By Electronic submission to privacyframework@nist.gov

21 October 2019

Ms. Katie MacFarland
National Institute of Standards and Technology
100 Bureau Drive, Stop 2000
Gaithersburg, MD 20899

Subject: **NIST Privacy Framework: Preliminary Draft Comments**

Dear Ms. MacFarland:

IEEE is pleased to provide comments on the draft, *NIST Privacy Framework: A Tool for Improving Privacy Through Enterprise Risk Management*, dated September 6, 2019.

Attached you will find the input from both the IEEE-USA, the Washington office of IEEE representing IEEE's US-based membership; and the IEEE Standards Association.

IEEE-USA's comments focus on two general concepts:

1. Avoiding terms that suggest that this approach is "sufficient" to assure privacy. It is important that organizations use the NIST tool(s), but also go beyond this in terms of the current and anticipated privacy risks.

2. Qualifying an aspect of the risks, "inferred" or "integration" risks. Technology allows organizations and their partners to deduce information though analytic techniques that go beyond the simple acquisition and retention of personal data. The additional information perhaps creates a greater risk, as it may not be evident to users, employees, or management that the data is being created and preserved.

The IEEE Standards Association has provided a list of additional standards that IEEE believes should be included in the NIST Privacy Framework.

Thank you for helping U.S. corporations to develop a complete approach to addressing privacy challenges. If we can be of any assistance to you, please feel free to reach out to Erica Wissolik (e.wissolik@ieee.org) in our DC office.

Sincerely,

Thomas M. Coughlin

Thomas Coughlin
2019 IEEE-USA President

Encl.

IEEE-USA | 2001 L Street, N.W., Suite 700, Washington, D.C. 20036-4928 USA
Office: +1 202 785 0017 | Fax: +1 202 785 0835 | E-mail: ieeeusa@ieee.org | Web: http://www.ieeeusa.org

Comments of the IEEE-USA

Comment No.	Org Name	Submitted by (name & email)	Page no.	Line no.	Section	Comment (include rational for comment)	Suggested change	Type of comment (Genera, editorial, technical
1	IEEE-USA	Erica Wissolik e.wissolik@ieee.org	4	135	1	The phrase, "What has been missing" implies a single solution	"One missing element has been"	General
2	IEEE-USA	Erica Wissolik e.wissolik@ieee.org	6	217	1.2.1	Should include other Data Actions	Include "integration" or "inference"	Technical
3	IEEE-USA	Erica Wissolik e.wissolik@ieee.org	8	261	1.2.2	The phrase, "privacy notices and consent mechanisms are a means," assumes current and future legality of privacy notice wording, etc.	Instead, the phrase, "privacy notices and consent mechanisms MAY BE a means" reflects the risk.	General
4	IEEE-USA	Erica Wissolik e.wissolik@ieee.org	8	284	1.2.2	May need to note that "Global evolution of privacy regulations should also be considered in risk.		General
5	IEEE-USA	Erica Wissolik e.wissolik@ieee.org	11	383	2.2	"individuals" – the privacy of organizations should also be considered.	Add "or organizations."	General
6	IEEE-USA	Erica Wissolik e.wissolik@ieee.org	29	687	App. B	As with the comment on 1.2.1, data actions should be included.	Include "integration" or "inference"	Technical

Comments of the IEEE Standards Association								
Comment No.	Organization Name	Submitted by (name & email)	Page no.	Line no.	Section	Comment (include rational for comment)	Suggested change	Type of comment (General, editorial, technical)
1	IEEE Standards Association	Karen McCabe, k.mccabe@ieee.org	12	452	3.1	Add standards to the List of Standards and Guidance	See Comment 1 below	General

Comment 1: Add the following standards to the *List of Standards and Guidance*:			
IEEE P2418.8	Standard for Blockchain Applications in Governments	This standard provides a common framework for using blockchain in government affairs. The framework addresses scalability, security and privacy challenges in implementation and operation. It covers multiple aspects and features of blockchain, including tokens, smart contracts, off-chain data storage, as well as both permissioned and permission-less blockchain.	Government agencies, international organizations, IT service providers, and the public being concerned about government affairs
IEEE P2418.9	Standard for Cryptocurrency Based Security Tokens	The standard provides a framework for designing cryptocurrency based digital security tokens. This standard includes technical requirements for designing a security token in compliance with regional security laws and regulations.	Blockchain developers, users, investors, broker dealers, transfer agents, crypto custodian, crypto exchanges, financial and capital markets.
IEEE P2418.10	Standard for Blockchain-based Digital Asset Management	This standard defines a baseline architectural framework and defines functional roles for blockchain-based digital asset management implementation, e.g. digital asset creator, distributor, consumers, judiciaries, and blockchain platform providers. In addition, this standard outlines the general process for digital asset management on blockchain, use cases, and specifies functional and security requirements.	Digital asset creators, distributors, consumers, judiciaries, blockchain platform providers. The industry sectors interested in this Standard will include culture and art, entertainment, etc.

