From: Judith Spencer
Sent: Monday, August 10, 2020 1:04 PM
To: dig-comments-RFC <dig-comments-rfc@nist.gov>
Cc: Matt Cooper ; Ryan Dickson; Chris Clements
Subject: SP 800-63 Comments

CertiPath appreciates the opportunity to provide input to the SP 800-63-4 Revision, a technical specification that is as important to industry as it is to the Federal Government.

Our input is of a general nature related to areas in the current SP 800-63 suite of documents that have given us concern over the past several years.

I. One of the primary decisions made when the SP 800-63-3 suite of documents replaced SP 800-63-2 was reimagining the (4) four Levels of Assurance found in SP 800-63-2 into three (3) Identity Assurance Levels (IAL), three (3) Authenticator Assurance Levels (AAL) and three (3) Federation Assurance Levels (FAL). However, this has resulted in a very broad IAL 2 which does not provide any delineation between a remote identity proofing event and an in-person (or supervised remote) identity proofing event. In addition, this category is so broad it encompasses a large majority of the actual identity proofing solutions/processes.

   On a related note, IAL3 is exceedingly narrow and almost impossible to achieve. Within the Federal Government, we have been given to understand the PIV credential meets IAL3 only because of "compensating controls." Establishing an IAL that is out of reach even for Federal organizations would seem to be self-defeating.

   CertiPath recommends reconsidering the IAL requirements in SP 800-63A and offers three suggestions.

   1. Return to four (4) IALs by dividing the IAL2 to separate remote proofing from in-person proofing; or
   2. Reconsider the requirements of IAL3 to make them more achievable for industry and government implementers and move <u>all</u> in-person proofing into that IAL; or
   3. A combination of 1&2 above – Return to four (4) IALs, dividing IAL 2 to separate remote proofing from in-person proofing *and* reconsidering the requirements of the highest IAL (IAL4?) to make them more achievable for industry and government implementers.

II. In the three tables in Section 5 of SP 800-63A – Table 5-1 Strengths of Identity Evidence, Table 5-2, Validating Identity Evidence, and Table 5-3, Verifying Identity Evidence – *Weak* Identity Evidence is defined. It sits between *Unacceptable* and *Fair*. However, there is no further reference to a process that would utilize *Weak* identity evidence, validation or verification. This begs the question as to why it is included and is *Weak* synonymous with Unacceptable (and if so, why are they not a single category)?

CertiPath recommends removing the reference to *Weak* identity evidence, validation and verification from the document.

III. In Section 6 of SP 800-63-3, *Selecting Assurance Levels*, an assessment of various impact categories is established for each of the three assurance levels, which can be applied across identity, authenticator and federation. However, there is no discussion of *likelihood* in association with the impact categories. The Low, Medium and High designations would seem to be limited to the actual impact, not its likelihood.

CertiPath recommends including the likelihood of an impact occurrence in Section 6 as a further measure in risk assessment through the use of a heat map or other device.

If you would like to discuss these comments further or would like any clarification, please do not hesitate to contact me.

Thank you

Judy

Judith Spencer.