***Introduction****:*

First it’s great that NIST is taking 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.

In general, the document does a great job in section one recapping the privacy efforts / views to date and NIST’s previous works, then goes on to establish key elements of the two pillars. Thus for a first draft, it’s well on the path to becoming a superb NIST document (as always!)

My observations focus primarily on the overall goal, objectives and enterprise risk alignment aspects of the document’s outcomes and the need for the privacy community to go beyond describing high-level guidance into providing common, buildable specifications for privacy enhancing technologies (PETs) to all design and build secure, interoperable capabilities.

***State of Privacy*** *in general:*

We don’t need to go into ALL the recent data breaches (including the especially egregious Anthem and USA OPM ones, losing the PII of many millions (and even more in the OPM case)) for this effort and audience that will provide comments. Yet suffice to say the technical community in general has not provided effective design guidance for PETs to help minimize the privacy risks. While we acknowledge that a major factor in almost all data breaches is caused by ‘operationally’ induced vulnerabilities (e.g., lack of effective security hygiene, weak access control, not using encryption, 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 way to address the key elements of privacy protection to then all collectively design to.

While we acknowledge the fact that the user community must take data security and privacy protection seriously – putting them before convenience in many cases, by keeping the cyber suite maintained, the technical community also needs to coalesce to demonstrate a common, standards based way to provide those users PETs, that themselves are built interoperable and secure. These privacy design goals have some existing resources and artifacts that individually do help set the stage (examples will follow later), yet are lacking an overall privacy end state goal and vision to map back to – as I sense this risk management based approach also lacks.

As a complex, systems of systems engineer (that knows cyber security pretty well too…), I realize we cannot ‘boil the ocean’ and need to eat the privacy elephant one chunk at a time. YET we all still must follow basic systems engineering processes in our quest of minimizing our collective privacy risks in a structured, common manner (nothing new here to you all). To me this means following a few key SysEngr / software design principles in our collaborative quest for effective, value-added privacy protection: (1) use an open systems architecture (OSA) approach (with its loose coupling, etc – like we learned in ‘OOP’ years ago), (2) taking a data-centric architecture view (including security) (which also ‘tends’ to reduce the tight coupling and complexity factors in the ‘who / what’ is assessing the data and the specific environment used in), (3) building in security, privacy and resiliency (re: NIST’s building trustworthy resilient systems - another great pub SP-800-160!), and (4) most importantly of all, as we all know well, get the requirements ‘right’ upfront (which may be virtually impossible to do in privacy, more on that below).

***The need for*** *--- common, universal Privacy Specifications:*

Taking a step back and focusing in 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 the PETs can actually use.

“In general” the way we ideally get to specifications in any industry, especially one that is regulated or has laws/statutes that also apply – as privacy does, is a flow down starting with a business need that has an associated overarching policy. Whether you agree that privacy has an intrinsic business need or not (e.g., think brand / reputation – the average value of that in the top 500 companies is almost 1/3) and that the policy is driven mostly government compliance based around protection of citizens, okay there too. Typically the operational requirements will be based on the business need AND the associated policies surrounding the capability; whereas in many cases the policy aspects are more demanding than the business capability needs (as is likely the case in privacy). In total, 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 PETS buildable specifications - several translations of what we think the business need and policy even are.

All programs have those translation issues to overcome, as users want X, we all build Y. We need to endure the processes and communications are robust enough to handle the iterations necessary to build what is desired by the paying customer (and affordable) ending up with the best value overall – as adjusted by what the policy aspects deem minimally acceptable too. So now we get to the more intractable privacy problem. The lack of any effective, common, global privacy policy that is generally accepted to even start with (we of course do have PbD, FIPPS, OECD, etc. - similar but not harmonized). So what happens with a lack of a common policy is that the requirements then are at best developed based on one viewpoint; hence this begets many requirements sets out of necessity, again also likely not harmonized. If specifications are built to these varied requirements sets, then the issues of interoperability and end-to-end security are unknowns and we have no common set to offer PETS.

So why go into this long privacy situational set up? To provide a basis by which we assert that the standard way to get to a common set of buildable specifications likely won’t happen top down, so let’s just collectively build them bottom up while accommodating as many requirements sets as we can. Soon after a few iterations, we should get to an ‘approximately good’ set that is useable. That is, if the problem is seems too hard or ‘wicked’ - then change the approach to address it. Nothing new here to many of the PbD team, but the typical focus is on ‘their’ requirements set which likely won’t interoperate or scale to other environments.

***There are other existing models*** *and methodologies to leverage / incorporate:*

This is where I see the biggest missed opportunity for NIST - to integrate, leverage and harmonize their own great NIST publications to facilitate building the foundation for their risk management approach. I mentioned a couple earlier, whereas in any endeavor one should look to see what’s been done before and leverage what makes sense (as they are using RMF here). I list a few obvious NIST documents to consider, for those possibly not familiar, to offer a suggestion on how they should take an enterprise cyber ecosphere view first, establish the typical cyber environment’s baseline (and thus manage expectations up front), before getting deep into quantifying their privacy engineering objectives and then a risk model.

As mentioned earlier, without a reasonably definitive global privacy policy to map back to, a major point for NIST to consider is 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 and OECD elements of course) and at least propose a minimal set from those by which to base their two pillars on. While I generally concur with the FIPPS being high level and not risk based, I think the paper missed a great opportunity to not explore and collate the intent the major privacy defining aspects “requirements” (partially listed earlier, though they have similar high level precepts as we know) and not just point out all the FIPPS general high level nature and shortcomings. What will the RM process be based on? As all we / they do must point back to requirements. How will you measure success of this RM effort?