IEEE P2140.1	Standard for General Requirements for Cryptocurrency Exchanges	The factors of concern for this standard involve multiple aspects, including self-discipline and professional ethics of cryptocurrency exchange platforms, as well as relevance between them and to the cryptocurrency wallets. This standard also describes the exchanges' business logic, operational procedures, transaction specifications, user authentication programs, and fair voting system to ensure the safety of users' assets and keep the overall exchanges fair and transparent to all participants. In addition, the standard provides a small but necessary technical category of requirements, including terminologies, data modeling, basic architectural framework, key indicators, end-user interface specifications, to achieve the previously mentioned goals.	The universality and practicality of this standard relates to not only cryptocurrency exchange operators, but also to the market makers, blockchain projects teams, media, public/private investors, and others including, but not limited to, entity/individual traders who are interested in profit from ordinary investment to high-frequency trading and require a fair, friendly, transparent, orderly environment.
IEEE P2140.2	Standard for Security Management for Customer Cryptographic Assets on Cryptocurrency Exchanges	This standard defines requirements for multiple aspects of security management for customer cryptographic assets on cryptocurrency exchanges, such as user identification using multi-factor authentication, prioritized protection of customer assets under unforeseen circumstances, and professional ethics of operation for cryptocurrency exchange platforms.	The universality and practicality of this standard relates to not only cryptocurrency exchange operators, but also to the market makers, blockchain projects teams, media, public/private investors, and others including but not limited to entity/individual traders who are interested in profit from ordinary investment to high-frequency trading and require a fair, friendly, transparent, orderly and safe environment.
IEEE P2140.3	Standard for User Identification and Anti-Money Laundering on Cryptocurrency Exchanges	This standard defines requirements for multiple aspects of user identification and Anti-Money Laundering on cryptocurrency exchanges, such as KYC (Know Your Customer) and AML (Anti-Money Laundering) regulations, outsourcing proper compliance measures to third-party solutions, and	The universality and practicality of this standard relates to not only cryptocurrency exchange operators, but also to the market makers, blockchain projects teams, media, public/private

		building up a self-regulatory layer of security and accountability among exchanges. It is to keep customers from malignant influence of unethical and illegal money that can be traced back inside/outside the cryptocurrency space. It is different from the P2140.2 standard, which is based on the protection of customer cryptographic assets.	investors, and others including but not limited to entity/individual traders who are interested in profit from ordinary investment to high-frequency trading and require a fair, friendly, transparent, orderly and safe environment.
IEEE P2140.4	Standard for Distributed/Decentralized Exchange Framework using DLT (Distributed Ledger Technology)	This standard defines an extension framework based on P2140.1. The extension framework uses a Smart Contract mechanism to process transactions on an exchange, to replace the role of exchange operators. Cryptographic solutions to provide "data privacy" and "data protection" are defined. This standard also defines a series of extensible interfaces for the exchange scenario, enabling support of third-party financial derivatives using tokens.	The universality and practicality of this standard relates to owners of digital assets and cryptocurrency, blockchain project teams, digital assets evaluators, cryptocurrency market makers, public/private investors.
IEEE P2140.5	Standard for Custodian Framework of Cryptocurrency	This standard defines a standard framework of a custodian service for cryptocurrency and digital assets. The framework includes a custodian reference technical architecture, business logic description, custodian service business models, digital asset evaluation criteria, operational procedure models, and regulatory requirement support models.	The universality and practicality of this standard relates to owners of digital assets and cryptocurrency, blockchain project teams, digital assets evaluators, cryptocurrency market makers, public/private investors, security device manufacturers and custodian operators.
IEEE P2141.1	Standard for the Use of Blockchain in Anti-Corruption Applications for Centralized Organizations	This standard provides a common framework for blockchain-based Anti-Corruption Systems (ACS) for centralized organizations. This standard summarizes the uses cases and business flows for blockchain-based ACS, and specifies the implementation requirements including in the functional, performance, security and privacy aspects.	Large enterprises (especially global ones), research institutes, government agencies, international organizations, NGOs, IT service providers.

