REVISED COMMENTS FROM THE SECURE TECHNOLOGY ALLIANCE

Date:	August 10, 2020
Submitted by:	Randy Vanderhoof, Secure Technology Alliance
Contact For Organization:	rvanderhoof@securetechalliance.org
Contact For Clarification of Responses:	Thomas Lockwood, NextGenID and Identity Council Chair tlockwood@nextgenid.com

About this submission:

As the Executive Director of the Secure Technology Alliance (STA), we are submitting the following comments on SP 800-63 Digital Identity Guidelines, SP 800-63A Enrollment and Identity Proofing, SP 800-63B Authentication and Lifecycle Management, and SP 800-63C Federation and Assertions.

Unfortunately, due to COVID -19 and other factors, the group of organizations representing the Identity Council that worked on these comments were unable to complete their recommendations in time for them to be submitted for review and approval by our board before the deadline of August 10th. As a result, please accept these recommendations as the views and opinions of members of the Identity Council and other affiliated industry groups who support the Secure Technology Alliance, but these comments are not representative of the stated position of the Secure Technology Alliance.

Responses:

Furthering Alignment and Strategic Synergy between OMB M-19-17 and 800-63. OMB M-19-17 provides strategic intent and direction to enable mission delivery through improved identity, credential and access management. OMB M-19-17 specifically places 800-63 as the foundation to that policy. In doing so, OMB created a strategic leveraging opportunity for continuing enhancement of the identity ecosystem.

In gaining further alignment and support of OMB M-19-17's strategic intent, if 800-63 included controls and requirements for electronic validation and verification sources in the encouragement and anticipation that more Federal Agencies will establish these services, 800-63 can foster continuing progression away from the orientation of reliance on physical documents as evidence towards electronic sources.

Remote Proofing Maturation – Identity Council recommends further development of performance requirements for live-selfie-to-credential face matching. Additionally, device requirements should be considered one capture biometric data for remote proofing at different assurance levels. (I. E. Hardware security, cryptographic elements, hardware ownership, etc.)

Today, the reader is directed to use biometric matching FMR numbers, but this approach is less than optimal for the selfie-matching topic. There are increasing numbers of vendors attempting performance requirements for live-selfie-to-credential face matching and it's difficult to determine how consistently well this binding verification step is being done both in the matching algorithms and the control of the biometric capture hardware..

STA believes the performance requirements would be very valuable to the community at large and could have significant benefit.

Update SP-800-63 to reflect Mobile Driver's License (mDL) Entry into the Identity System -NIST SP 800-63 requires update to reflect state implementation/issuance of Mobile Driver's Licenses (mDLs) within the identity ecosystem.

Currently, four states are issuing mDLs in addition to card-based DLs and 2 more states are in final contract action. Members of STA's mDL Initiative project a total of 8 states are expected to be issuing mDLs by the end of 2020 and a projected 16-25 states issuing mDLs in 2021.

Examples cited in NIST SP 800-63-3 and NIST SP 800-63-3(a) refer to restrictions/limitations of card-based of DLs. mDLs allow digital verification within issuers and provide identity proofers a superiority capability within proofing processes. For example, in NIST SP 800-63-3, Page 13. Identity Evidence example is not valid for mDLs. Additionally, in 800-63A, page 6, an mDL might dramatically enhance remote proofing processes and alter the example on page 6.

mDLs should be a preferred capability when accepting state driver's licenses for proofing purposes.

Real ID Compliant DLs/mDLs - Strong+ Evidence
Real ID is in active implementation within the identity ecosystem. DHS-recognized Real ID Compliant Issuing States have progressed since the current version of 800-63. DLs/mDLs support individual document verification of Real ID compliance and in the case of mDL, real time verification of issuer and holder status.

DMVs should be explicitly identified as trusted ID proofing entities in the NIST implementation guidelines and Conformance Criteria. This can be accomplished by creating a "STRONG+" category of evidence and integrated into the main body.

More Formalized description of Credential Usage - The Identity Council recommends NIST include a more formalized description of credential usage. SP 800-63-3 discusses that an IAL3 credential should be able to be used for IAL1 purposes, etc. The Identity Council encourages a more formalized discussion on how this process looks in the Federated environment and how trust is appropriately established when using a credential at a different level is needed. To that end, NIST should consider recommending an additional discussion on how a credential is escalated after creation. For example - if the individual has an IAL2 credential and wishes to obtain an IAL3 credential from the same issuer, does the previous evidence remain valid or should the entire credential process begin again with fresh presentation of evidence begin again?

800-63(3) Reimagining 4 levels of Assurance to 3 and the Resulting Experienced Concerns. One of the primary decisions made when the SP 800-63-3 suite of documents replaced SP 800-63-2 was reimagining the four(4) Levels of Assurance found in SP 800-63-2 into three (3) Identity Assurance Levels (IAL) and three (3) Authenticator Assurance Levels (AAL). 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, 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. The Identity Council recommends NIST should reconsider the IAL requirements; STA offers two possible solutions.

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 all in-person proofing into that IAL; or
3. A combination of 1 and 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.

Also, in the three tables in Section 5 - 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)? STA recommends clarification to or removal of he reference to *Weak* identity evidence, validation and verification from the document.

In section 6 of 800-63-3 selecting assurance levels, an impact assessment of various impact categories is contemplated. We feel the impact categories are well covered and defined. However, there is no contemplation of likelihood of an impact category. Often this is achieved using a heat map or numbering scheme where the impact of the risk is measured against the likelihood of occurrence. NIST should consider adjusting the risk assessment methodology in section 6 such that the likelihood of an impact occurrence is contemplated within the methodology.

Biometrics Capture, Retention, Use Clarification – STA members note broad adoption and use of SP 800 63 outside of federal practices. Recently, multiple states have passed biometric use limiting legislation including California, Illinois, Texas, and Washington. Given acceleration of state and major city legislation limiting and in some instances banning facial recognition/biometrics capture and use - it may be of value/need to include clarifying language.

For example, proposed legislation in Massachusetts and the City of Portland are among the most far-reaching.

- Massachusetts - proposes a statewide ban to all agencies, not only law enforcement. IBIA is actively pursing and a link to more detailed comments are available here.
- Portland - legislation applies to private as well as government use of facial recognition. In addition, both bills use expanded definitions of facial recognition, to include surveillance and also the use of algorithms as a source of information about an individual's characteristics, such as emotions, criminal proclivities, sexual orientation etc. IBIA is actively pursing and a link to more detailed are available here.

While not applicable to federal use due to Article VI, Paragraph 2 of the U.S. Constitution commonly referred to as the Supremacy Clause, applying SP 800-63 as a best practices by non-

federal public and private organizations should include a note to review State and Local legal applicability and restrictions.

Risk Framework – The Identity Council recommends enhancing guidance and clarifying steps to support relying parties' awareness and informed decisions regarding identity requirements and risk assessment.

This includes support to help relying parties in identifying and defining minimum identity requirements for their systems and for the management and use of the same identity across multiple relying parties' systems and applications in a federated environment.

Additionally, outside of the federal space, many non-federal public and private sector organizations have adopted 800-63 but possess workforces composed of more generalists having a limited identity knowledge base. These enhancements would support both federal and non-federal community members.

Several private sector federated communities - for example the aerospace-defense and healthcare communities - provide risk frameworks that could be considered. These frameworks foster adoption and securing enterprise benefits of trusted identities in federated environments.