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

Please submit responses to dig-comments@nist.gov by October 7, 2024.

Organization:	*Treasury*
Name of Submitter/POC:	*Mesay Kassa*
Email Address of Submitter/POC:	[redacted]

Comment #	Publication (Base, 63A, 63B, 63C)	Section	Page #	Line #	Comment (Include rationale for comment)	Suggested Change
1	All publications				General concern over the impact of the revamped risk management processes and metrics for continuous evaluation. This has the potential to increase the level of effort (LoE), both time and resources, to deploy digital identity solutions. For example, Treasury has hundreds of RPs that will be directly impacted with this change. This appears to be unfunded mandate.	Suggest a consideration around timelines to implement these added risk management requirements as they will take longer than the standard one year to implement. Understanding these are OMB mandates, however there may be opportunities for certain exceptions or as specifically directed by OMB.
2	63-Base	3	22-48	930	Requirement for GSA to update the Digital Identity Risk Management (DIRM) Playbook to coincide with the official release of NIST SP 800-63-v4 suite.	Suggestion is to release the final revision of NIST SP 800-63-4 in concert with and updated GSA DIRM Playbook.
3	63-Base	3.3.2.1	35	1358	Provide more details on an "IAL0" option since there no longer exists an option to identity proof through self asserted claims and to provide an option for agencies to better track and avoid future complexities with this pathway.	Bring back the following sentence from NIST SP 800-63-4 IPD: In addition to a “no identity proofing” level, IAL0, this document defines three IALs that indicate the relative strength of an identity proofing process.
4	63-Base	3	40	1526-1527	The new tailored process adds additional risk to an agency digital identity service as this advocates soloed Relying Party (RP) deployments. This impacts require agency to support soloed/one-off deployments, and unique Cybersecurity and Auditing assessments to ensure compliance. Additionally, agencies rely on common assurance levels that span their enterprise. Tailoring presents the potential loss of portability across an agency and federal government as customized deployments lack standard baseline controls. Without the ability to rely on common baseline controls there could be a large financial impact due re-identity assurance proofing for every tailored PR instance and CSPs are now required to track and address the difference as part of these tailored/customized deployments. The ability to tailor individual RP relationship will increase risks to agencies and CSPs will be require to support multiple RP instances and manage these unique deployments. These multiple RP deployments will increase risk and costs. *Referenced Statement: "In doing so, CSPs MAY offer and organizations MAY utilize tailored sets of controls that differ from the normative statements in this guidance."*	NIST 800-63 should mandate full compliance with the assurance levels baseline statements. The ability to tailored shall only allow for additional compensating or supplemental controls. Otherwise, without the reliance of common baseline assurance level controls agencies would see increased risks to identity management service. Suggestion is to restrict the tailoring to only the addition of compensating and supplemental controls. Do not permit the removal of xALs baseline controls/statements. Suggested Change: *"In doing so, **CSPs SHALL at the minimum meet normative xALs statements and RPs** MAY utilize tailored sets of controls that **compensate and/or supplement** normative statements in this guidance."*
5	63A	2.1.3	8	611-613	Due to the controls/requirements associated with Remote Unattended identity proofing process, it may not be a needed/requirement pathway if at least one attended identity proofing process option is available to the applicant. *Referenced Statement: "CSPs that offer IAL1 & IAL2 services SHALL provide a Remote Unattended identity proofing process and SHALL offer at-least one attended identity proofing process option."*	Suggest not requiring a Remote Unattended identity proofing process (at least for IAL1). *Suggested Change: "CSPs that offer IAL1 & IAL2 services **SHOULD** provide a Remote Unattended identity proofing process and SHALL offer at-least one attended identity proofing process option."*
6	63A	2.4.1.3	12	720-721	For Superior Evidence Requirements, enrollment should only be restricted to Onsite Attended (Not Remote Attended), given the risk factor involved. *Referenced Statement: "The issuing source had the subject participate in an attended enrollment and identity proofing process that confirmed their physical existence."*	Suggest limiting to only Onsite Attended enrollment. *Suggested Change: "The issuing source had the subject participate in an **onsite** attended enrollment and identity proofing process that confirmed their physical existence."*
7	63A	2.5.1	14	787-791	When describing the ability to conduct authentication and federation protocols as an identity verification method for both in person and remote, it would be helpful to clearly state all the identity proofing types this will be supported under. *Referenced Statement: "Authentication and Federation Protocols. The individual is able to demonstrate control of a digital account (e.g., online bank account) or signed digital assertion (e.g., verifiable credentials) through the use of authentication or federation protocols. This may be done in person, through presentation of the credential to a device or reader, but can also be done during remote identity proofing sessions."*	Suggest adding a clarifying statement on the identity verification methods that can be properly verified through this identity verification method. For example, is it only possible during attended remote sessions to be able to view the presentation of the credential or is there a pathway through an unattended remote session. *Suggested Change: "This may be done in person, through presentation of the credential to a device or reader **(i.e., attended, unattended)**, but can also be done during remote identity proofing sessions **(i.e., attended, unattended)**."*
8	63A	3.1.13.1	32	1387	Proofing Trusted Referees at lower IALs or not at all is a vulnerability in the identity proofing process. *Referenced Statement: "The CSP MAY offer trusted referee services for either onsite-attended or remote-attended sessions. These sessions SHALL be consistent with the requirements of these proofing types based on the IAL of the proofing event."*	Suggest adding back the statement from NIST SP 800-63A version 3 to ensure identity proofing process for trusted referee takes place at the intended IAL or higher as the applicant. *Suggested Change: "**The CSP SHALL proof the trusted referee at the same or higher IAL as the applicant proofing."***

