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

Please submit responses to dig-comments@nist.gov by March 24 April 14, 2023

Organization:	*KnowBe4, Inc.*
Name of Submitter/POC:	*Roger A. Grimes*
Email Address of Submitter/POC:	[REMOVED]

Comment #	Publication (Base, 63A, 63B, 63C)	Section	Page #	Line #	Comment (Include rationale for comment)	Suggested Change
0	All	n/a	n/a	n/a	I just want to say what an excellent, excellent document this is. I really like it. It contains far more information than the previous edition, more examples, and is far more readable and actionable. My hat is off to everyone to help developed this draft. Just a job well done!	
1	63-Base	2	3	352	Internet is spelled with a lowercase i, as internet. These is likely due to the incorrect source recommendations, such as the AP Stylebook, that Internet should always be spelled with a lowercase i unless starting a sentence. This is incorrect. Internet with a lowercase i is a shortened form of internetwork, which means two joined internal networks. Internet, as written by everyone who helped invent the Internet began with an uppercase I and was always used with an uppercase I when referring to the global internetwork known as the Internet. Here is an explanation of the issue: https://en.wikipedia.org/wiki/Capitalization_of_Internet	Always spell Internet, when referring to the global Internet, with a capital I.
2	63-Base	2	3	357	Line is, "A digital identity is always unique in the context of a digital service...". I'm not sure "digital service" is the right concept. I've always thought that a digital identity is unique within a relied upon, shared, namespace, regardless of the number of services involved. Hence, an Internet email address is a unique digital identity within services that use the Internet's DNS service, but can be used by any service that wants to use the same name space for its identity management/labels.	Change wording to say, "A digital identity is always unique in the context of a shared, relied upon, namespace..."
3	63-Base	2.1	5	437	Lines 437-443 lists excepted subjects. Not sure if all excepted subjects are exampled.	Possibly add networks and services/daemons into the list of things this guide does not address.
4	63-Base	4.1	11	610	You mention "attribute" without first defining it in text (although it is defined in Section 3/Appendix A) and use "attribute" to mean "a-trib-bute" as well above. So, it's used twice in different ways. Could be confusing.	Define attribute prior or during first use or in previous section above
5	63-Base	4.31	17	730	This section is very good and lists the "traditional" authentication factors. It doesn't, however, mention the potentially hundreds of authentication factors that many CSP/RP/etc., use to make a risk determination about a particular authentication event (such as geometric attributes, behaviors, session fingerprint (i.e., OS, browser, etc.), behaviorial attributes, etc.). Today's sophisticated authentication session often involve dozens to hundreds of other less traditional traits of authentication.	
6	63-Base	4.31	18	783	Document states, "A biometric...". Is "biometric" equivalent to "biometric authenticator"?	Say "biometric authenticator instead"
7	63-Base	4.4	21	865	Document seems to be tying pseudonymity to federation. Is federation needed for pseudonymity?	Explore if federation is needed for pseudonymity
8	63-Base	5	23	938	Tailored is not defined. This term may be customary in the federal space and the intended audience may already know it...but if not, define. I guess is that tailored means customized?	Define "tailored" somewhere
9	63-Base	5.14	29	1155	Document states that failure to authentication subject may be due to "barriers" and lists mostly equity barriers. Most authentication failures will be do to usability issues and that either needs to have its own bulletpoint or the existing line updated to include usability first.	Include usability as a risk that can lead to false-negative authentication failure.
10	63-Base	5.2.2.2	32	1218	AAL3 requires "protocol resistant to phishing attacks". I think this is a GREAT idea!! However, does that imply impervious to all phishing attacks or just some attacks? If just some attacks, as it likely does, what types of attacks are or aren't allowed. Every authentication scenario can be successfully phished, but some authentication scenarios are very resistant to some forms of phishing. This is a subject I spend much time and research on and can provide more detail.	Decide if AAL3 is resistant to "some popular and common types of phishing attacks", or if AAL3 means resistant to all possible phishing attacks?
11	63A	5.1.6	21	880	Section deals with expiration periods of enrollment codes. Does the document need to consider enrollment codes sent via "chat" mediums like Slack or MS-Teams?	Consider whether it is acceptable for enrollment codes to be sent via a "chat" communication's channel, like Slack.
12	63A	5.1.8	22	905	Missing biometric example of voice/sound in the examples. Voice-recognition (poor as it may be) is a very common biometric attribute these days.	Consider adding "voice" as a common biometric example along with the other examples
13	63A	5.1.8	23	935	Document states that a false match rate SHALL be 1:10000 and false non-match rate must be 1:100. I don't believe any current technology meets this currently based on NIST's own testing. Examples include: https://nvlpubs.nist.gov/nistpubs/ir/2014/NIST.IR.8034.pdf and https://pages.nist.gov/frvt/reports/11/frvt_11_report.pdf and based on third party contest like http://www.vc-challenge.org/.	Review whether requiring 1:10000 and 1:100 accuracy rates would allow any biometric candidate to be approved.
14	63A	5.1.9.1	24	993	Current requirements for Trusted Referees does not include an IAL/AAL minimum requirement to prove who the Trusted Referree is.	Trusted Referees should meet the min IAL/AAL requirements of the levels they are being a trusted referee for.
15	63A	5.1.9.2	25	1003	Current requirements for Applicant References does not include an IAL/AAL minimum requirement to prove who the Applicant Reference is.	Applicant References should meet the min IAL/AAL requirements of the levels they are being an Applicant Reference for.
16	63A	5.3.1	26	1046	"Account lockout/rate throttling" is one of the primary ways to mitigate automated attack prevention examples	Add "account lockout/rate throttling" to automated attack prevention examples
17	63A	5.4.1	28	1096	"Account lockout/rate throttling" is one of the primary ways to mitigate automated attack prevention examples	Add "account lockout/rate throttling" to automated attack prevention examples
18	63A	5.5.8	31	1209	There is no requirement that CSP staff be IAL/AAL proofed to the level of the proofing they are doing themselves.	Require that CSP staff involved in proofing be proofed themselves to the same or higher IAL/AAL as the work they are performing.
19	63A	6.3.2	32	1280	There is no indication of how timely the termination must be done. Right now, someone could be terminated a year after the termination was required and still meet requirements. Since "stale" accounts are a huge problem in IdM, there needs to be a timeliness factor between when the subsciber should be terminated and when they are terminated.	Indicate a maximum timeperiod between when an account should be terminated and when it is terminated.
20	63A	7.1	38	1319	There is a lot of missing information and good, common examples missing from Table 3. Very weak table, not overly useful to most readers. I would be glad to help flesh out a better table if asked.	Table 3 needs major improving, missing lots of common elements and mitigations.

