Comments on NIST Publication 800-63A-4 (Initial Public Draft) Enrollment and Identity Proofing

April 14th, 2023

Executive Summary

LexisNexis Risk Solutions (LNRS) overarching mission as it relates to identity and identity solutions is primarily two-fold. First and foremost, we are pro-people, and anti-fraud. Equitable access is a critical topic promulgated by the COVID-19 pandemic and the challenges that government agencies faced regarding large-scale identity verification for critical government benefits. Equitable access has been the foundation for our solutions for decades, leaving the agencies that utilized our services and the people they served in a winning position pre, during, and post-pandemic, all the while defending against fraud attacks at all levels. Tangentially, we draw the distinction that an identity is a person with history, relationships, and individual nuances, versus mere data points that can be represented or misrepresented by various forms of evidence when trying to prove someone is who they claim to be. No two identities will look or behave the same, so looking beyond data points to understand an identity is critical, and no single source of truth can provide the solution to the identity verification challenges that NIST is addressing.

It is encouraging that equitable access versus merely fraud prevention is now at the top of mind for consumers, agencies, industry, lawmakers, and standards organizations like NIST. We understand the need for standards across government agencies and are generally encouraged by these revisions as they allow for more flexibility for agencies deciding the assurance levels that are appropriate to serve both their clients and business stakeholders. We are encouraged by the revisions included by the NIST authors put forth in this 800-63-4A (IDP) that broadens the flexibility of agencies to choose the path that they see fit for the people they serve on all fronts, and the flexibility to choose their level of assurance.

There are fundamental areas that need to be addressed differently when NIST takes this initial public draft to final publication. The continued heavy reliance NIST places on a government-issued credential is the fundamental challenge with IAL-2 and IAL-2 as written. These standards continue to rely on credentials that are already highly susceptible to compromise and general risk. It is globally recognized that all U.S. identities have been stolen. It is also globally recognized that technologies are readily available to replicate government-issued identities. The approaches effectively assess an identity as a static entity where in reality an identity, particularly when compromised, is highly non-stationary. The next iteration of standards must put credibility and weight on the engagement methods by which an identity transacts in an unsupervised remote identity verification transaction: Bring digital assessment into the IAL standards such as assessing the device utilized, device velocity, origin of the transaction, the email utilized, and knows risk signals.

In contrast to the private sector, the Government cannot selectively choose its customers, and likewise, customers are unable to choose their own service providers. As a result, it is important for us as a collective to strive for the best possible experience for both parties in this potentially reluctant relationship. This can be achieved by implementing workflows that prioritize a positive experience for legitimate applicants while also making it difficult for malicious actors to exploit the system. The approach must take into account the sophisticated tactics used by fraudsters as well as the lack of

knowledge among legitimate users. Additionally, we cannot force good people to have to bind themselves to a commercial entity outside of an agencies jurisdiction just to interact with the government. The government needs to remain the lynchpin when it comes to establishing a trusted relationship with its people.

Updating IAL-1 for broader usability is a great start. However, IAL-1 needs to be more attainable, and different than IAL-2. However, as written in 800-63-4A (IDP), there are notable challenges in achieving equitable access and avoiding biometrics. Currently, the similarities of the rigors found in both assurance levels in this revision will likely not overcome the hurdles that many consumers encountered when forced into IAL-2 processes during the COVID-19 pandemic. Example of the unintended, real-world consequences are noted in this CNN Report when unemployment insurance agencies utilized technology that utilizes facial recognition to conform to the IAL-2 standard. In the article, Eva Vasquez from the Identity Theft Resource Center was quoted saying that when a state chooses to use a tool, they know it has a tendency to not work as well on some people. She thinks that a tool "starts to invade something more than privacy and get at questions of what society values and how it values different members' work and what our society believes about dignity."

There are better ways to accomplish a secure, equitable remote identity authentication process than what is represented in this draft. LNRS has provided commentary and suggestions to various areas of 800-63-4A IDP in the response workbook as requested. The fundamental sentiment of our responses is categorized and explained below to add context to our workbook responses and suggestion points.

Less Reliance on Documents and Biometrics in Identity Verification

By putting most of the weight of identity verification on an existing identity credential/document, the agency is merely repurposing an existing identity credential, just verified by another source (i.e., the DMV). As stated previously, if there has been a compromise with that existing credential, the effectiveness of that credential for successful identity proofing is gone. Additionally, criminals legitimize synthetic identities, though legitimate government credential providers and undetectable forged documents are big business for criminals; this is something NIST needs to consider when relying so heavily on document verification and association to identities.

