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:	*Centers for Medicare and Medicaid Services (CMS)*
Name of Submitter/POC:	*Office of Information Technology (OIT) / Information Security and Privacy Group (ISPG)*
Email Address of Submitter/POC:	[redacted]

Comment #	Publication (Base, 63A, 63B, 63C)	Section	Page #	Line #	Comment (Include rationale for comment)	Suggested Change
1	63-Base	1.3.2	6	543	Extra space in "Organizations ,"	
2	63-Base	2.1	10	640	Extra dash in "Subscriber — - The"	
3	63-Base	2.1	10	646	Typo: "relyin party"	relying party
4	63-Base	3.4.2	43	1642	Typo: "CSPs and IDPs" -- IDP is written as "IdP" elsewhere	IdP
5	63-Base	3.7	50	1800	Typo: "TTPs that Could impact"... unneccessary capitolization of Could	TTPs that could impact
6	63-Base	Overall			I find the new font to be very pleasing to the eyes. Also, thank you for choosing a sans-serif font where capital i and the number 1 are distinct.	none
7	63-Base	3	23	1002	The inclusion of the 5th step of "Define the Online service" is great. This is foundational, and by encouraging teams to center why the service exists it will help them in the later steps pick the right tools and technology.	If Figure 6 could be closer to the list of the 5 steps that would be nice, but it looks hard to do.
8	63-Base	3			The clear statements of "output" for the 5 steps makes it clear what is expected of teams using this. Nice addition.	
9	63-Base	Overall			The team clearly put a lof of effort into making this document easier to read by rewriting significant portions in plain language. This decreased the amount of time I needed to read the document, I had fewer questions along the way, and I didn't need to keep looking things up in the glossary. Thank you and great work.	
10	63-Base	3.1	27		User Groups and Impacted Entities: These explanations are great, and the examples are clear. This is an improvement over the initial draft merely considering Individual and the Organization, and different individuals will have differen access and conerns.	
11	63-Base	3.2.4	33	1307	With the introduction of user groups, impacted individuals, and the advice on how to combine the impact level, Federal agencies could benefit from a workbook (or spreadsheet) to help them track these calculations. Otherwise, every agency will have to make their own, or more expensively, pay a contractor to do it. It would be similar to Table 1 in the Initial Public draft, but with room to expand on the User Groups as well as a couple of methods of combinatorial analysis.	Create a (separate) workbook for agencies to use to guide them through the impact levels for user groups.
12	63-Base	3.3.1	35-36		Tables 1-3 are really helpful! I love the clear objectives of what types of attacks/issues the controls are trying to prevent.	
13	63-Base	3.4.1	42	1592-15	Thank you for encourging agencies to talk to the entities and communities served! This kind of user feedback will help us make better IdPs.	
14	63-Base	3.4.1	42	1564-15	Thank you for expanding the Equity section to be more specific. This will help motivate teams who haven't been as engaged in making equitable services.	
15	63-Base	3.5.2	46		Table 4: Performance Metrics -- thank you for not just recommending that teams have performance metrics, but also giving teams a starting point. Staring at a blank page can be hard. All of the intent to make a usable and equitable product doesn't really matter if we are checking to see if it actually is either one.	
16	63-Base	3.5.3	48	1725	Thank you for adding in measuring for equity and accessibility, as well as reminding us to avoid collecting additional personal information because there are ways to get approximate comparisons.	
17	63-Base	3.6	48	1740	Thank you for adding the Redress section -- this is a valuable addition and one I hadn't considered, but people who use our services need a way to tell us if we've caused harm and we need to remedy it as best we can. Not being able to complete identity proofing may lead to a delay in benefits that could be more than inconvenient.	
18	63A	3.1.13.3	33	1412	Applicant reference should be limited to a small subset of users	I recommend that NIST provides addional guardrails or guidelines to ensure that referecnes used in the identity proofing process are of high integrity and capable of verifying an applicant's identity realiable. Without explicit guidelines, there is a risk of unqualified individuals serving as references, which could weaken the security of the RIDP process. NIST should explicitly define the types of acceptable references, such as licensed professionals (e.g. , doctors) , goverment officials or individuals recognized in leadership positions (e..g. Pastors, community leaders). This will enhance security by ensuring that references are vetted and capbale of providing trustworthy validation.