21	63A	9.4	50	1702	During post-enrollment period it could be helpful to educate subscriber about the different types of fraudulent attacks that could occur against their identity and authenticators.	Educate subscribers about the common types of attacks against their identity and authenticators, how to recognize those attacks, how to mitigate, and how to report. Seventy to ninety percent of successful attacks involve social engineering, we need to have CSPs and others better educate subscribers on how to recognize and mitigate common attacks.
22	63B	2	4	396	In general, ascribing "phishing-resistance" requirement to an AAL3 process only will allow weak authenticators to abound at AAL2.	Phishing resistance should be both a AAL2 and AAL3 requirement. We can differentiate by requiring stronger anti-phishing controls in AAL3 versus AAL2…but allowing phishing-susceptible authenticators in AAL2 is going to make AAL2 weaker than desired. I would be glad to have a longer discussion about this. Getting this wrong will significantly weaken 800-63-4 at a time when we need stronger authenticators for the average person and scenario and not allowed weaker ones.
23	63B	4.1.1	6	447	Permitted authenticator types do not include biometrics…is that a desired outcome? Biometrics are more discussed in AAL2 and AAL3, but does that mean biometrics are not acceptable as an AAL1 solution?	Discuss if biometrics are allowed in AAL1
24	63B	5.1.1	14	666	Memorized secret examples do not include pattern matching, which is a type of authentication available with Windows Hello (called a Picture Password) and often used on mobile device logons. It's still something the user knows…but isn't a password or a pin.	Consider if patching matching should be added as a memorized secret example.
25	63B	5.1.1.1	14	676	Document requires a minimum of 8-character passwords. Today, 8-character passwords are not considered adequate enough. The most common min. password length size is 12-characters for most environments. Today, I am frequently seeing human-created passwords up to 18-characters routinely guessed. Today, 12-characters is only acceptable if randomly-generated. If humans create their own passwords they need to be 20-characters or longer. I understand that no one wants to create or use 12-character randomly generated or 20-character human-created passwords...but that's the state of the art around password security these days. Sufficiently capable quantum computers will only make passwords weaker. I can discuss more if contacted.	Consider if 8-character passwords are long enough
26	63B	5.1.1.2	16	751	Is not the appropriate time to recommend quantum-resistant hashing algorithms? Some of the password hashes mentioned are quantum resistant and others aren't.	Consider if hashes need to be quantum-resistant or not, required or recommended.
27	63B	5.1.1.2	17	772	In the document it states that 10,000 rounds of PBKDF2 is enough. That used to be the case, but now is being significantly increased. Today's most common recommendations recommend 100,000 to 1,000,000 rounds. For example, OWASP recommends 600,000 rounds. See https://en.wikipedia.org/wiki/PBKDF2.	Discuss if 10,000 rounds of PBKDF2 considered enough these days.
28	63B	5.1.3.3	23	916	Presidential executive order (EO 14028) had a clarifying follow-up memo (https://zerotrust.cyber.gov/federal-zero-trust-strategy/#identity) that stated, "For routine self-service access by agency staff, contractors and partners, agency systems must discontinue support [emphasis added] for authentication methods that fail to resist phishing, such as protocols that register phone numbers for SMS or voice calls, supply one-time codes, or receive push notifications."	Discuss how PTSN, OTP, or push-based notifications can be used when a President executive order disallows it.
29	63B	5.2.3	32	1253	May want to include voice-recognition as an example of biometrics	May want to include voice-recognition as an example of biometrics
30	63B	5.2.3	33	1281	Document states that a false match rate SHALL be 1:10000 and false non-match rate must be 1:100. I don't believe any current technology meets this currently based on NIST's own testing. Examples include: https://nvlpubs.nist.gov/nistpubs/ir/2014/NIST.IR.8034.pdf and https://pages.nist.gov/frvt/reports/11/frvt_11_report.pdf and based on third party contest like http://www.vc-challenge.org/.	Review whether requiring 1:10000 and 1:100 accuracy rates would allow any biometric candidate to be approved.
