The Social Security Administration (SSA) appreciates the opportunity to submit pre-draft comments for the Special Publication (SP) 800-63 suite, *Digital Identity Guidelines*. We recognize the importance of strong identity proofing and authentication, and have implemented much of the existing guidance, including two-factor authentication for transactions that disclose personally identifiable information (PII).

Since 2012, we have credentialed over 50 million individuals for access to our electronic services. Strong and risk-based digital identity guidelines are critical to providing secure services to the public while promoting ease of access to the public. We appreciate your consideration of these comments as you draft the next version of the guidelines.

We look forward to supporting NIST on drafting the revised guidelines for implementing identity proofing and authentication solutions with new and enhanced privacy requirements and considerations (based on existing laws, e.g., the Privacy Act and E-GOV) to help mitigate potential associated privacy risks.

If you have any questions with respect to these comments, We would welcome the opportunity to discuss our current efforts in the areas we discuss. We look forward to working with you through the development of the new guidelines.

1. Identity Assurance for Low-Risk Transactions

When we submitted comments in 2017, we expressed concern that the revised guidance would require an overly burdensome enrollment for members of the public who conduct low-risk business with the agency. Of particular concern was that the revised guidance required the same level of identity proofing controls to protect both moderate- and low-impact systems.

This remains our concern. To our understanding, no agency has been successful in balancing operational effectiveness, true risk commensurability, and customer experience while simultaneously establishing compliance with the guidelines. The IAL2 guidelines cover any transaction from one where the risk of an error is mere inconvenience, to transactions where an error can result in serious damage. The guidance requires that reasonably innocuous disclosures, such as the time of a person's upcoming appointment at one of our field offices, receive the same level of protection as much more sensitive disclosures, such as a person's disability file, despite the immense difference in the expected impact of an identity proofing error.

Under NIST SP 800-53, Control IA-8, Identification and Authentication of Non-Organizational Users, agencies are responsible for using risk assessments for “balancing the need to ensure ease of use for access to federal information and information systems with the need to protect and adequately mitigate risk.” In the interest of allowing agencies to strike a more reasonable balance for low-risk transactions, and minimize the information we collect, we urge NIST to reconsider this decision and specifically consider the following changes:

- Rename IAL1, which represents a *prohibition* on identity proofing, to IAL0 or IAL-None. Unlike the other assessment categories where xAL2 is subsumptive to xAL1, this principle does not apply to IAL (e.g., an IAL2 solution is not also IAL1 compliant).

- Introduce controls for a new IAL1 standard that require reasonable identity assurance for transactions that the agency assesses at an impact level of LOW, comparable to LOA3 standards in NIST SP 800-63-2. This level may include controls such as allowing verification at the level of FAIR, and a single piece of STRONG evidence.

- In 800-63-4, permit identity proofing at IAL1 for transactions where the high-water mark of any impact category, with the exception of personal safety, is assessed at LOW.

The purpose of these changes is to recognize that transactions where the potential impact of error is MODERATE, bearing the risks of serious damage, demand a greater degree of protection of transactions where the potential impact of error is LOW, where the impact of an error could be a mere inconvenience.

We believe that such a change would be consistent with the direction to agencies in OMB M-19-17, which advises agencies that that "it is imperative that agencies manage the risk to services and public user data at a level commensurate with the risk inherent to the digital service offering as well as with the sensitivity of the data collected to provide the digital offering," while still offering a strong identity proofing standard that supports the public's access to digital services.

Identity Assurance Level				
Impact Categories	**0** **(No proofing – currently IAL1)**	**1**	**2**	**3**
Inconvenience, distress or damage to standing or reputation	*Not evaluated.* The absence of identity proofing implies no risk of identity proofing error.	Low	Mod	High
Financial loss or agency liability		Low	Mod	High
Harm to agency programs or public interests		Low (with low probability)	Low (with significant probability)/Mod	High
Unauthorized release of sensitive information		Low	Mod	High
Personal Safety		N/A	Low	Mod/High
Civil or criminal violations		Low	Mod	High

It is important to note that a ‘Digital Identity Acceptance Statement’ as provided in 800-63-3 Section 5.5 does not address the need for three actual levels of identity proofing that are commensurate with risk.

2. Providing alternatives to facial image verification technology

At IAL2 and IAL3, NIST requires that Credential Service Providers (CSPs) verify an applicant at the level of STRONG. To achieve this level, NIST requires either comparison to a photograph or biometric comparison.

In remote scenarios, this comparison effectively requires agencies to use facial image verification technology, also known as Facial Recognition Technology (FRT), to confirm the identity of a remote applicant. FRT has become an increasingly controversial technology, and concerns include potential bias in resolution rates across minority and underrepresented populations. Congress is currently considering multiple bills that would restrict federal funding of FRT. In preliminary testing, we have found a sizable number of customers are uncomfortable submitting a photograph or lack the technical knowledge or hardware to do so successfully.

NIST provides an alternative in the form of a biometric comparison; however, ID evidence available to the public – most typically a driver's license or passport – does not provide a biometric template from which to compare, nor are most customers equipped with the sensor hardware required to obtain or submit a biometric sample. This leaves FRT as the only practicable option to complete remote verification at IAL2.

Given privacy, usability, technology, and policy concerns around FRT, we urge NIST to identify an alternative mechanism to remotely verify identity at the STRONG level (IAL2/IAL3) that (a) is compatible with ID documents commonly issued to members of the public, and (b) does not mandate FRT. For instance, if an applicant confirms that he or she can access a code sent to the address printed on the face of the identity document or electronic address associated with the evidence, could the agency use that confirmation to establish reasonable confidence that applicant is the same person to whom the identity document was issued?