IEEE P2142.1	Recommended Practice for E-Invoice Business Using Blockchain Technology	This standard describes the blockchain based application reference architecture of e-invoice, including roles of participants, typical e-invoice business scenarios, blockchain-based business platform frameworks and security requirements.	Catering companies, Retail companies, E-commerce, Online to Offline (O2O) services, Public Transport, Regulatory Authorities, E-invoice service providers, Mobile Payment Service providers.
IEEE P2143.1	Standard for General Process of Cryptocurrency Payment	This standard defines the general process of cryptocurrency payment between consumers and merchants. This process describes how a consumer purchases goods or services with cryptocurrency and how the merchant receives fiat money in return. It involves multiple aspects such as cryptocurrency payment operators playing an agent role, consumers owning cryptocurrency, merchant accessing to a cryptocurrency payment platform, banks and cryptocurrency exchanges.	Consumers, merchants, cryptocurrency payment operators, banks, cryptographic wallet operators and cryptocurrency exchanges.
IEEE P2143.2	Standard for Cryptocurrency Payment Performance Metrics	This standard defines the performance metrics of cryptocurrency payment between consumers and merchants required to quantify the experience assessment of both consumers and merchants, such as the duration time required to complete a transaction made in cryptocurrency through a general process of cryptocurrency payment.	Consumers, merchants, cryptocurrency payment operators, banks, cryptographic wallet operators and cryptocurrency exchanges.
IEEE P2143.3	Standard for Risk Control Requirements for Cryptocurrency Payment	This standard defines the risk control requirements for cryptocurrency payment between consumers and merchants. It addresses how to control the risks on related sides and manage the security of fiat money and cryptocurrency in the value transferring process.	Consumers, merchants, cryptocurrency payment operators, banks, cryptographic wallet operators and cryptocurrency exchanges.
IEEE P2144.1	Standard for Framework of Blockchain-based Internet of Things (IoT) Data Management	This standard defines a framework of Blockchain-based Internet of Things (IoT) data management. It identifies the common building blocks of the framework that Blockchain enabled during IoT data lifecycle including data acquisition, processing, storage, analyzing, usage/exchange and obsoletion, and the interactions among these building blocks.	IoT service provider, consumer, government, IoT equipment manufacturer.

IEEE P2144.2	Standard for Functional Requirements in Blockchain-based Internet of Things (IoT) Data Management	This standard defines the functional requirements in data compliance, governance and risk management in the operational process for Blockchain-based IoT data management systems.	IoT service providers, consumers, governments and IoT equipment manufacturers.
IEEE P2144.3	Standard for Assessment of Blockchain-based Internet of Things (IoT) Data Management	This standard defines the assessment framework for data compliance, governance and risk management in Blockchain-based IoT data management, provides performance metrics such as availability, security, privacy, integrity, continuance, scalability, etc.	IoT service providers, consumers, governments, IoT equipment manufacturers.
IEEE P3141	Standard for 3D Body Processing	This standard addresses the fundamental attributes that contribute to 3D body processing quality of experiences, as well as identifying and analyzing existing metrics and other useful information relating to these attributes. It defines a standardized suite of objective and subjective methods, tools and frameworks for assessing 3D body processing quality of experience attributes, and it specifies methods, tools and frameworks to facilitate standards-based interoperability, communication, security and comparison among 3D body processing technologies such as 3D/depth sensors, scanners, digitization, simulation and modeling, analytics and animation/visualization for solution providers as well as for consumer facing companies such as in retail, health/wellness, sports/athletics, medical industries.	Makers/providers of 3D/depth sensors, scanners, digitizers, simulation and modeling, analytics and animation/visualization technologies as well as consumer facing companies such as in retail, health/wellness, sports/athletics, medical industries.
IEEE P2089	Standard for Age Appropriate Digital Services Framework - Based on the 5Rights Principles for Children	This standard is the first in a family of standards focused on the 5Rights principles, and establishes a framework for developing age appropriate digital services for situations where users are children. The framework centers around the following key areas a) recognition that the user is a child, b) has considered the capacity and upholds the rights of children, c) offers terms appropriate to children, d) presents information in an age appropriate way and e) thereby offers a level of validation for service design decisions. The standard provides a specific impact	The stakeholders are society-wide: governments and policymakers; international institutions and civil society organizations; business and tech sector especially digital service providers; parents, teachers, and children.

