Comment Template for: NIST SP 800-63-4 Suite (Initial Public Draft)

Please submit responses to dig-comments@nist.gov by March 24, 2023

Organization:	*Easy Dynamics*
Name of Submitter/POC:	*Sarah Villarmarzo*
Email Address of Submitter/POC:	[REMOVED]

Comment #	Publication (Base, 63A, 63B, 63C)	Comment (Include rationale for comment)	Suggested Change
1	63-Base	Mobile Drivers' Licenses are a promising emerging technology that is starting to appear in practice. NIST should continue to monitor the technical specifications for this technology as described in emerging ISO and NISTIR publications, and update SP 800-63-4 as appropriate to align with these models.	Recommend continuing to work with the mDL standards teams to align forthcoming standards.
2	63-Base	Agencies can struggle with defining their own risk models in a federated environment where there is limited control over how risk scores are defined and assigned to applicants/subscribers. NIST may wish to add clarity or examples for what types of variables may go into defining a user risk score, perhaps not in this document but as supplemental guidance or through partnership with GSA. Having more standardization in understanding user risk will support interoperability efforts and federation analytics.	Recommend providing guidance on how to assign risk scores to users in a flexible and transparent scoring model.
3	63A	Defining demographic types would be helpful here. The January 2021 Executive Order On Advancing Racial Equity and Support for Underserved Communities Through the Federal Government has strong definitions here that could be leveraged.	Recommend referencing the White House memo on equity.
4	63A	CSPs should strive for continuous evaluation and improvement of their biometric algorithms to understand impact across demographic groups, refine anti-fraud models, etc.	Recommend including a requirement for CSPs to identify continuous improvement targets, subject to a privacy impact assessment.
5	63A	One challenge that has been discussed is whether NIST should set a security standard that will drive the market to meet it, or set standards around where the market is currently or is heading. We do not have an answer to this, but suggest that NIST take into account common practices across the identity field and seek to at least weigh in on how to manage risk while using these solutions. One example is the emergence of "behavioral biometrics" as a part of identity proofing processes as a risk-based alternative to 63A requirements. These solutions are largely untested, intentionally opaque, and have unknown outcomes such as pass rates, demographic impacts, user redress, and privacy impacts. While these solutions are not yet mature enough to be measurable secure and thus included as NIST requirements, since they are becoming more used in production across the government, NIST should seek to provide some type of guidance for agencies at least on what questions to ask these providers to	Recommend providing guidance on what risk factors to consider and what information to obtain from CSPs employing risk-based alternative approaches.
6	63B	There is a difference between federal regulations on phishing-resistant authenticators at AAL2 and the stated requirements. Most agencies can expect to include phishing resistance in their FISMA metrics moving forward to show progress on federal policy mandates. Making this a requirement would encourage CSPs to add this to their suite of authentication to make it easier for agencies with federated models to comply with these regulations.	Recommend making it a requirement at AAL2 to offer one phishing-resistant option.
7	63B	For the discussions on biometric performance within demographic types, it would be helpful for NIST to specify a threshold for acceptable performance. Do different groups need to be within x percentage points of another group's FMR and FNMR, for example? Is there the ability to account for improvement over time?	Recommend adding guidance on what constitutes acceptable levels of difference for biometric performance between demographic groups.
8	63C	To support supply chain clarity and security, CSPs should be required to provide a Software Bill of Materials (SBOM), including a Privacy SBOM detailing all components under the hood, including data types, exact data sources, and clear details around processing.	Recommend adding a requirement for CSPs to provide an SBOM.