Subject: Developing a Privacy Framework

To: *privacyframework@nist.gov*

The Federated Identity Resilient Ecosystem subgroup (FIRE) of the Kantara Initiative is pleased to submit the following comments in response to the Request for Information (RFI) issued by the National Institute of Standards and Technology (NIST) on November 14, 2018, document number 2018-24714.

In responding to this RFI, our primary area of response will be focused on the RFI's "Organizational Considerations" and "Structuring the Privacy Framework" sections. This response is divided into three parts as follows: Background of the Identity Ecosystem Framework; IDEF Privacy Requirements; and, Using the IDEF's Privacy Requirements in the NIST Privacy Framework.

Background of the Identity Ecosystem Framework (IDEF)

In April 2011, the White House introduced The National Strategy for Trusted Identities in Cyberspace (NSTIC), an initiative to work collaboratively with the private sector, advocacy groups, public sector agencies and other organizations to improve the privacy, security and convenience of online transactions. The Identity Ecosystem envisioned in the NSTIC is an online environment where individuals and organizations are able to trust each other because they follow agreed upon standards to

obtain and authenticate their digital identities – and the digital identities of devices. NIST established an NSTIC National Program Office which was charged with leading the day-to-day coordination of NSTIC implementation across government and the private sector.

To achieve this objective, the NSTIC established guiding principles for the creation of an Identity Ecosystem. These principles require that the Identity Ecosystem should be developed with identity solutions that are:

- Privacy-enhancing and voluntary;
- Secure and resilient;
- Interoperable; and
- Cost-effective and easy to use.

The NSTIC vested responsibility for the creation of policy and standards for the Identity Ecosystem in the Identity Ecosystem Steering Group (IDESG), a private sector-led organization. The IDESG became an independent, non-profit association after delivering version one of the Identity Ecosystem Framework in late summer/early fall of 2015.

On June 25, 2018, Kantara Initiative and the Identity Ecosystem Steering Group (IDESG) jointly announced that Kantara would take on the work artifacts, current workstreams, committees and membership of the IDESG as of July 31, 2018.

IDEF Privacy Requirements

NSTIC envisioned widespread, trusted identity exchanges using federated methods that are secure, interoperable, privacy-enhancing and easy to use. Requirements were developed over a number of years that describe a set of functions that parties must be able to fulfill, and a set of criteria for assessing those capabilities.

The requirements are an informed step forward in privacy, security, interoperability and usability based on the work of the IDESG's diverse membership[1] of experts from many different fields. The privacy requirements were developed using the Fair Information Practice Principals as a starting point and expanding and analyzing/incorporating requirements from evolving privacy standards and regulations around the world consistent with the goals of NSTIC. The appendices contain some of the privacy work developed, including references and guides in Appendix 1, high level privacy requirements in Appendix 2, and privacy requirements in Appendix 3 which form a foundational framework for defining how online transactions and the associated personal data should be collected and managed in any given transaction and business vertical, whether a one-time

[1] A listing of individuals and organizations that participated in the IDESG can be found at https://idesg.edufoundation.kantarainitiative.org/Membership/Member-List.

interaction or long-term customer-business relationship.

Using the IDEF's Privacy Requirements in the NIST Privacy Framework

It is our belief and contention that the privacy requirements contained in the appendices 2 and 3, developed with significant NIST input and funding under the NSTIC initiative, are very relevant to the work contemplated under the NIST Privacy Framework and can be used as a starting point for discussion and review of the development of an Enterprise Risk Management Tool or policies. For this reason, we encourage the consideration of the privacy framework as contained in the appendices be included in the Privacy Framework development process.

Appendix 1

Privacy References and Guides

Available at https://wiki.idesg.org/wiki/index.php?title=Privacy_References_and_Guides.

References listed in this section are provided as potential tools for helping organizations understand how to evaluate their system for alignment to the privacy requirements. References should be considered informative guides only.