9	63A	4.1.6	37	1552-1553	The use of confirming the applicants address assumes this can be both for both the physical and digital address options. *Referenced Statement: "Confirming the applicant's ability to return a confirmation code delivered to a validated address associated with the evidence;"*	Suggest adding physical and digital addresses as the two options when verifying applicants address associated with the evidence as the applicant may not have a physical address as an option available to them. *Suggested Change: "Confirming the applicant's ability to return a confirmation code delivered to a validated address **(i.e., physical, digital)** associated with the evidence;"*
10	63A	4.1.7 - 4.1.9	38-39	1568-1620	The following sections encompass requirements around (1) Onsite Unattended Requirements (Devices & Kiosks), (2) Onsite Attended Requirements, and (3) Remote Attended Requirements; the assumption is that these are all the possible options for IAL1 requirements (not the remote unattended pathway).	Suggest is to verify why the remote unattended pathway is not listed as an option under section 4.1 Identity Assurance Level 1 Requirements. If it is an option, it is recommended to have a section dedicated for it to be consistent with the other options listed.
11	63A	4.2	39	1646-1647	To ensure the below sentence is clear, it would be helpful to list all pathways for IAL2. *Referenced Statement: "IAL2 can be achieved through a number of different types of proofing (e.g., remote unattended, remote attended, etc.)..."*	Suggest changing this statement to the below: *Suggested Change: "IAL2 can be achieved through remote unattended, remote attended, onsite unattended, onsite attended types of proofing..."*
12	63A	4.2.1	40	1656-1657	Can the following statement be clarified a bit more on what the options are outside of section 2.1.3? *Referenced Statement: "Identity proofing at IAL2 MAY be delivered through any proofing type, as described in Sec. 2.1.3."*	Suggest changing MAY to SHALL or providing clarity on the MAY statement as to what the other proofing types could be used. Is it when the Trusted Referee plays a role in the decision making or when the CSP leverages combined proofing type pathways? *Suggested Change: "Identity proofing at IAL2 **SHALL** be delivered through any proofing type, as described in Sec. 2.1.3."*
13	63A	4.2.6.1	42	1707-1714	The use of the term "Non-Biometric" Pathway to describe processes that still involve biometric comparison is somewhat confusing. It is not immediately intuitive to the reader.	Suggest renaming 4.2.6 subsections to the following: **4.2.6.1 Manual Biometric Comparison Pathway** **4.2.6.2 Digital Evidence Pathway** **4.2.6.3 Automated Biometric Comparison Pathway**
14	63A	4.2.6.2	43	1735	The IAL2 Verification - Digital Evidence Pathway section does not include visually comparing the applicant's facial image to a facial portrait on evidence. We assume this is because some forms of digital evidence may have had automated biometrics match as part of the initial issuance of those digital documents/evidence. Similar to relying on a PIV certificate for verification where the cryptography on the certificate and associated infrastructure is relied upon to verify the applicant rather than comparison of biometrics present on the evidence.	Suggest adding the clarifying statement why the biometric comparison (e.g., visually, biometric capture) is not listed as an option here.
15	63A	4.3.8	47	1884-1885	The document describes the requirement to have a high resolution video transmission as part of this process, but it is unclear what that standard high resolution video should be. *Referenced Statement: "The CSP SHALL monitor the entire identity proofing session through a high-resolution video transmission with the applicant."*	Suggest adding details to the recommended high resolution video transmission, such as the minimum resolution needed, or referencing another publication/document that captures the requirement.
16	63A	7.4	59	2111-2124	As part of the guidelines for CSPs to redress issues that arise. CSPs should be responsible for notifying all impacted users and providing the relying party with a list of the impacted users and the status of their notification.	Recommend adding language for the notification of end users when an incident occurs resulting in the exposure of PII or user information. *Suggested Change: **"Prior to implementing new or adjusted capabilities in an effort to redress applicant complaints, the CSP SHALL notify all affected subscribers concerning the nature and impact of the change."***
17	63C	2.5 and 4.9	7 and 63	587-588; 2352-2353	Since AAL2 allows for phishing and non-phishing resistant options, it would be beneficial to identify if the subscriber authenticated at the compliant assurance level based on OMB M-19-17 and M-22-09.	Allow the assertion of AAL2 to include phishing and non-phishing resistant claims by policy.
18	63C	2.5	7	600	Given the changes in IALs, it will be beneficial to acknowledge that there could be a lower identity assurance level than IAL1. *Referenced Statement: "…assume the account meets "IAL1", the lowest numbered IAL described in this suite."*	*Suggested Change "…considered to have "no IAL" and the RP SHALL **assume "IAL0" for the account,** the lowest numbered IAL described in this suite."*
19	63C	3.7.1	25	1147	There is no notice for when the RP terminates an account.	Suggest to add a bullet for the subscriber notification of termination of accounts.
20	63C	3.11.1	32	1406-1407	Note, the private key (not the public key) is used to sign assertions. This is a global change across this volume.	Suggest replacing the public key with private key instead. *Suggested Change: "..such as by verifying that the **private** key used to sign the assertion is included in the signature of the attribute bundle."*
21	63C	3.13	36	1551-1553	Typo: *"Similarly, a bearer assertion reference can be presented **own its own** to the RP and used by the RP to fetch an assertion."*	Suggested Change: "SimilarlC27:G31 reference can be presented on its own to the RP and used by the RP to fetch an assertion."