		rating system and evaluation criteria, and sets out how vendors, public institutions and the educational sector can meet the criteria.	
IEEE P2843	Standard for Measuring Accessibility Experience and Compliance	This standard defines test evaluation criteria which can be used to measure the accessibility user experience of devices, applications, websites, appliances and emerging immersive devices such as augmented and virtual reality (AR/VR) systems by people with different disabilities and the elderly. Evaluation criteria for both user experience and compliance are defined.	1. Disabled Community and Aging Population 2. Design and Developer Community 3. Manufacturers and Marketers/Distributors 4. Regulators
IEEE P2813	Standard for Big Data Business Security Risk Assessment	This standard describes security risk assessment methodologies of user behavior, the applicable analysis layer and the fundamental analysis layer for big data.	The stakeholders include providers, operators and customers of big data services, including internet financial services, ecommerce services, and on-line social networks.
IEEE P2049.1	Standard for Human Augmentation: Taxonomy and Definitions	This standard specifies the taxonomy and definitions for human augmentation. Human augmentation, also known as human enhancement, is used to refer to technologies that add to the human body and enhance human productivity or capability. Recent advancements in many technical areas have led to a large variety of implants, wearables and other technologies that could be classified as human augmentation.	Device manufacturers, service providers, technology developers, government agencies, consumers.
IEEE P2049.2	Standard for Human Augmentation: Privacy and Security	This standard specifies requirements, systems, methods, testing and verification for human augmentation to preserve the privacy and security of both consumers and non-consumers of human augmentation. Human augmentation, also known as human enhancement, is used to refer to technologies that add to the human body and enhance human productivity or capability. Recent advancements in many technical areas have led to a large variety of	Stakeholders include device manufacturers, service providers, technology developers, government agencies, and consumers.

		implants, wearables and other technologies that could be classed as human augmentation.	
IEEE P2049.3	Standard for Human Augmentation: Identity	This standard specifies the requirements and methods for verifying the identity of a person equipped with human augmentation technologies. Human augmentation, also known as human enhancement, refers to technologies that add to the human body and enhance human productivity or capability. Recent advancements in many technical areas have led to a large variety of implants, wearables and other technologies that could be classified as human augmentation.	Device manufacturers, service providers, technology developers, government agencies, and consumers.
IEEE P2049.4	Standard for Human Augmentation: Methodologies and Processes for Ethical Considerations	This standard specifies methodologies and processes to prioritize ethical considerations in the creation of human augmentation technologies. Human augmentation, also known as human enhancement, refers to technologies that add to the human body and enhance human productivity or capability. Recent advancements in many technical areas have led to a large variety of implants, wearables and other technologies that could be classified as human augmentation.	Device manufacturers, service providers, technology developers, government agencies, and consumers.
IEEE P2786	Standard for General Requirements and Interoperability for Internet of Clothing	This standard provides the definitions and terminologies, data structure and encoding scheme, reference information model for Internet of Clothing (IoC) system. Architectural framework, protocols and interface requirements are also defined to ensure interoperable, agile, and scalable network solutions and service delivery that are able to be implemented and maintained in a sustainable manner.	Manufacturers and users of IoC products, technology developers, devices and appliance manufacturers, networking equipment vendors, system integrators, service providers, and vertical enterprises that adopt IoC for better business outcome.
IEEE P2812	Guide for Minor Guardianship System for Online Mobile Gaming	This guide describes functional safeguards in online mobile gaming environments for minors, such as gaming time settings and consumption settings. This guide also specifies requirements on a monitoring	Mobile Gaming end users, guardians of minors that are end users, mobile Gaming industry developers and producers, social media

		system but does not specify the specific parameters on guardianship to minors.	networks, mobile application developers.
IEEE P2785	Standard for Architectural Framework and General Requirements for Smart Home Systems	This standard provides the definitions and terminologies, information modeling, architectural framework, key technological requirements, and applications related to the Smart Home systems.	Technology developers, system manufacturers, networking equipment vendors, device and components suppliers, and service providers.
IEEE P2811	Standard for Architectural Framework and Technical Requirements for Smart Lock	This standard provides definitions, terminologies and key technological requirements for smart lock systems. Architectural framework and requirements for the overall functionality including requirements to achieve security are addressed.	Smart lock device and components vendors, service providers, home system manufacturers, technology developers.
IEEE P2823	Standard for System Architecture and Technical Requirements for Smart Speakers	This standard specifies a system architecture and technical requirements for smart speakers, along with definitions, terminologies, functional descriptions, and reference designs. Requirements for performance and quality control of smart speakers are defined. In addition, this standard provides guidelines for the implementation, manufacturing, and validation of smart speakers, including testing, marking, packaging, transportation and storage, etc.	Chip vendors, device manufactures, service providers, and users.
IEEE P360	Standard for Wearable Consumer Electronic Devices - Overview and Architecture	This standard gives overview, terminology and categorization for Wearable Consumer Electronic Devices (or Wearables in short). It further outlines an architecture for a series of standard specifications that define technical requirements and testing methods for different aspects of Wearables, from basic security and suitableness of wear, to various functional areas like health, fitness and infotainment etc.	Consumers, wearable components, hardware and software manufacturers, wearable, smartphone and cloud application developers, health, fitness and other application service providers.
IEEE P2048.4	Standard for Virtual Reality and Augmented Reality: Person Identity	The standard specifies the requirements and methods for verifying a person's identity in virtual reality.	Device manufacturers, content providers, service providers, technology developers, end users and other parties that are relevant to Virtual Reality (VR).