31	63B	5.2.3	33	n/a	Not sure if applicable in this document, but it would be nice if all biometric solutions DIDN'T store a user's biometric trait in cleartext where it can be more easily copied and re-used if an attacker has access to the biometric trait database. Even better, the storage of biometric user traits should be obscured or hashed so that a stolen biometric database doesn't immediately result in compromise of a person's biometric trait for life. Give biometric trait storage the same security you give someone's password.	Decide if this document should recommend/require that user's biometric traits be stored in a non-plaintext format.
32	63B	5.2.5	34	1348	Document states, "…ability of an authentication protocol to detect…". Most phishing-resistant protocols do not detect phishing attacks. Most are designed to prevent such that common phishing attacks simply don't work when they are involved.	Remove the words, "...detect and...". Designed to prevent is enough.
33	63B	5.2.5	35	1366	Text states, "Two methods of phishing resistance are recognized…" There are more than two methods of phishing resistance. This section and related subsections need to be fleshed out a bit. For example another method is device binding, where authentication will not work unless coming directly from device where authentication session originated. Another would be number matching...doesnt' stop AitM attacks, but stops some times of phishing attacks. Another type of solution would be one where all logons are required to be initiated through a predefined SSO portal. I can discuss more if contacted.	Discuss if text should state that only two forms of phishing resistance is acceptable where there are more methods.
34	63B	5.2.8	37	1433	Text states that "OTP" devices are replay resistant. Time-based OTP normally are, but MAC-based OTP (HOTP) solutions are not by default.	Replace "OTP" with "TOTP" or "time-based OTP". Also, expiring authentication codes prevents replay attacks. I don't see mention of simply expiring authentication codes.
35	63B	6.1.2.3	44	1688	Text does not mention chat communication media channel, like Slack or MS-Teams, as a valid way to communicate. Chat-based mediums are becoming more popular than email in some organizations.	Consider if chat-based media needs to be added as an example communication channel
36	63B	8.1	52	1940	Table 3 is missing some threats, including: exploitation of coding vulnerabilty, misconfiguration, supply chain attack, trusted insider, etc.	I'll be glad to discuss more inclusive threat modeling if contacted.
37	63B	8.1	54	1940	Social engineering should include push-based fatigue attacks	Social engineering should include push-based fatigue attacks
38	63B	8.1	54	1940	There are many other types of social engineering attacks, such as redirecting an end-user to a fake site and duplicating the authentication experience, which then fakes the user into thinking they have successfully authenticated, and into revealing further secrets. Here are some other phishing examples: https://www.linkedin.com/pulse/phishing-resistant-mfa-does-mean-un-phishable-roger-grimes	I'll be glad to discuss more inclusive threat modeling if contacted.
39	63B	8.3	58	1962	I love this section, but it only describes the problem. It doesn't make any recommendations. I would say something like, "Ensure that a subscriber losing control of a legitimate authenticator can regain control or setup a new authenticator without needing to set up a new identity account.	I would say something like, "Ensure that a subscriber losing control of a legitimate authenticator can regain control or setup a new authenticator without needing to set up a new identity account.
	63B	General	n/a	n/a	Document frequently refers to OTP as if they are all time-based OTPs. Some OTPs are MAC-based or Event-based OTPs (HOTPs) and they operate differently. Many of the observations and recommendations made about OTP assume all OTPs are TOTP…but don't apply to HOTPs.	Review where OTP is used and make sure it applies to all OTPs and not just TOTPs. Many times OTP is the correct usage, but other times the context is referring ONLY to TOTPs and does not include HOTPs, and vice-versa.

	63B	General	n/a	n/a	Does document need to mention and recommend crypto-agility, so that if a cryptographic update is needed, it can be more easily done so by the vendor and user? This is becoming a very big issue as post-quantum cryptography is getting ready to be needed to replace existing quantum-susceptible cryptography.	Recommend crypto-agility of cryptographic components
	63B	General	n/a	n/a	Voice-based biometrics seems omitted throughout the document when biometrics are being discussed. Is that intentional?	Does voice-based biometrics need to be discussed?