Additionally, as written in this IDP, the only way to remotely verify an identity against document evidence is to still utilize biometric capture and matching to bind the evidence to the individual presenting the evidence. The reliance on document and biometric comparison does not need to happen, whether unsupervised or supervised remote, when an identity can be securely verified at the time of transaction by the agency with no reliance on that identity being 'pre-verified.' As you will see through our responses provided in the Excel spreadsheet, there are better ways to verify identities at the IAL-1 level. IAL-2 can and should still exist in its current form as a high-friction option. However, IAL-1 should be updated to provide low-friction, high-security, more inclusive remote identity proofing. This is what most benefit programs strive for across government.

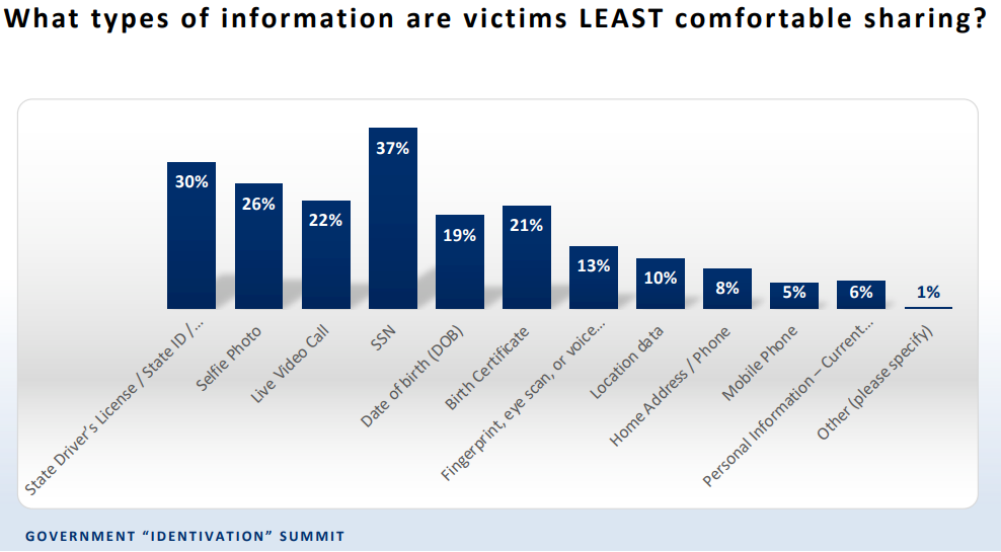
As written, the needs of the critical mass of users interacting with unsupervised government remote identity proofing processes has not fully been met as. A recent memorandum from the U.S. Department of Labor (DOL) DOL OIG Memorandum identifies the challenges when utilizing facial recognition in a workflow when there were a significant number of UI agencies that successfully prevented fraud and provided equitable identity verification without the need for facial recognition before, during, and post-pandemic.

Focus on Getting Automation Right Versus Reliance on Trusted Referees

In the case that a consumer cannot verify their identity through an automated process, the use of a Trusted Referee may reduce agency workload. The perceived effectiveness of the use of the Trusted Referee comes at a cost. For those individuals with no means to receive a passcode due to technological means or economic circumstances, or those whose gender identification and physical appearance contradict a driver's license photo, can be singled out and directed into a Trusted Referee workflow. For example, a transgender person may fail the biometric-document comparison as prescribed in the IAL-2 standard. In terms of remediation/assistance, forcing a transgender individual to interact with a Trusted Referee subjects them to additional scrutiny due to no fault of the applicant.

Additionally, we must face the facts that Trusted Referees are people who can make subjective decisions and introduce risk by way of compromising the applicants' sensitive PII. We understand that at some point, there may need to be manual intervention to help consumers through the process, but it is up to the industry to provide better automation versus more Trusted Referee options.

Based on a report from the *Identity Theft Resource Center* titled "Identification in a Post-Pandemic World, the Views of Consumers, Victims, & Government Execs" where they surveyed consumers, identity theft victims, and government executives, there are obvious concerns, particularly with those who have been victims of identity theft, with utilizing live video calls, state-issued ID's, selfie photos, and SSN's.



In conclusion, when it comes to equity, inclusion, and threat prevention, NIST has an excellent opportunity to provide a standard that can better serve government agencies and the people that depend on those agencies. There are proven approaches that government agencies depend on today that do not rely on document and biometric processes nor rely on Trusted Referees as their equitable access option. LNRS recommends that NIST consider these approaches in their standard to make true low-friction, equitable, and fraud-preventative experiences available for all government agencies to utilize.