My view on several overarching NIST pubs (not listing all the great FIPS, etc) that they could easily integrate into an expected cyber environment (whereas most efforts need to frame their effort in an enterprise architecture (EA) view to define the various elements to, so do we / they here) by which to at least frame their Privacy RM approach and be able to refer their choices of objectives and methods back to the EA. This is of course expecting a given that they also use the Privacy Management Reference Model and Methodology (PMRM) – integrate that excellent privacy resource into the EA process as well (and I’m not being parochial, as I’m not in that WG).

<http://docs.oasis-open.org/pmrm/PMRM/v1.0/csd01/PMRM-v1.0-csd01.pdf>

NIST SPs to consider using several in an integrated cyber EA: Cloud 800-144; PII 800-122, IA controls 800-53, and building trustworthy resilient systems 800-160, and likely several and more. These all seem to fit HOW to build data security in (privacy) – thus would seem to be elements in any RM effort thereof.

***Privacy Risk Management for Federal Information Systems Observations****:*

After briefly reviewing the NISTER 8062 Draft, I offer these high-level observations:

* Fully agree on their risk management approach, following RMF!
* We all / they also need to be ‘all in’ on NIST’s very own ‘cyber security framework’ mapping the privacy elements into their five phases - identify, protect, detect, respond and recover as much as we can. Though mentioned, I did not see the CSF mapping, which can then help support the privacy controls in SP 800-53A V4 too.
* The RM privacy approach should generally try to map to the usual “IA” coverage as well - the usual “C-I-A” triangle – which the document covers and endorses. Yet it would have been useful to see a closer association to the new objectives than just the statement at the end of page 20 ‘ together, these three privacy engineering objectives, complemented by the CIA triad, to address unauthorized access to PII, provide a core set of information system capabilities… ” It’s unclear on how those six items inter-relate and support each other… what’s missing in CIA that these three provide?
* The RM needs some level of requirements base / foundation to point back too even if a notional, best of breed approximation based on existing rule sets (PbD, FIPPS, etc).
* What is the overall goal of the Privacy RM 8062. What is the vision? Aka, so what?

Yes quantify privacy risk, to then minimize risk overall – how do we do that with the other enterprise risk elements of varying impacts, etc..? Also, risk is always relative, so it’s not clear how we apply that (re: with fuzzy requirements, what matters more?), except to get the usual engineer’s response “it depends” (which almost always means a lack of the big picture); thus we’re left with continuing high-level guidance that does not help to design PETs. Risk Management is always a great approach to take - yet at some point WE ALL need help to BUILD in privacy, upfront, design it in - not just provide more high-level documents?

* Requirements themselves need to harmonize globally (if we ever can?) AND somehow lead to buildable specifications so folks can build privacy enhanced technologies (PETs)

- For example, the three main objectives they define (predictability, manageability and disassociability) are different from the ones European privacy groups have defined – while this is a RM focus effort, we do need to harmonize globally too. At least address the deltas, as RM also needs to be universal…

- Also mapping back to an overall, generally accepted, global ‘privacy policy’ as a foundation FIRST (collectively the PbD, FIPPS, OECD, etc.. and what of our own USA Privacy ACT?) , then suggest how we gauge the effectiveness of any requirements first – based on what references, THEN decide how we develop common specifications to build to them?

- It seems a better approach is to set the stage on the KEY NEEDs first, what is NIST’s privacy vision? Then as suggested, use / aggregate the many privacy requirements that exist into something as a ‘common core’ directly aligned to the RM approach, et al..

* Our collective privacy community needs to have common, buildable privacy specifications. (the major thrust of the intro material we suggested earlier)

- We sense we can’t get their waiting on a common global privacy policy (maybe if we all just used the more global OECD?) or expecting any entity to provide universal requirements that mesh and integrate in an open architecture framework – especially for the EU and USA.

- Thus we continue to propose that we define privacy specifications from the ground up and adjust them as needed to integrate more and more unique requirements.

- Not to sound parochial, but that’s what we proposed in our published IEEE CE paper (based on a specification based – open privacy framework (OPF)) and we still continue down that course, as the usual policy to requirements to specifications flow down process won’t happen in privacy.

<http://www.sciap.org/blog1/wp-content/uploads/Cyber-4-Privacy-Design-IEEE-CE-article.pdf>

*Privacy Risk Management Framework Questions:*

With the above rationale, caveats and framing observations I respond to the specific questions asked of the NIST effort, which I fully support.

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

It’s my sense it will HELP when fully mature, if the general items noted earlier are at least acknowledged, as other aspects to consider, if not partially addressed therein. I especially think they need to follow the four system engineering tenets suggested up front. Start 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?**

Likely it will, 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.

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

Yes, addressed in the overall observations section above. Mostly in the need to present a vision / goal, provide a notional cyber environment, key requirements to measure to at least, 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.

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

Yes – better map 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 probably – assuming the C-I-A ink is shown and how the three privacy objectives can contribute to other sorts of risks.

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

Probably, the OASIS group has specific recommendations there. I 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, this is akin to prioritizing the data actions that can cause the greatest impacts. Given the damages that can come from ‘rare’ events, the weighting and assessment need to account for those (as we know from security valuations, using “ALE” etc)

**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?**

Yes, 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)

**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?**

Within the larger privacy context, the answer is yes, and even goes further than organizations (which have the bulk of the legal responsibilities too) – how to incorporate non-person-entities data security (health devices, power plants, etc) that need to account for the life-altering controls they have, re: IoT privacy and beyond.