#	Organization/ Submitter Name (required)	Type*	Page # (req'd)	Document #	Section #	Comment/Rationale (required)	Proposed Change (required)
1	Google	ge	24	63A	7. Threats and Security Considerations	Need to ensure the doc stays current with new and emerging threats.	Would like to see the section be updated based on 2020 current and emerging threats, for example to include digital mailers, and other new threat areas. A place to look could be the OWASP top 10 for 2020.
2	Google	te	29	63A	8.6. Agency Specific Privacy Compliance	Need to add clarification that it's important to have awareness and understanding of the purpose.	**Add text "of the purpose":** "Due to the many components of digital authentication, it is important for the SAOP to have an awareness and understanding **of the purpose** of each individual component."
3	Google	te	5	63B	4. Authenticator Assurance Levels	Replace SHOULD with MAY as a CSP may want to give a re-enrolled subscriber their previous ID, but also may want to give the option to have a new ID. This would require the establishment of a new identifier for a given subscriber, if a new ID is desired. This gives the subscriber and/or CSP flexibility on subscriber ID.	**Modify:** "Subscriber identifiers SHOULD NOT be reused for a different subject but **SHOULD** be reused when a previously-enrolled..." **To:** "Subscriber identifiers SHOULD NOT be reused for a different subject but **MAY** be reused when a previously-enrolled..."
4	Google	te	5	63B	4. Authenticator Assurance Levels	Delete this paragraph as what's written - any CSP that collects (even self-asserted) "personal information" would have to use multi-factor authentication. According to the definition of "personal information" in Appendix A of 800-63-3, this would include CSPs that log the IP address of subscribers, collect names or profile photos - in other words virtually all CSPs.	**Delete paragraph:** "~~**At IAL1, it is possible that attributes are collected and made available by the digital identity service. Any PII or other personal information — whether self-asserted or validated — requires multi-factor authentication. Therefore, agencies SHALL select a minimum of AAL2 when self-asserted PII or other personal information is made available online.**~~"
5	Google	te	7	63B	4.2.1 Permitted Authenticator Types	Add another bullet point "Multi-Factor Out-of-Band Device" as the security provided by an (on-device) multi-factor cryptographic software and an multi-factor out-of-band device is equivalent (just like for AAL1 single-factor cryptographic software and out-of-band devices are already considered equivalent in this document). See proposed edits in Section 5.1.3 for the definition of a "multi-factor out-of-band device".	**Add a bullet:** "• Multi-Factor OTP Device (Section 5.1.5) • Multi-Factor Cryptographic Software (Section 5.1.8) • Multi-Factor Cryptographic Device (Section 5.1.9) • **Multi-Factor Out-of-Band Device (Section 5.1.3)"**
6	Google	te	11	63B	4.5. Summary of Requirements	Add text MF Out of Band Device as an additional item in the list	**Add text "MF Out-of-Band Device": "MF Out-of-Band Device** MF OTP Device; MF Crypto Software; MF Crypto Device; or Memorized Secret plus:..."
7	Google	te	13	63B	5.1.1.2 Memorized Secret Verifiers	Most providers truncate of white space at the beginning and at the end of secret.	**Modify: "Truncation of the secret SHALL NOT be performed."** **To: "Truncation of white space at beginning and end of secret MAY be performed."**
8	Google	te	15	63B	5.1.1.2 Memorized Secret Verifiers	Replace all "key derivation function" with "password hash" in the paragraph as NIST specifies key derivation functions (e.g. in SP 800-108) and they are not suitable in this context. Password hashing is a separate primitive and NIST should not confuse them. The naming of PBKDF2 is unfortunate, but it's better to stem the conflation.	**Change to:** Verifiers SHALL store memorized secrets in a form that is resistant to offline attacks. Memorized secrets SHALL be salted and hashed using a suitable one-way **password hash**. **Password hashes** take a password, a salt, and a cost factor as inputs then generate a password hash. Their purpose is to make each password guessing trial by an attacker who has obtained a password hash file expensive and therefore the cost of a guessing attack high or prohibitive. Examples of suitable **password hashes** include Password-based **password hash** 2 (PBKDF2) [SP 800-132] and Balloon [BALLOON]. A memory-hard function SHOULD be used because it increases the cost of an attack. The **password hash** SHALL use an approved one-way function such as Keyed Hash Message Authentication Code (HMAC) [FIPS 198-1], any approved hash function in SP 800-107, Secure Hash Algorithm 3 (SHA-3) [FIPS 202], CMAC [SP 800-38B] or Keccak Message Authentication Code (KMAC), Customizable SHAKE (cSHAKE), or ParallelHash [SP 800-185]. The chosen output length of the **password hash** SHOULD be the same as the length of the underlying one-way function output.

