From: Marshall.Toburen@rsa.com <Marshall.Toburen@rsa.com>
Sent: Friday, October 18, 2019 5:25 PM
To: privacyframework <privacyframework@nist.gov>
Subject: Privacy Framework Feedback

Thank you for the opportunity to comment on the most recent iteration of the NIST Privacy Framework. My comment is attached.

Marshall Toburen
Risk Strategist, Risk Management Solutions | RSA, a Dell Technologies Business
o: 913.549.1521 | m: 913.370.6659
marshall.toburen@rsa.com

Comment #	Organization Name	Submitted By (Name/Email)	Page #	Line #	Section	Comment (Include rationale for comment)	Suggested Change	Type of Comment (General/Editorial /Technical)
1	RSA	Marshall Toburen / marshall.toburen@rsa.com	42	950	[3]	Footnote [3] links to a PRAM. Looking at the "Prioritizing Risk.xlsx" workbook contained in the PRAM, the worksheet "Prioritizing Risk.xlsx" only provides an example of assessing the impact of privacy risk from the perspective of impact to the organization. The guidance on the worksheet and in the Privacy Framework are clear that the privacy risk assessment should, if possible, be performed from the perspective of the individual. Since that is the guidance, the example impact assessment in this PRAM workbook should include an assessment of impact on the individual. I am concerned that if you leave the example PRAM impact risk assessment as it is, organizations embracing the Privacy Framework may adopt the example PRAM without questioning whether the methodology should be enhanced to assess the impact to the individual. In many scenarios, the impact to the organization alone is not an accurate proxy of impact to individuals.	The example privacy impact assessment contained in the "Prioritizing Risk.xlsx" of the PRAM referenced in footnote [3] should be expanded and incorporate columns for rating the impact of the Potential Problems for Individuals. In this way the example will incorporate a privacy impact assessment from both individuals and the organization's perspective and effectively challenge and encourage practitioners to try and perform privacy risk assessments from the perspective of individuals, where practical.	Technical