7 October 2024

To: National Institute of Standards and Technology (NIST)

RE: Draft Digital Identity Guidelines

The IEEE Standards Association (IEEE SA) welcomes the opportunity to provide its comments on the Special Publication 800-63, Digital Identity Guidelines, 800-63-4, 800-63A-4, 800-63-B and 800-63-C and on the specific topics that NIST requested.

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.

IEEE SA has the following brief comments directed at the list of topics NIST was specifically interested in receiving feedback and recommendations:

For Identity Proofing and Enrollment, the question asked about the updated structure of the requirements around defined types of proofing sufficiently clear: Are the types sufficiently described? This may need further elaboration as IEEE SA has a corresponding question: How do the "types" deal with exceptional conditions?

For Authentication and Authenticator Management, recommended additional controls that should be applied: Are there specific implementation recommendations or considerations that should be captured? IEEE SA that Negative Authentication factors (e.g., something you do not have, and something you are not) can be as effective as the given conventional authentical factors and should be considered.

In general, regarding specific implementation guidance, reference architectures, metrics, or other supporting resources that could enable more rapid adoption and implementation of this and future iterations of the Digital Identity Guidelines, IEEE SA notes that greenfield deployments will certainly benefit from the given knowledge. However, a few examples of how to transform/retrofit the existing architecture used by potential adopters into the standard models will add value and may save cost for them.

IEEE has a portfolio of standards and resources that cover digital identity that might be of interest to NIST as it addresses digital identity online risks and the ever-changing digital threat landscape.

They include:
IEEE P2958™ Standard for a Decentralized Identity and Access Management Framework for Internet of Things, which defines a decentralized identity and access management (IAM) framework for the Internet of Things (IoT) based on the emerging concepts such as decentralized identifiers (DIDs) and verifiable credentials (VCs). The framework addresses the integration of

DIDs and VCs into the lifecycle of IoT devices as well as the decentralized IoT security services such as device authentication, data authorization and access control.

IEEE 3812.1-2023 ™ IEEE Standard for General Requirements for Identity Framework for Metaverse, which contains the requirements of an identity framework for metaverse for use across different metaverse systems. Furthermore, the relevance between real world and virtual world entities is recognized. Business logic, operational procedures, and authentication programs are covered in this standard. Also, terminologies, a basic architectural framework, and key indicators are defined.

IEEE P3222.01 ™ Standard for Blockchain-based Digital Identity System Framework, establishes requirements for blockchain based digital identity systems. The standard addresses the following attributes of the system, including but not limited to, digital identity definition, distributed digital identity creation, distributed digital identity authentication, distributed digital identity note (refers to identity credentials such as identity card, work card, member card), data or asset circulation protocols.

IEEE P1912 ™ Standard for Privacy and Security Framework for Consumer Wireless Devices, defines a privacy scale that shall be applied to data that is defined as personal identifiable information that is being collected, retained, processed or shared by or among applications implemented on networked edge, fog, or cloud computing devices. This privacy scale data provides input to assessment tools that developers or users of these applications use to develop, discover, recognize, or implement appropriate privacy settings for types or levels of personal data resident on these devices.

IEEE/UL 2933-2024 ™ IEEE/UL Standard for Clinical Internet of Things (IoT) Data and Device Interoperability with TIPPSS--Trust, Identity, Privacy, Protection, Safety, and Security, is a framework with TIPPSS principles (trust, identity, privacy, protection, safety, and security) for Clinical Internet of Things (IoT) data and device interoperability is established in this standard. This includes wearable clinical IoT and interoperability with healthcare systems including electronic health records (EHR), electronic medical records (EMR), other Clinical IoT devices, in-hospital devices, and future devices and connected healthcare systems.

For an additional list of Digital Identity Standards, please check the following link: https://digitalprivacy.ieee.org/standards#:~:text=IEEE%20Standard%20on%20Employer%20Data,decisions%20with%20their%20personal%20information.

We would look forward to further discussions with NIST on Digital Identity.

If you have questions, please do not hesitate to contact Karen Mulberry at [redacted]