9	Google	te	15	63B	5.1.1.2 Memorized Secret Verifiers	The Argon2 family of password hashes is widely recommended and best in class. NIST should not limit industry best practices.	**Modify:** "The key derivation function SHALL use an approved one-way function **such as** Keyed Hash Message..." **To:** "The key derivation function SHALL use an approved one-way function **such as but not limited to** Keyed Hash Message..."
10	Google	te	17	63B	5.1.3 Out-of-Band Devices	This type of on-device-prompt 2nd factor mechanism is common and in practice more secure than SMS (https://security.googleblog.com/2019/05/newresearch-how-effective-is-basic.html), which is already a accepted 2nd factor for AAL2. It should therefore also be an acceptable AAL2 authenticator type.	**Add a bullet:** "...• The claimant compares secrets received from the primary channel and the secondary channel and confirms the authentication via the secondary channel. **• The claimant approves on the out-of-band device the authentication session that is being established on the primary channel. The approval message is submitted via the secondary channel."**
11	Google	te	17	63B	5.1.3.1 Out-of-Band Authenticators	Delete this paragraph since there are a lot of references to PSTN. Major lockscreen show the SMS. It contradicts what is written in the document.	**Delete paragraph: "~~If a secret is sent by the verifier to the out-of-band device, the device SHOULD NOT display the authentication secret while it is locked by the owner (i.e., requires an entry of a PIN, passcode, or biometric to view). However, authenticators SHOULD indicate the receipt of an authentication secret on a locked device.~~"**
12	Google	ge	18	63B	5.1.3.1 Out-of-Band Authenticators	Add pictures for clarity in this paragraph	
13	Google	te	18	63B	5.1.3.1 Out-of-Band Authenticators	This type of on-device-prompt 2nd factor mechanism is common and in practice more secure than SMS (https://security.googleblog.com/2019/05/newresearch-how-effective-is-basic.html), which is already a accepted 2nd factor for AAL2. It should therefore also be an acceptable AAL2 authenticator type.	**Add a bullet:** "• The authenticator SHALL present a secret received via the secondary channel from the verifier and prompt the claimant to verify the consistency of that secret with the primary channel, prior to accepting a yes/no response from the claimant. It SHALL then send that response to the verifier. **• The authenticator SHALL present information pertinent to the authentication session (for example, geographic location of the device connected to the verifier over the primary channel) and prompt the claimant to verify the consistency of this information with the primary channel prior to accepting a yes/no response from the claimant. It SHALL then send that response to the verifier."**
14	Google	te	19	63B	5.1.3.3 Authentication using the Public Switched Telephone Network	It is important to include "infrastructure compromise" in the list of risk indicators as PSTN does not provide end to end protection for eavesdropping.	**Modify:** "Verifiers SHOULD consider risk indicators such as device swap, SIM change, **number porting, or** other abnormal behavior before using... **To:** "Verifiers SHOULD consider risk indicators such as device swap, SIM change, **number porting, infrastructure compromise or** other abnormal behavior before using...
15	Google	te	19	63B	5.1.3.4 Multi-factor Out-of-Band Authenticators	Multi-factor out-of-band authenticators are an attractive authentication mechanism for AAL2, since they don't require the user to remember a password. The user would simply interact with their phone other other device playing the role of the multi-factor OOB authenticator, but we get the same security as a two-factor authentication (similar to the multi-factor crypto software and multi-factor crypto device already permitted in AAL2).	**Add a clause: 5.1.3.4 Multi-factor Out-of-Band Authenticators A multi-factor out-of-band authenticator operates like an out-of-band authenticator, but requires the user to provide a "something you know" or "something you are" factor before displaying the authenticator secret (when transferring it from the secondary to the primary channel), sending the secret to the verifier (when transferring the secret from the primary channel to the secondary channel), or sending an approval message (when no secrets are being transferred and the user is simply approving the authentication on the authenticator).**
16	Google	te	19	63B	5.1.4 Single-Factor OTP Device	Phishing of OTP has existed for a while, there are open source phishing framework with OTP support and talks at RSA and Usenix conferences covering this (https://www.rsaconference.com/industry-topics/presentation/anatomy-of-phishing-campaigns-a-gmail-perspective).	**Add a caveat: "Use of single-factor OTP as described in the section is vulnerable to verifier impersonation and should be considered RESTRICTED as described in Section 5.2.10. Verifiers SHOULD consider phishing risks and consider additional mechanism to attempt to detect man-in-the-middle attacks"**

17	Google	te	20	63B	5.1.5 Multi-Factor OTP Devices	Phishing of OTP has existed for a while, there are open source phishing framework with OTP support and talks at RSA and Usenix conferences covering this (https://www.rsaconference.com/industry-topics/presentation/anatomy-of-phishing-campaigns-a-gmail-perspective).	**Add a caveat: "Use of single-factor OTP as described in the section is vulnerable to verifier impersonation and should be considered RESTRICTED as described in Section 5.2.10. Verifiers SHOULD consider phishing risks and consider additional mechanism to attempt to detect man-in-the-middle attacks"**
18	Google	te	22	63B	5.1.7 Single-Factor Cryptographic Devices	This is an important additional concept for this section	Add to the draft text for this section content about "Direct connection" suggests that, of the commonly used transports, only USB is permitted. However, allowing mobile devices (that otherwise meet all the requirements) to be used over BLE and local-networks will promote the use of these authenticators over passwords."
