportunity to explore and collate the intent of extant, major privacy policies. Without that, what will the RM process be based on? As all we do in design, we must point back to requirements. Without that, how will you measure success of this RM effort?

The OASIS Privacy Management Reference Model and Methodology (PMRM) v1.0 is a tool to enable the development of these baseline sets of (or harmonized) privacy policy requirements: <http://docs.oasis-open.org/pmrm/PMRM/v1.0/csd01/PMRM-v1.0-csd01.pdf>

Again, this NISTIR needs to have the goal of privacy engineering as the core of its process. Additionlly, this NISTIR must reinforce the iteration part of mitigating risk. Privacy policies and requirements must be addressed first, followed by an iterative risk assessment and risk mitigation methodology. Without a rigorous methodology and documentation that tracks from business needs and legal requirements to privacy policies to requirements to controls, risk assessment and mitigation are not possible.

**Model Design Issues and Linkages to the PRIPARE PSbD methodology**

The PRIPARE project is an EU-funded 7th Framework research project, running from October 2013 to September 2015, designed to facilitate the application of a privacy and security -by-design methodology that will, among other objectives, foster a risk management culture through educational material targeted to a diversity of stakeholders and specify a privacy and security-by-design software and systems engineering methodology, using the combined expertise of the research community and taking into account multiple viewpoints (advocacy, legal, engineering, business). PRIPARE has incorporated elements of the PMRM specification for its project.

See: http://cordis.europa.eu/project/rcn/110590\_en.pdf

Measured against the PRIPARE work to date, there are several comments on the NISTIR model, as described in:

NISTIR, line 191: “The model defines an equation and a series of inputs designed to enable (i) the identification of problems for individuals that can arise from the processing of personal information and (ii) the calculation of how such problems can be reflected in an organizational risk management approach that allows for prioritization and resource allocation to achieve agency missions while minimizing adverse events for individuals and agencies collectively”.

Although this takes into account risks affecting data subjects, it reflects them only at an organizational level and does not reflect how such risks directly impact these same data subjects. There is no reference on *when* to conduct this risk assessment. It seems to “ignore or neglect” privacy by design principles such as taking into account privacy issues from the onset of project and systems.

Security Risk Assessment vs. Privacy Risk Assessment: PRIPARE also emphasizes the synergy as well as the difference between a security risk assessment and a privacy risk assessment in its methodology. PRIPARE has published its draft methodology (which is now under review): The Privacy and Security-by-design Methodology: http://pripareproject.eu/wp-content/uploads/2013/11/PRIPARE\_Deliverable\_D1.2\_draft.pdf

From the PRIPARE perspective, a privacy risk management framework should provide the capability to assess the risk of problems for individuals arising from the operations of the system that involve the processing of their information. Cybersecurity risk management frameworks, standards, and best practices can be used to address risks to individuals arising from unauthorized access to their information.

The PRIPARE Model explicitly talks about having the “demonstration of specified privacy-preserving functionality” as a business objective.  This view will be reflected in the final version of the PSbD methodology.

The PRIPARE framework is based on three privacy engineering objectives that have been developed for the purpose of facilitating the development and operation of privacy-preserving information systems: predictability, manageability, and disassociability. These principles can be mapped to PRIPARE’s suggested privacy principles:

|  |  |
| --- | --- |
| Predictability | Accountability |
| Transparency and openness |
| Compliance with notification requirements |
| Limited conservation and retention |
| Manageability | Data quality |
| Purpose specification and limitation (finality or legitimacy) |
| Purpose specification and limitation for sensitive data |
| Right of access |
| Right to object |
| Right to erasure |
| Disassociability | Confidentiality and security |
| Privacy and data protection by default |
| Privacy and data protection by design |

It is an important and welcome perspective that mitigated risks always be kept in sight, since removing them from observation is a risk itself as it “can create an inaccurate assessment of existing or potential risks, and often created temptation for pilots to dismiss potential risks’ existence because they were already perceived as resolved.” This view will also be reflected in the final version of PRIPARE’s PSbD methodology.

A major concern regarding the draft NISTIR model is that it may neglect addressing issues that are likely to occur and with a high level of impact on individuals if they do not have a direct organizational impact. This approach steps away from user-centric models where a data subject and his/her information *are*the asset to protect and completely focuses on protecting the organization. It is no longer protecting data subjects from privacy issues but protecting the organization from its consequences upon them.