3. Providing operationally useful assessments of facial image verification technology

For facial image verification technology, we suggest that NIST consider providing metrics using test methods that reflect a real-life operational environment to provide agencies with usable evaluations of current FRT technologies (and other remote identity proofing technologies). Analysis of voice characteristic technology would also be useful.

Testing should include test subjects with no photo experience using their phones under a variety of lighting conditions, etc. taking into account the (much) older photos available on some licenses. The algorithm and software should also be tested on a demographically representative sample.

This is critical due to the increase in the need for remote identity proofing engendered by the pandemic.

4. Practical considerations for Driver's License

For most Americans, a driver's license or equivalent State-issued identification card is their primary or only identification document. Several of the validation requirements are impractical to implement given existing exchanges that the States offer to validate these identity documents. To reflect practical considerations in validating information on driver's licenses against authoritative sources, we suggest that NIST consider the following adjustments:

- Specifically indicate that unexpired passports and REAL ID Act-compliant driver's licenses and state-issued identification cards documents are acceptable at the SUPERIOR level.

    - The guidance requires that for evidence to be considered SUPERIOR, that digital information "is protected using approved cryptographic or proprietary methods, or both, and those methods ensure the integrity of the information and enable the authenticity of the issuing source to be confirmed." In its discussion of the implementing regulations (See 73 FR 5272 (Jan. 29, 2008), codified as amended at 6 CFR part 37), DHS considered requiring the Machine Readable Zone (MRZ) of drivers licenses to be encrypted. DHS ultimately decided to not require encryption "given law enforcement's need for easy access to the information, and the complexities and costs of implementing an encryption Infrastructure." This definition excludes REAL ID-compliant driver's licenses from being considered SUPERIOR evidence. We suggest reconsidering this requirement.

- The guidance for validation uses the term "issuing source or authoritative source(s)" to describe the source with which identity evidence must be validated. The guidance also only allows the single piece of STRONG or SUPERIOR evidence to be acceptable if the CSP "validates the evidence directly with the issuing source". We suggest that these requirements be expanded to allow verification through non-authoritative publishers, such as information clearinghouses. Generally, States use services provided by the American Association of Motor Vehicle Administrators (AAMVA) to verify driver's license information, and validating license details through the issuing source directly is not supported.

- At the STRONG and SUPERIOR levels, validation requires that "All personal details and evidence details are confirmed as valid." In practice, States restrict the personal details on the document that can be verified through standard exchanges, such as the name and license number. In addition, States are permitted to include information beyond that required, and verifying this supplemental data would require custom validation methods for each State. To account for this practical restriction, we recommend that the guidance permit validation of a subset of personal details rather than "all personal details and evidence details".

5. Allowance of One-Time Use Scenarios

The guidance in 800-63-2 provided a mechanism for claimants to be identity-proofed for immediate one-time access to an application (See SP 800-63-2 Section 5.3.4, Requirements for One-Time Use). This scenario was removed from SP 800-63-3, under which identity proofing always culminates in issuance of a credential. There are some situations where immediate access to an application without a credential is desirable, and we suggest NIST clarify whether this scenario continues to be permitted.

One-Time Use scenarios are particularly useful for telephone identity proofing scenarios, where a user may need to be identity proofed to access an Interactive Voice Response (IVR) or similar telephonic application. Issuing a compliant credential in such cases may be impractical. We discuss this scenario more in the following section.

We note that in one-time use scenarios, the Authentication Assurance Level (AAL) would not be applicable. If the guidance is clarified to support one-time use scenarios, we recommend clarification to the informative guidance in the executive summary of 800-63A to clarify that the AAL would not necessarily be required for federated systems.

6. Guidance for Digital Identity in Telephone and Cross-Channel Scenarios

The current guidance and its predecessors did not specifically address guidelines for identity proofing and authentication over Interactive Voice Response (IVR) prompts. Authentication and identity proofing by phone introduce complications such as non-availability of transport-level encryption, while also offering additional capabilities such as the availability of automatic number identification (ANI) to obtain the originating phone number and to initiate outbound calls. Specific guidance for identity proofing, authentication and federation for telephone scenarios would be useful to agencies in providing services for individuals who are unable or who do not wish to use Internet services but still prefer a digital channel.

7. Validity of Enrollment Code Period

800-63A Section 4.4.1.6, Step 4, states that an enrollment code, if provided, SHALL be valid for a maximum of 7 days in the CSP is performing in-person proofing.

When the enrollment code is mailed to a verified address, we suggest that NIST consider parity between the maximum validity in this step and those in Step 5 in the same list (e.g., 30 days when the code is sent to a postal code outside the contiguous United States.) If an enrollment code is sent to a mailed address, a validity period of 7 days may not be sufficient for the notice to be printed and received by the applicant, especially if the applicant resides outside the contiguous United States. Customer testing has informed us that mailing delays are very common in more rural areas and access to internet is not guaranteed within field offices.

We recommend that the maximum validity of 7 days be retained for electronic addresses. An applicant who performs in-person proofing may not have access to use a code sent to telephone or email address of record during the in-person registration event.

In addition, 800-63A Section 4.4.1.6, Step 5f introduces a requirement that the CSP send the enrollment code and notification of proofing to different addresses of record. The guidance does not explicitly state that the notification of proofing is required, and if it is inherently introduces a requirement to obtain two validated addresses. We recommend clarifying this requirement.