19	63A	4.1.7	38	1568	While video proofing is effective, it may not fully accommodate individuals with limited access to high-speed internet or necessary devices for video conferencing, thus raising concerns about Diversity, Equity, and Inclusion (DEI). Specifically, individuals in rural areas, low-income households, or those with disabilities may face challenges participating in video-based sessions.	Develop and include specific guidelines in the Remote Attended proofing section that outline processes for validating and verifying an individual's identity via phone calls. These guidelines should address security controls and mitigation strategies that account for the limitations of phone-based proofing. Including phone calls as a Remote Attended proofing option will ensure that identity verification processes are accessible to a wider range of individuals, thereby promoting DEI principles. Additionally, this alternative would serve as a practical backup method for users in the event of technological difficulties during video sessions.
20	63A	2.4	10	649	Provide more guidance on how CSPs should handle expired identity documents at IAL2, particularly for applicants from countries where document renewal may be slow or inaccessible. Allowing for more leniency in document expiration (with additional fraud controls) would improve accessibility without significantly increasing risks	Justification: Some individuals may face challenges in renewing their official documents, especially in certain jurisdictions or countries. Allowing expired documents with mitigating fraud checks can provide flexibility while maintaining security.
21	63A	A.2	80	2729	Incorporate Additional Forms of Identification	Expand the list of acceptable evidence documents at IAL2 to include community-based IDs, refugee documentation, or other non-traditional forms of identification to ensure equitable access to identity proofing for underserved populations.
22	63B	2.1.2 & 2.2.2	5 & 7	524 and 577	For AAL 1 "...implementation need not be validated under [FIPS140]" which implies that for AAL2 implementation SHALL be validated under [FIPS140]. However, nowhere in section 2.2.2 does it say that implementation SHALL be validated under [FIPS 140].	Either include a statement in section 2.2.2 that implementation SHALL be validated under [FIPS 140] or clarify that implementation for AAL2 also does not have to be validated under [FIPS 140].
23	63B	4.2.2.1	45	1766-1768	This sentence states that "...accounts at AAL1 are without identity proofing..." and therefore "...repeated identity proofing is not possible." The implication is that AAL1 aligns with "No identity proofing" in section 1.2 of 63A page 2 line 412 and not with "IAL1" in the same section of 63A (line 416) which does require identity proofing.	If AAL1 applies to both to 63A's No identity proofing and to IAL1 then 63B needs to say that with a section dealing with recovery for accounts with no identity proofing, where it makes sense to say "The CSP SHALL require the successful use of a saved recovery code, issued recovery code, or recovery contact." But then there should also be a separate section describing the recovery method for accounts at IAL1 which did undergo identity proofing (as indicated by 63A) and therefore could be subject to repeated identity proofing.
24	63B	5.2	51	1975 - 1977	The phrase "special considerations apply to session management and reauthentication" is stated at both the beginning and end of the sentence beginning on line 1975.	Delete one of the redundant clauses.
25	63B	3.2.2	29	1225	"Accepting only authentication requests from IP addresses from which the subscriber has been successfully authenticated before" IP spoofing is too easy for this to be a reasonal mitigation to use as throttling. The use of previously known IP addresses as a part of a risk-based techniques kinda covers this any way and is more useful.	Remove this suggestion
26	63C	2.5 Requesting and Processing xALs	7	592	Not clear on the statement "If the xAL is unchanging for all messages between the IdP and RP" - Can not think of a scenario where the IAL, AAL info will be same for all transactions. Can we add example where it will be same?	
27	63C	3.15 Bound Authenticators	38	1586	In the IDP managed bounded authenticator use case, does the IDP have to maintain the Authentication authenticators and FAL 3 bounded authenticators seperately?	

28	63C	3.15.2 Subscriber-Provided Bound Authenticator Binding Ceremony	40	1657-16	This section describes that a RP MAY allow a subscriber to bind multiple subscriber-provided authenticators but then on line 1392 it talks about asking the subscriber to present existing bound authenticator and after it is successful it will immediately prompt for the newly bound authenticator, this reads like replacing existing authenticator with a new one instead of adding another one which in support of "allowing multiple authenticators".	