A second concern is that it does not link to other efforts in terms of privacy protection. For example, privacy impact assessments (PIAs) largely recognize the need for assessing and managing privacy risks. There are existing PIA frameworks that provide useful risk framework or model guidance (e.g. BSI PIA assessment guideline <https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/ElekAusweise/PIA/Privacy_Impact_Assessment_Guideline_Langfassung.pdf?__blob=publicationFile>)

**General State of Privacy Implementations is Disappointing**

A review of recent privacy implementation benchmark studies regarding the maturity of privacy programs in general shows disappointing results. Few entities have been able to embed privacy as a rigorous discipline into IT engineering. 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.

However, very few, if any have been implemented at a more granular level to effectively assist systems designers and engineers. This makes it important that NIST take a strong lead for U.S. government systems.

**The Need for the Privacy Engineer**

Very few privacy offices and systems development organizations have in place the skill sets, bandwidth, knowledge of existing privacy standards, or the structured and disciplined collaborative mechanisms needed to translate high level privacy regulations, organizational privacy policies, and privacy control statements into system design and software development requireemants and processes.

By contrast, with respect to security (a critically important component of data privacy), the software engineer today has access to a myriad of valuable standards and technologies to build security into an IT design and to choose appropriate controls, services and mechanisms appropriate to manage security risks. This is clearly not true for privacy, which encompasses a broader set of Fair Information Practices/Principles (FIPPs) than just security. The FIPPs thus must form the basis for NIST’s privacy risk management efforts, and those efforts should recognize the need for a new technical role devoted to privacy: the Privacy Engineer.

Such a Privacy Engineer would:

* bring to an IT project team a comprehensive set of high level privacy controls that meet regulatory and other policy requirements and integrate the policy requirements of the organization’s Privacy Officer, CIO, legal team, and other key stakeholders
* work collaboratively with system designers and engineers to translate high level control statements into detailed and granular privacy control statements and functional requirements, which in turn can be refined into detailed technical services and technical functionality, and software for that IT system, naturally taking into account the specific technologies employed
* update, document and categorize the comprehensive high level and more detailed privacy controls for use in other privacy-relevant IT projects

**Published models and methodologies that should be used by NIST**

As noted above, OASIS has published models and methodologies which make this possible, both in security-specific standards such as SAML and XACML, and in privacy-specfic documents directly relevant to engineering such as the PMRM and PbD-SE specifications.

These provide critical foundational practices: the models and methodology for making a privacy program and information systems development processes more predictable and manageable and form the basis for demonstrating accountability. They also 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 into the implementation of a privacy compliant system.

Without such foundational practices in place, it will be impossible to perform a reliable risk assessment.

**Specific Recommendations**

* We recommend that the the worksheets in Appendix D be revised to include more rigorous steps prior to the ‘Identify Data Actions” step based on the OASIS PMRM and PbD specifications
* We 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 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 requirements apply to personal information, etc. When completing each list or matrix, capture the more detailed controls required, the risks, and the summary issues, such that when you move to the final risk assessment step, you will have a much more comprehensive baseline.
* Regarding “Data Actions,” we recommend that you make the diagram more complete, by considering the components of the OASIS PMRM and PbD-SE specifications
* In addition to the two Privacy Engineering Objectives of Predictability and Manageability, we recommend that you consider Regulatory Compliance and Accountability as objectives.
* We question the ‘Disassociabiilty’ objective, as this would more reasonably be understood as a specific use-case requirement flowing from policy.
* We recommend updating the appendices to follow a more rigorous process, ensuring that there is a connection from one Appendix to the next, creating traceability from requirements to implemented controls via services and mechanism

**Responses to NIST Questions**

***The Framework***

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

The NISTIR is a good start. 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.

From a practical perspective, we suggest applying a trial approach (such as the two year trial approach of the smart grid DPIA template in Europe).

With such improvements, the NISTIR may be of help when fully mature, if the general items noted earlier are at least acknowledged, as other aspects to consider, if not partially addressed therein. We especially think they need to follow the four system engineering tenets starting with the general requirements set within an expected cyber environment – to set the stage and expectations and have a baseline to measure against - and functionally decompose the key privacy elements into their privacy engineering objectives, then build the risk model around that.

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

It may, if:

* the major collective community comments are addressed. Currently the lack of even a notional requirements set to help harmonize the operators / management and technical / developers seems less likely to bridge this typical communications gap.
* there were to be a direct mapping of requirements and regulations to controls along with a more comprehensive ‘data actions.’ This would allow a non—technical individual to understand how a requirement has been implemented.

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

Yes, there are many gaps - see extensive general comments above.