General

- NSTIC FIPPs
- Privacy By Design
- AICPA Privacy Maturity Model
- AICPA GAPP
- OASIS Privacy Management Reference Model
- PrivacyTrust.org Privacy Policy Requirements
- ArcGIS Global Privacy Requirements
- ISO/IEC 27018 Information technology -- Security techniques -- Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors
- ISO/IEC 29100 (2011) Privacy Framework
- ITU IDM Requirements Document
- Microsoft-Trustworthy Computing, A guide to Data Governance for Privacy, Confidentiality and Compliance
- The Sedona Conference - Cloud Computing & Data Privacy
- Privacy Impact Assessment Handbook
- Privacy and Biometrics: Building a Conceptual Foundation
- For issues related to clear communication with users (expectation-setting, communicating changes or updates, policy-writing, etc.), please see the User Experience Requirements and Supplemental Guidance.

Regarding Privacy Risk Assessment

- Draft NISTIR 8062: Privacy Risk Management for Federal Information Systems
- MITRE Privacy Engineering Framework
- DHS Information Technology Sector Baseline Risk Assessment
- "The Role of Risk Management in Data Protection" Centre for Information Policy Leadership, Hunton & Williams

For Healthcare Organizations

- HIPAA Privacy Rule Information Page

For Organizations Doing Business with the US Government

- FICAM Trust Framework Provider Assessment Package Application
- Privacy Certificate Guidance for Federal Grantees required by 28 CFR Part 22
- NIST SP 800-162: Attribute Based Access Control Definition and Considerations (2014)
- NIST SP 800-53 "Recommended Security and Privacy Controls for Federal Information Systems and Organizations", Appendix J (Privacy Control Catalog)

For Organizations Doing Business in the EU

- US Department of Commerce: Privacy Shield Summary

Appendix 2

High-Level Privacy Requirements

Available at https://wiki.idesg.org/wiki/index.php/Privacy_Requirements.

High-level requirements utilized in guiding functional requirements development.

- Organizations shall limit the collection and transmission of personal information to the minimum necessary to fulfill the transaction's purpose and related legal requirements.
- Organizations shall limit the use of the personal information that is collected and transmitted to the specified purposes of the transaction.
- Organizations shall limit the retention of personal information to the time necessary for providing and administering the services and transactions to the individual end-user for which the personal information was collected, except as otherwise required by law, regulation or legal process.
- Organizations shall provide concise, meaningful, timely, and easy-to-understand mechanisms to communicate to end-users how they collect, use, disseminate, and maintain personal information.
- Organizations shall assess the privacy risk of aggregating personal information, and deploy controls to minimize that risk, including limiting linkages across transactions.
- Organizations shall provide appropriate mechanisms to enable individuals to access, correct, and delete personal information.

- Organizations shall determine the necessary quality of personal information used in identity assurance solutions based on the risk of that transaction, including to the individuals involved.
- Organizations shall be accountable for conformance to these requirements, and provide mechanisms for auditing, validation, and verification.
- Organizations shall provide effective redress mechanisms for, and facilitation on behalf of, individuals who believe their rights under these requirements have been violated.
- Where individuals make choices regarding the treatment of their personal information (such as to restrict particular uses), those choices shall be automatically applied to all parties downstream from the initial transaction.
- Organizations shall, where feasible, utilize identity solutions that enable transactions that are anonymous, anonymous with validated attributes, pseudonymous, and/or uniquely identified.
- Organizations will request individuals' credentials only when necessary for the transaction and then only as appropriate to the risk associated with the transaction or only as appropriate to the risks to the parties associated with the transaction.
- Participation in the Identity Ecosystem shall be voluntary.
- Organizations shall clearly indicate to individuals what personal information is mandatory and what information is optional prior to the transaction.
- Controls on the processing or use of individuals' personal information shall be commensurate with the degree of risk of the processing or use.

- Identifiers shall be segregated from attributes whenever feasible.
- Organizations shall, upon any material changes to a service that affects the prior or ongoing collection, use, dissemination, or maintenance of users' personal information, provide users with compensating controls designed to mitigate privacy risks that may arise from the material changes, which may include seeking express affirmative consent of users in accordance with relevant law or regulation

Appendix 3

Privacy Requirements

Available at https://idefregistry.edufoundation.kantarainitiative.org/idef-knowledge-base/privacy with supplemental guidance, references and applicable roles.

The Privacy requirements define the ways that users' information should be handled for online transactions so that only what is needed is collected to be used and the information that is collected is handled carefully and appropriately with users' consent.

