21 April 2023

To: National Institute of Standards and Technology (NIST)

RE: Request for Comments on NIST Special Publication NIST SP 800-157r1 and NIST Special Publication NIST SP 800-217

The IEEE Standards Association (IEEE SA) welcomes the opportunity to provide its input to the National Institute of Standards and Technology (NIST) Special Publication SP 800-157r1 ipd Guidelines for Derived Personal Identity Verification (PIV) Credentials and the Special Publication NIST SP 800-217 ipd Guidelines for Personal Identity Verification (PIV) Federation.

IEEE SA is a globally recognized standards-setting body within IEEE, the largest organization of technology professionals in the world. We develop consensus standards through an open process that engages industry and brings together a broad stakeholder community.

As stated in the Request for Comments, IEEE SA recognizes that this is an initial step in helping to improve the implementation of standards based, secure, reliable credentials that are issued by federal departments and agencies to individuals. We note that Personal Identity recognition is vital to the security and trust needed for the digital information society to flourish.

However, IEEE SA would like to point out that the ethics of creating and capturing secret and proprietary data from people's personally identifiable information (PII) needs to be considered based on the potential impact to the human condition. To preserve human dignity and establish trust in the use of interoperable identity credentials, policies, protections, and practices should provide individuals some control over their digital personas and identity similar to what they exercise in their real-world iterations no matter what process may be in place to monitor, assist, or interact with their data.

There is a fundamental need for people to have the right to define access and provide informed consent with respect to the use of their personal data (as they do in the physical world). Individuals require mechanisms to help curate their unique identity and personal data in conjunction with policies and practices that make them explicitly aware of consequences resulting from access and use of their personal information.

Individuals should have knowledge and awareness of the use of any trusted identity verification services to validate, prove, and support the context-specific use of their identity.

IEEE SA also has the several standards that may be of interest as NIST looks to develop a trusted environment to manage Personal Identity Verification Credentials and Federation:

They are:

IEEE 7000™, IEEE Standard Model Process for Addressing Ethical Concerns during

System Design which incorporates a set of processes by which organizations can include consideration of ethical values throughout the stages of concept exploration and development Processes incorporated in the standard provide for traceability of ethical values in the concept of operations, ethical requirements, and ethical risk-based design are described in the standard.

7000-2021 IEEE Standard Model Process for Addressing Ethical Concerns during System Design which establishes a set of processes by which engineers and technologists can include consideration of ethical values throughout the stages of concept exploration and development, which encompass system initiation, analysis, and design. This standard provides engineers and technologists with an implementable process aligning innovation management processes, system design approaches, and software engineering methods to help address ethical concerns or risks during system design.

7001-2021 IEEE Standard for Transparency of Autonomous Systems which establishes measurable, testable levels of transparency, so that autonomous systems can be objectively assessed, and levels of compliance determined.

7002-2022 IEEE Standard for Data Privacy Process which contains requirements for a systems/software engineering process for privacy-oriented considerations regarding products, services, and systems utilizing employee, customer, or other external user's personal data.

7005-2021 IEEE Standard for Transparent Employer Data Governance which contains specific methodologies to help employers in accessing, collecting, storing, utilizing, sharing, and destroying employee data, including specific metrics and conformance criteria regarding the types of uses from trusted global partners and how third parties and employers can meet them.

7007-2021 IEEE Ontological Standard for Ethically Driven Robotics and Automation Systems which contains a set of ontologies with different abstraction levels that contain concepts, definitions, axioms, and use cases that assist in the development of ethically driven methodologies for the design of robots and automation systems.

7010-2020 IEEE Recommended Practice for Assessing the Impact of Autonomous and Intelligent Systems on Human Well-Being which provides specific and contextual well-being metrics that facilitate the use of a Well-Being Impact Assessment (WIA) process in order to proactively increase and help safeguard human well-being throughout the lifecycle of autonomous and intelligent systems (A/IS).

We would look forward to further discussions with your agency on Derived Personal Identity Credentials and Federation. If you have questions, please do not hesitate to contact Karen Mulberry.