Primarily, the framework does not take into account the important methodological elements identified in the PMRM v1.0 and document requirements and maturity model of the Oasis PbD-SE v1.0 specifications. Additionally, in the need to present a vision/ goal, provide a notional cyber environment, key requirements to measure to, and the details to build in an adequate set of privacy controls within a set of buildable specifications.

***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?**

Designers and engineers need to have a reference framework within an enterprise architecture to best build in interoperable and secure capabilities. In essence privacy objectives need to support buildable specifications for the many reasons stated earlier.

System Designers and Engineers also need very specific control statements and a rigorous process to translate those control statements into technical services and on into mechanisms, as illustrated in the PMRM v1.0 specification. Certainly the risk management results inform the Systems Designers and Engineers as to where they must prioritize their work, given that implementing privacy is risk based.

NIST should examine 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.
* Although we do not agree with the inclusion of disassociability, if we maintain the terms predictability, manageability, dissassociability, we recommend changing the order to dissassociability, predictability, and manageability. We 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.

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

Yes, see discussion above. Also, it is critical to develop the job description and rigorous methodology for the Privacy Engineer. It would also be valuable to map more closely to the IA C-I-A triad and harmonize with the EU’s three objectives

***Privacy Risk Model:***

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

It is a standard risk equation, so it may be useful, assuming the C-I-A link is clearer and how the three privacy objectives can account for additional privacy-specific (as opposed to security) risks. As stated before we would recommend a trial approachto determine effectiveness.

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

Possibly, with major additions to the ‘data actions’ model and addition of other recommnendations, above. The OASIS [PMRM and PbD-SE specifications] group has specific recommendations there. We would also list the key data authoritative sources in some manner to ensure that “data” is defined and used the same way. <https://www.milsuite.mil/wiki/Authoritative_Data_Sources_Process>

<http://www.data.gov/> and <https://www.niem.gov/Pages/default.aspx>

**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. This is akin to prioritizing the data actions that can cause the greatest impacts. Given the damages that can come from ‘rare’ events, the risk weighting and assessment factors needs to account for those (as we know from security valuations, using “ALE”)

While this risk based approach will help prioritize privacy implementation designs, it is often the outlier operational surprise that catches the porgram manager and Privacy Office off guard. Implementing and managing a Privacy Program must be holistic.

**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.To get the full impact in each, unique environment, a designer needs to factor in context. This is where definitions and using common syntax, ontology, data dictionary, provenance, etc, etc become a critical aspect to the usability of the risk model. Within the data centric environment, they talk about managing all aspects of data’s ‘4’Vs” – they need to be applied to privacy aspects as well. (4 V’s = Volume, Variety, Velocity and Veracity.)

Context can be best captured using a use case model, which enables risk assessment and mitigation in specific systems, applications and related engineering efforts. The OASIS PbD-SE and PMRM specifications provide important guidance to implementing such a use case centric model.

**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?**

There are multiple levels of risk assessment for data privacy systems: the overall assessment developed when conducting initial PIA’s, including risks to individuals against required policies (example: a “data quality” policy for a government system which has high impact on an individual, such as access to benefits or inclusion on a no-fly list); organizational risks, including cascading risks from interconnected systems; etc.

But the starting point must always be the specific privacy policies and requirements that are applied to specific systems and application use cases. Abstractions are useful and necessary, but risks cannot be understood and managed in the abstract. This is why the PMRM is valuable: it moves from abstract policies to specific functionality in a use-case context.

Consequently, understanding and managing the privacy risks associated with data actions is important. From that, organizational risks assessments are then possible. As noted above, the PMRM v1.0 and the PbD-SE specifications are important tools for exposing all levels of risks.

Beyond organizational and individual risk assessment, we also need to begin addressing non-person-entities (NPE) such as health devices, power plants, etc. that are part of extended, complex and interoperable systems. Again the PMRM accounts for this, by including in its methodology the concepts of Inherited, Internal and Exported privacy controls and Incoming, Internally Generated, and Outgoing PI.

***In-Line Comments:***

**Line 206:**

“The PRMF described herein does not address the processing of personal information 207 outside of information systems. It also does not examine specific controls or their 208 applicability to specific privacy risks. A future document will explore in greater detail 209 controls that an agency could use to mitigate privacy risk in information systems.”

**Comment:** Excluding “controls” as part of a risk analysis framework excludes a key component that is virtually universally recognized as fundamental to privacy risk management, including in NIST’s own publications, such as Appendix J, SP-800-53.