PRIVACY-1. DATA MINIMIZATION

Entities MUST limit the collection, use, transmission and storage of personal information to the minimum necessary to fulfill that transaction's purpose and related legal requirements. Entities providing claims or attributes MUST NOT provide any more personal information than what is requested. Where feasible, IDENTITY-PROVIDERS MUST provide technical mechanisms to accommodate information requests of variable granularity, to support data minimization.

PRIVACY-2. PURPOSE LIMITATION

Entities MUST limit the use of personal information that is collected, used, transmitted, or stored to the specified purposes of that transaction. Persistent records of contracts, assurances, consent, or legal authority MUST be established by entities collecting, generating, using, transmitting, or storing personal information, so that the information consistently is used in the same manner originally specified and permitted.

PRIVACY-3. ATTRIBUTE MINIMIZATION

Entities requesting attributes MUST evaluate the need to collect specific attributes in a transaction, as opposed to claims regarding those attributes. Wherever feasible, entities MUST collect, generate, use, transmit, and store claims about USERS rather than attributes. Wherever feasible, attributes MUST

be transmitted as claims, and transmitted credentials and identities MUST be bound to claims instead of actual attribute values.

PRIVACY-4. CREDENTIAL LIMITATION

Entities MUST NOT request USER credentials unless necessary for the transaction and then only as appropriate to the risk associated with the transaction or to the risks to the parties associated with the transaction.

PRIVACY-5. DATA AGGREGATION RISK

Entities MUST assess the privacy risk of aggregating personal information, in systems and processes where it is collected, generated, used, transmitted, or stored, and wherever feasible, MUST design and operate their systems and processes to minimize that risk. Entities MUST assess and limit linkages of personal information across multiple transactions without the USER explicit consent.

PRIVACY-6. USAGE NOTICE

Entities MUST provide concise, meaningful, and timely communication to USERS describing how they collect, generate, use, transmit, and store personal information.

PRIVACY-7. USER DATA CONTROL

Entities MUST provide appropriate mechanisms to enable USERS to access, correct, and delete personal information.

PRIVACY-8. THIRD-PARTY LIMITATIONS

Wherever USERS make choices regarding the treatment of their personal information, those choices MUST be communicated effectively by that entity to any THIRD-PARTIES to which it transmits the personal information.

PRIVACY-9. USER NOTICE OF CHANGES

Entities MUST, upon any material changes to a service or process that affects the prior or ongoing collection, generation, use, transmission, or storage of USERS' personal information, notify those USERS, and provide them with compensating controls designed to mitigate privacy risks that may arise from those changes, which may include seeking express affirmative consent of USERS in accordance with relevant law or regulation.

PRIVACY-10. USER OPTION TO DECLINE

USERS MUST have the opportunity to decline registration; decline credential provisioning; decline the presentation of their credentials; and decline release of their attributes or claims.

PRIVACY-11. OPTIONAL INFORMATION

Entities MUST clearly indicate to USERS what personal information is mandatory and what information is optional prior to the transaction.

PRIVACY-12. ANONYMITY

Wherever feasible, entities MUST utilize identity systems and processes that enable transactions that are anonymous, anonymous with validated attributes, pseudonymous, or where appropriate, uniquely identified. Where applicable to such transactions, entities employing service providers or intermediaries MUST mitigate the risk of those THIRD-PARTIES collecting USER personal information. Organizations MUST request individuals' credentials only when necessary for the transaction and then only as appropriate to the risk associated with the transaction or only as appropriate to the risks to the parties associated with the transaction.

PRIVACY-13. CONTROLS PROPORTIONATE TO RISK

Controls on the processing or use of USERS' personal information MUST be commensurate with the degree of risk of that processing or use. A privacy risk analysis MUST be conducted by entities who conduct digital identity management functions, to establish what risks those functions pose to users' privacy.

PRIVACY-14. DATA RETENTION AND DISPOSAL

Entities MUST limit the retention of personal information to the time necessary for providing and administering the functions and services to USERS for which the information was collected, except as otherwise required by law or regulation. When no longer needed, personal information MUST be securely disposed of in a manner aligning with appropriate industry standards and/or legal requirements.

PRIVACY-15. ATTRIBUTE SEGREGATION

Wherever feasible, identifier data MUST be segregated from attribute data.