Date: **6 October 2015**

To: Kimberly Little Sutherland, Plenary Chair,
Matt Thompson, Management Council Chair

From: Jenn Behrens, Privacy Committee Chair

Subject: Submission of Privacy Review Report for Plenary Consideration

The following Privacy Review Report was prepared for the following work product:

IDEF Baseline Functional Requirements v1.0 with Supplemental Guidance

Submitted for privacy evaluation on:

28 September 2015

By **the Framework Management Office**

Based on our evaluation of the work product and our efforts to identify and remediate any privacy issues or risks, consistent with the Privacy Evaluation Methodology, we are submitting our report along with the following intention regarding a 5.3.3.2 objection:

☐ No Privacy Issues

X Privacy Issues, No Objection

☐ Privacy Issues, Formal Objection

List of Privacy Issues (if applicable)

INTEROP-1: Acceptance of more than one third-party authenticator does not necessarily give the user much choice of authentication provider ("IdP"). Wide user choice of IdP is specified in the NSTIC strategy and is indirectly a privacy issue because a user must trust his/her IdP to protect their relationships.

INTEROP-2: It is not clear whether the assertions themselves or just the format of the assertions must be acceptable to multiple third parties. Privacy is enhanced through the use of non-correlatable (directed) assertions that are only usable by a specific third party.

INTEROP-5: In the next version of this document, a reference to privacy or UXC requirements about notice should be included.

SECURE-6: It is not clear to which parties the account to credential pairing is supposed to be identifiable. Support for anonymous and pseudonymous usage requires that account to credential pairing not be visible to the relying party in those cases, although that linkage is visible to the user’s IdP. It should also be noted that the unique identifier will be different for different relying parties when non-correlatable (directed) identifiers are used.

SECURE-9: At line 977, there is a potential privacy issue associated with requesting additional verified attributes for risk assessment. Suggest adding, “This must be done in accordance with relevant privacy requirements, such as PRIVACY-10 and PRIVACY-13”.

SECURE-14: Since this involves the retention of data past the transaction, it should be noted that audit records and logs must be handled consistent with SECURE-2, PRIVACY-3, PRIVACY-6, and PRIVACY-14. The definition of “environment” should be clarified (in SECURE-13 as well).

SECURE-15: Auditing of security logs should be mentioned in notice to users described in PRIVACY-6.

USABLE-3: It would be helpful to cross reference PRIVACY-6 with respect to usage notices.

USABLE-4: Since it discusses portability, it would be helpful to cross reference INTEROP-7 (user redress).

PRIVACY-BP-A: Should cross-reference PRIVACY-1, PRIVACY-5, and PRIVACY-13.

Justification for Formal Objection (if applicable)

No formal objection.

Non-Privacy Comments

INTEROP-1: Should include Authentication in Applies To Activities.

INTEROP-7: Applies To Activities should include basically everything.

INTEROP-8: If logging is intended to support future auditing, it would be good to reference SECURE-14 and SECURE-15.

SECURE-5: Should note the requirement to protect unissued tokens/credentials if they could potentially be used.

USABLE-7: Perhaps the title should be changed from User Requirements to User Requests to be consistent with the wording changes in the body.

INTEROP-BP-D: Advocates the use of public open standards, but references an ISO/IEC specification which is not.

USABLE-BP-A: At line 1580, “requirements” should perhaps be “requests”

Minority Privacy Committee Opinion (if applicable)

Not applicable.