Date: 7 September 2017

To: Jenn Behrens, Adam Migus

From: Jeff Brennan, Privacy Coordination Committee Chair

Subject: Submission of Privacy Review Report for Plenary Consideration

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

FIDO Universal Authentication Framework and FIDO Universal 2nd Factor.

Submitted for privacy evaluation on: **17 Aug 2017** by Standards Coordination Committee

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 these documents:

- ☑ No Privacy Issues
- ☐ Privacy Issues, No Objection
- ☐ Privacy Issues, Formal Objection

List of Privacy Issues (if applicable)

None noted.

Justification for Formal Objection (if applicable)

Not Applicable.

Non-Privacy Comments

Please note that neither standard was evaluated against NIST SP 800-53 v5. Additionally, as noted on the August 31 Standards call, David Kelts provided input to the FIDO UAF description that is worth noting for clarification, so I will include them here for the record:

1) In line 5, the server actually registers the public key with the user account. It is then used to verify the challenge signed with the device private key, as written in the text. That public key is never circulated, and therefore not correlatable.
2) At the end of that first paragraph… "user unlock is accomplished after any combination of user-friendly and secure actions". (This is how MFA can be accomplished over UAF when an "acr" (e.g. LOA) is passed with the UAF request.)

Minority Privacy Committee Opinion (if applicable)

None noted during the meeting.