**General observation:** The Kantara US Federal Privacy Profile (“Profile”) takes account of both credential issuance (identity verification/assurance) and authentication, but the Guidance seems to be focused only on authentication.

**Questions for resolution**

1. Does FICAM envision identical application of Privacy Principles at all Levels of Assurance (LOA)?

*Recommendation*: Please greater emphasis on Minimalism and opt-in at LOA 1 and greater emphasis on Notice at higher LOAs. Given the greater sensitivity of the data in higher LOA systems, those systems may need to provide less privacy protection to credential users in order to provide greater privacy protections to individuals whose data is housed in those systems.

1. **Informed Consent** within the Profile seems to be inconsistent with the Notice and Opt-In provisions in Guidance. The Profile requires a description of how the service works, so that the individual can be informed about identity verification/proofing, credential issuance, and continuing management and use of credentials, while Guidance section 2.1.1, Adequate Notice, addresses only adequate notice about authentication or credential use.

*Recommendation:* Notice provided at the time of registration should include information about the entire credential lifecycle. Additional, potentially abbreviated, notice may be provided at the time of the authentication event and deal with authentication.

1. **Informed Consent** within the Profile states that CSPs should provide the ability to deny release of individual attributes to federal applications and provides some exceptions to the requirement for individual attribute-level opt-out. Guidance section 2.1.2 requires (using the term “must”) affirmative opt-in before any attribute is transmitted and requires that the user be presented with all attributes, although it does permit the user to waive consent for subsequent transmissions. There are no exceptions for pre-negotiated attribute transmission. Guidance further states that users should be able to opt out of transmission of individual attributes for each transaction.

*Recommendation*: Follow the structure of the Profile. The attributes necessary to complete a transaction with a Government RP are usually determined by that RP. Government RPs usually provide notices about required and non-required information, and even in cases of non-required information, notices often state that if the individual does not provide the information the transaction may not be completed. Particularly in cases where the IDP and the RP negotiate attributes to be transmitted with authentication (and in cases where some attributes are mandatory to make an authentication legally binding, like electronic prescribing), a presentation of individual opt-out screens would reduce usability and adoption without creating commensurate privacy benefits.

1. **No Activity Tracking** within the Profile permits exceptions for data disclosure to support proper operations of the identity service or as required by law. Guidance section 2.1.4 prohibits activity tracking for any purpose other than federated authentication. There is no discussion in Guidance about whether data about credential use in one federal agency may be disclosed to another federal agency.

*Recommendation*: Follow the structure of the Profile. IDPs will be obligated disclose credential use as required by law, and should be able to disclose for proper operations of the IDP, and for fraud detection and prevention. Given the number of data breaches that have resulted from hijacked or misused credentials, it would be difficult to make a business case for an accreditation that prohibits the use of credential activity data to secure high-LOA systems from fraud.