**Line 302, ff:**

“As a result of these ubiquitous privacy concerns, NIST guidelines and reports 305 increasingly feature privacy considerations.7 To date, these efforts to address privacy 306 have generally been based on privacy principles such as the Fair Information Practice 307 Principles (FIPPs).8 Principles such as the FIPPs have helped many organizations develop 308 baseline considerations for the protection of individuals’ privacy as new technologies 309 enter the marketplace. Nonetheless, there are ongoing debates about the adaptability of 310 these principles to new technologies.9 311 312 These debates may have less to do with the FIPPs as concepts of enduring value and 313 more to do with the metaphorical problem of forcing a square peg into a round hole. That 314 is, agencies need methods that yield repeatable and measurable results if they are to be 315 able to implement privacy protections in information systems on a consistent basis. There 316 are a number of reasons why the FIPPs, notwithstanding their conceptual value, do not 317 have the characteristics of a repeatable and measurable methodology. 318 One is that there can be wide-ranging interpretations about their meaning.”

**Comment:** FIPPs are actually the heart of data privacy, and in fact are embodied in global laws and regulations, best practices documents and standards. Characterizing them as having only “conceptual value” and – mistakenly – as a “methodology” ignores their criticality in understanding the fundamental components that together constitute data privacy, which must be addressed in any risk management framework.

It is correct that there is no agreement on definitions of FIPPs, but translating variations of existing FIPPs into a common set of policy expressions, and then further into sets of related services and associated functionality would be a useful focus of NIST’s risk assessment work. We recommend that NIST use a very valuable study, Analysis of Privacy Principles: Making Privacy Operational v2, published by the International Security Trust and Privacy Alliance (ISTPA) in 2007.

The study analyzed twelve international privacy regulations and best documents [instruments] in order to determine if a "common" set of FIPPs could be extracted or inferred. The study methodology included the use of a working set of privacy principles in order to facilitate cross-instrument mapping while also accommodating their many variations in the twelve instruments: Accountability, Notice, Consent, Collection Limitation, Use Limitation, Disclosure, Access and Correction, Security/Safeguards, Data Quality, Enforcement, and Openness.

Using direct references extracted from each instrument, mapped against these terms in tabular format, the Analysis compares and correlates the language in each instrument associated with these key principles and identifies in nine instances where a particular principle is composed of additional, definable components.

**Line 334 ff.:**

“334 The National Strategy for Trusted Identities in Cyberspace (NSTIC) is one example of an 335 initiative that demonstrates both the value of the FIPPs and their challenges.”

**Comment:** The references to the NSTIC use of FIPPs fails to differentiate between the FIPPs as foundational components of data privacy and their relationship to privacy controls, privacy requirements, and the functionality necessary to design and implement privacy-compiant systems and applications that meet privacy risk management objectives.

**Line 348 ff:**

“In practice though, PIAs have not 351 achieved their full potential as a process for assessing and understanding (and therefore 352 anticipating) privacy concerns in information systems.18 Where agencies focus largely on 353 using them to support regulatory compliance, it can be difficult to translate the 354 information in PIAs into actionable technical design recommendations. Enabling 355 agencies to better define privacy risk and system objectives for privacy could expand the 356 utility of PIAs and their benefits as a tool for addressing privacy concerns in federal information systems.”

**Comment:** Both the OASIS Privacy by Design Documentation for System Engineers (PbD-SE) and Privacy Management Reference Model and Methodology (PMRM) specifications provide usable standards by which PIA’s can bridge into actionable technical design recommendations. Recognizing the uses of PIA’s and their important relationship to operational systems and technical functionality would be a valuable focus for NIST.

**Line 361 and Line 381 ff.:**

360 361 The FIPPs and other related principles remain an important part of an overall privacy 362 protection framework.19 However, experiences with the NSTIC pilots and other NIST 363 efforts have demonstrated that although principles can provide important considerations 364 for policy development, they need to be supplemented with additional tools that facilitate 365 repeatable and measurable methods for identifying, prioritizing, and mitigating privacy 366 problems. Given the lack of such tools, NIST determined that developing a consistent 367 process for addressing privacy concerns in information systems would be beneficial for 368 internal NIST work and federal

agency missions. “

**Comment:**  As noted above tools do exist such as the PMRM, PbD-SE, and other standards. We note that the draft NISTIR has no references to these specifications and other standards developed by OASIS, ISO, IETF and other standards organizations, and encourage NIST to research the literature in order to examine available tools an their support for a broader risk management framework.

**Line 503 ff:**

“503 A privacy risk management framework, therefore, should provide the capability to assess 504 the risk of problems for individuals arising from the operations of the system that involve 505 the processing of their information.”

