From: Dan Bogdanov <dan.bogdanov@cyber.ee>
Sent: Thursday, October 24, 2019 8:45 AM
To: privacyframework <privacyframework@nist.gov>
Subject: Submission of comments to the Preliminary Draft of the NIST Privacy Framework

Dear Sir/Madam,

It is with pleasure that I forward comments to the Preliminary Draft of the NIST Privacy Framework.

These comments are driven by similar work done in ISO/IEC JTC 1 Sub-committee 27, where projects such as ISO/IEC 29101 (Privacy Architecture Framework) introduce certain technologies like secure multi-party computation, homomorphic encryption. In recent times, trusted execution environments such as Intel's SGX and AMD's TrustZone have been used for similar purpose.

Please find attached the comments. We will be glad to provide additional references or input about the use of the technologies in practice, should this be needed.

Best regards,

Dan Bogdanov, PhD
Head of the Department of Information Security Systems Cybernetica AS (Tartu office) Ülikooli 2, 51003 Tartu, ESTONIA
Phone (+372) 52 75 525 @danbogdanov
https://gcc01.safelinks.protection.outlook.com/?url=https%3A%2F%2Fsharemind.cyber.ee&data=02%7C01%7Charvey.weeks%40nist.gov%7Ca8df063549d34676303208d7588044ca%7C2ab5d82fd8fa4797a93e054655c61dec%7C1%7C1%7C637075180307733115&sdata=Y%2FXLMEuxAuGW1tR0nSOl278S6q6lfdQstMCjmxoLTWE%3D&reserved=0

Comment #	Organization Name	Submitted By (Name/Email)	Page #	Line #	Section	Comment (Include rationale for comment)	Suggested Change	Type of Comment (General/Editorial /Technical)
1	Cybernetica AS	Dan Bogdanov (dan.bogdanov@cyber.ee)	27	Category	PR.DS-P	Data-in-use can also be protected through technologies including, but not limited to, secure multi-party computation, homomorphic encryption (not necessarily fully) and trusted execution environments.	Please add new subcategory PR.DS-P3 (shift existing P3 and P4 etc forward by one). The new category would be named "Data-in-use is protected".	Technical
2	Cybernetica AS	Dan Bogdanov (dan.bogdanov@cyber.ee)	28	Category	PR.PT-P	Sticky policies (whether achieved through distributed computing technologies or trusted execution environments) are a helpful technology for enforcing that private data is processed according to the purpose.	Please add new subcategory PR.PT-P5. The new category would be named "Policy enforcement technologies such as distributed computing with consensus or trusted execution environments with attetation are used."	Technical

3	Cybernetica AS	Dan Bogdanov (dan.bogdanov@cyber.ee)	28	Category	PR.PT-P	Should secure computing technologies be a better fit here, please consider the following change instead of Cybernetica comment 1 above.	Please add new subcategory PR.PT-P6. The new category would be named "Secure computing technologies (including, but not limited to, secure multi-party computation, homomorphic encryption and trusted execution environments) are used to protect private data even from the host, data user (independently of the role).	Technical