From: Steve Coplan <steve@bigid.com>
Sent: Wednesday, October 23, 2019 3:54 PM
To: privacyframework <privacyframework@nist.gov>
Subject: NIST Privacy Framework: Preliminary Draft Comments

Thank you for the opportunity to comment on the current draft of the NIST Privacy Framework. We feel that the initiative comes at a critical time, and builds effectively on the broad market acceptance for the NIST CSF.

Bridging privacy and security through a clearly defined framework will prove invaluable to bringing current resources and expertise to bear on operationalizing privacy protection - and scoping the incremental organizational, technical and policy elements that should be put in place.

As enterprises come to terms with a growing number of privacy protection and data breach notification laws across the US, we are appreciative of the work that has gone into providing clarity and structure to achieve outcomes.

Attached are our comments related to the Identify and Govern Functions.

Best,

Steve Coplan

Director of Product and Solution Marketing

BigID - Redefining Personal Data Protection & Privacy

---

165 Mercer St, 4th Floor, New York, NY, 10012

m: (646) 567-3752 | e: steve@bigid.com |

see: bigid.com/product/tour | read: bigid.com/blog | try: bigid.com/demo

Comment #	Organization Name	Submitted By (Name/Email)	Page #	Line #	Section	Comment (Include rationale for comment)	Suggested Change	Type of Comment (General/Editorial /Technical)
1	BigID	Stephen Coplan, steve@bigid.com	21	684	Appendix A	Currently, the scope of personal information isn't formally addressed in the framework- which is in effect a superset of PII. For the Identify-P function, the framework could be strengthened with guidance that is specific to the discovery and definition of personal information/data (ie data related, linked, associated to a person). The CSF includes language for discovery of sensitive and regulated data in the context of breach notification, and similar language could be mirrored in the PRF. The process of defining and determining what constitutes personal information through collaboration with stakeholders would in turn informs how Functions are implemented.	Include examples that delineate the distinction between personal information and sensitive or regulated data, such as IP address, religion, sexual orientation, health status etc	General
2	BigID	Stephen Coplan, steve@bigid.com	22	684	Appendix A	The Govern Function could be elaborated to establish a distinction between anonymization at the data element tier, as compared with encryption as mitigating control for the CSF - to account specifically for the risk of re-identification in the context of profiling.	Include language or recommendations to consider increased risk of re-identification without provision for anonymization or redaction of identifiable attributes in the context of profilinng or analytics processes.	Technical
3								