Thank you,

Justin Hyde
Vice President
Government Market Planning
LexisNexis Risk Solutions

Topics that NIST is Specifically Interested in Receiving Comments and Recommendations

(Beginning on page ii in NIST SP 800-63A-4 ipd)

Identity Proofing and Enrollment

- **What technologies or methods can be applied to develop a remote, unattended IAL2 identity proofing process that demonstrably mitigates the same risks as the current IAL2 process?**
  - Based on what NIST has proposed with regard to enhancing IAL-1, IAL2 can remain with minimal changes to serve as an option for agencies that determine that they want to utilize a facial recognition-based solution. NIST should focus their non-biometrics standard on the IAL-1 workflow. Our suggestions for achieving appropriate identity verification measures are noted in the accompanying spreadsheet with our suggestions. Additionally, we suggest that some of the informative sections in the standard become normative to better prevent sophisticated fraud to the IAL-2 and IAL-1 workflows.

- **Are these technologies supported by existing or emerging technical standards?**
  - The LNRS security program is based on ISO 27002. The program uses the ISO family of standards as it is the primary framework of controls utilized by the majority of customers across a multitude of industry sectors. LNRS enforces the following compensating controls: strict access controls with quarterly entitlement reviews, strong network segmentation, a standard three-tier architecture model (web, app, DB) separated by hardened firewalls, active IPS/IDS and enterprise monitoring and logging, servers/databases/network infrastructure built on industry standard security configurations, full background checks for all employees, policies and procedures based on the ISO 27002 standard, yearly independent SOC2 Type II audits, and a robust computer incident response plan.

- **Do these technologies have established metrics and testing methodologies to allow for assessment of performance and understanding of impacts across user populations (e.g., bias in artificial intelligence)?**
  - The suggested approaches as noted in the accompanying spreadsheet, have been proven successfully effective across all types of industries including government, healthcare, financial, insurance, e-commerce, etc.

- **What methods exist for integrating digital evidence (e.g., Mobile Driver's Licenses, Verifiable Credentials) into identity proofing at various identity assurance levels?**
  - We are aware that ISO/IEC is making advancements on the ISO 18013-07 standard that supports the utilization of 'digital evidence' for remote identity proofing. We suggest that NIST includes digital birth certificates as they consider this approach.

- **Are there existing fraud checks (e.g., date of death) or fraud prevention techniques (e.g., device fingerprinting) that should be incorporated as baseline normative requirements? If so, at what assurance levels could these be applied?**

- Yes, there are fraud checks that should be incorporated as normative requirements. These include utilizing corroborative data to identify high-risk of various fraud types including synthetic fraud. Additionally, knowing what an identity and its attributes (physical and digital) should look like before the transaction occurs will know if there are anomalies indicative of fraud. We have made suggestions in the accompanying spreadsheet.

- **How might emerging methods such as fraud analytics and risk scoring be further researched, standardized, measured, and integrated into the guidance in the future?**
  - We recommend that NIST directs the standards away from the allowance of Artificial Intelligence. When an agency is making an important decision, transparency is key.

- **What accompanying privacy and equity considerations should be addressed alongside these methods?**
  - Unsupervised remote identity proofing is the most equitable form of identity verification; allowing for broad-based access without the downfalls that come with subjective, high-risk human interaction. Making sure it is done right without the use of biometrics or reliance on pre-verified identity credentials further supports equity and privacy. Data transparency and IAL options for agencies to choose how they can best work with the applicants they serve compounds the service equity to the populations they serve.

- **Is there an element of this guidance that you think is missing or could be expanded?**
  - We have noted areas that we think are missing or could be expanded in our Executive Summary and our accompanying spreadsheet's comments and suggestions. Most notable is around our thought that IAL-1 is a great opportunity for NIST to allow flexibility to agencies for an alternative, low friction, high equity workflow so long as the standard is architected in the best way.

- **Is any language in the guidance confusing or hard to understand? Should we add definitions or additional context to any language?**
  - Any language that we found confusing or hard to understand is noted in our accompanying spreadsheet's comments and suggestions.

- **Does the guidance sufficiently address privacy?**
  - The biggest privacy gap that we have noted is the reliance on Trusted Referees as the fallback in the case that people cannot or will not be identity verified remotely and unsupervised. Utilizing a real person opens up the door to identity embezzlement as well as subjective decisioning. Our concern here has been expanded in the Executive Summary and accompanying spreadsheet.