**Comment:** The focus on risks arising from the “operations of the system” as well as “problems for individuals” are very important concepts, and suggest that a risk management framework must apply to both the design phase and at “run-time.”

**Line 514 ff in particular, line 553 ff:**

“563  **Design privacy controls.** Having prioritized risk in the previous phase, this phase 564 is focused on the selection and implementation of controls to mitigate identified 565 privacy risks. The design process includes selection and implementation to enable 566 the development of tools and guidance for increasing agency awareness of the full 567 spectrum of available controls, including technical measures that may supplement 568 or improve upon existing policy-centric controls based on the FIPPs.”

**Comment:** There are several flaws here. First, regarding the PRMF concept generally, it appears that the focus is on “design” and not “operation.” Abstract assessments of high level risks do not, for example, address failures of components in interacting systems to function properly. The level of analysis made possible by the OASIS PbD-SE and PMRM specifications properly address all levels of risks.

Second, the treatment of “privacy controls” assumes these are mere policy expressions. However, privacy controls fulfill two important purposes: first, they represent “tangible” controls that are necessary to deliver privacy, and when properly developed are a bridge from policy to technical implementations and operatons. The implication here is that they stand apart from technical controls; in fact, they should be completely aligned and integrated.

**Line 646 ff:**

**“**638 639 NIST has developed three privacy engineering objectives for the purpose of facilitating 640 the development and operation of privacy-preserving information systems: predictability, 641 manageability, and disassociability. These objectives are designed to enable system 642 designers and engineers to build information systems that are capable of implementing an 643 agency’s privacy goals and support the management of privacy risk.”

**Comment:** We recommend that NIST reconsider this set of engineering objectives as the core objectives for delivering privacy. They represent valuable high-level ideas, particularly Manageability, when applied to privacy-associated systems. But the foundational engineering objectives must be to build systems that translate privacy requirements (FIPPs>PIA’s>Implementing Service> functionality/code). Of the three, Disassociability appears more properly addressed at the design and operational levels of privacy systems rather than a key objective; particular use cases would dictate. Perhaps NIST should consider using the Privacy by Design Foundational Principles as engineering objectives (see OASIS PbD-SE specification) rather than creating new ones from whole cloth.

**Line 774 ff and 954:**

774 775 Using this new equation, agencies can calculate the privacy risk of a data action by 776 assessing likelihood and impact of the data action becoming problematic. It is important 777 to consider both of these factors, because neither one alone can aid an agency in 778 prioritizing controls and allocating resources. 779 780

954 **Data Actions**: Information system operations that process personal information.

**Comment:** Without using methodologies such as the PMRM and the PbD-SE, the ability of practitioners to use the formula would be near impossible, because the term “data Action” requires the identification all virtually all processes, data flows, data elements etc. In an evaluated application, system or sets of systems. Such identification must be a precursor requirement for a usable risk management framework.

**Line 937 ff:**

“937 To realize these goals, future areas of work in privacy risk management will focus on 938 improving the application of controls – policy, operational and technical – to mitigate 939 risks identified with the PRMF. It will require research to identify the breadth of controls 940 available, what kinds of privacy risks they can address, how they can be effectively 941 applied, and what kind of ancillary effects their application may create.”

**Comment: “** As noted above, a focus on controls – including their categorization and definitions - such that they may be referenced across agencies and private sector engineering efforts - should be a precursor step before moving to an abstract framework. A flaw in the current NISTIR is its move to a high level framework while remaining fundamentally detached from existing, well-established and accepted privacy components such as “controls,” but also from standards and practices (FIPPs, PIA’s, privacy enhancing technologies, etc.). This criticism is reinforced by the narrative in Appendix C.

**Line 1171 ff:**

**Appendix D Use Case**

**Comment:** The “use case” model is probably the best approach to understanding the full nature of privacy requirements in an application, system, or set of systems. We recommend that NIST make use of the OASIS PMRM specificaton’s analysis methodology as an effcient way to analyze use cases and generate usable output.

**Line 1321 ff:**

Appendix F: Catalog of Problems for Individuals

**Comment:** The fundamental issues to be addressed in designing and operating applications and systems that implicate personal information are those flowing from the FIPPs, their privacy controls that support them, and the technical and business services and functionality that make them operational and auditable.

Although these problems are interesting and relevant, they, along with the “Catalog of Problematic Data Actions” in Appendix E ,appear most relevant at the PIA step, where initial evaluation of privacy impacts and risk would be addressed.