19	Google	te	24	63B	5.1.9.1 Multi-Factor Cryptographic Device Authenticators	This is an important additional concept for this section	Add to the draft text for this section content about "Direct connection" suggests that, of the commonly used transports, only USB is permitted. However, allowing mobile devices (that otherwise meet all the requirements) to be used over BLE and local-networks will promote the use of these authenticators over passwords."
20	Google	te	25	63B	5.2.2 Rate Limiting (Throttling)	Add per hour as a way of bounding detecting DoS attacks.	**Add text "per hour":** "...attempts on a single account to no more than 100 **per hour**."
21	Google	te	27	63B	5.2.3 Use of Biometrics	A reasonable cap on attempts needs to be established. This limit needs to be set by each organization based on their risk profile and documented in policy.	**Modify:** "• Impose a delay of at least 30 seconds before the next attempt, **increasing exponentially** with each successive attempt..." **To:** "• Impose a delay of at least 30 seconds before the next attempt, **upto a limit of additional attempts as set by the organization's policy,** with each successive attempt..."
22	Google	te	28	63B	5.2.5 Verifier Impersonation Resistance	The current wording is ambiguous as to the definition of verifier impersonation: some sentences seem to suggest it means phishing, some sentences seem to suggest something stronger. The protocol requirements and examples given for resisting verifier impersonation in the current document support the stronger definition of verifier impersonation. This has the effect that none of the current AALs cover phishing resistance: AAL1 and AAL2 don't require it, and AAL3 requires something stronger than phishing resistance. This stronger threat model currently implied by AAL3, however, is one that authentication alone cannot address. It therefore makes more sense for AAL3 to require phishing resistance, and not more (which is something that authentication *can* address). The proposed clarified definition for Verifier Impersonation Resistance achieves this goal by distinguishing it from stronger, less meaningful, threat models.	**Replace the entire section 5.2.5 with the text below.** 5.2.5 Verifier Impersonation Resistance 5.2.5.1 Definition Verifier impersonation attacks, sometimes referred to as “phishing attacks,” are attempts by fraudulent verifiers and RPs to fool an unwary claimant into revealing, to an impostor verifier (for instance a website), information or secrets that would allow the impostor verifier to authenticate as the claimant to the verifier. Authentication protocols that possess Verifier Impersonation Resistance detect the presence of such an impostor, and deny them the ability to authenticate as the claimant to the verifier. 5.2.5.2 Preventing Verifier Impersonation A verifier-impersonation-resistant authentication protocol SHALL strongly and irreversibly bind the authenticator output to the party with which the claimant is interacting (e.g., by signing over a key, name, or other property that identifies that party). The verifier SHALL validate the signature or other information used to prove verifier impersonation resistance against its own key, name, or other property, thus establishing that the claimant didn’t interact with, and potentially revealed authentication secrets to, an impostor. This prevents an impostor verifier from replaying that authentication on a different authenticated protected channel. Approved cryptographic algorithms SHALL be used to establish verifier impersonation resistance where it is required. Keys used for this purpose SHALL provide at least the minimum security strength specified in the latest revision of SP 800-131A (112 bits as of the date of this publication).

23	Google	te	38	63B	7.1.1. Browser Cookies	The __Host- prefix enforces: a) the secure flag, b) that no domain override is set, and c) that the path is /. This is a common set of best practices. The SameSite property limits exposure to cross-domain request forgery attacks and, while SameSite=Lax is quickly becoming the default in browsers, it remains a good idea to set it explicitly.	**Add a point:** "1. SHALL be tagged to be accessible only on secure (HTTPS) sessions. 2. SHALL be accessible to the minimum practical set of hostnames and paths. 3. SHOULD be tagged to be inaccessible via JavaScript (HttpOnly). 4. SHOULD be tagged to expire at, or soon after, the session's validity period. This requirement is intended to limit the accumulation of cookies, but SHALL NOT be depended upon to enforce session timeouts **5. SHOULD have the '__Host-' prefix and set 'Path=/'.** **6. SHOULD set SameSite=Lax or SameSite=Strict**."
24	Google	ge	51	63B	10.1. Usability Considerations Common to Authenticators	Remove pronouns for readability and applicability	**Modify:** "...(e.g., the number of times a user has to authenticate, the steps involved, and the amount of information **he or she has to** track)." **To:** "...(e.g., the number of times a user has to authenticate, the steps involved, and the amount of information **being tracked**)."
25	Google	te	5	63C	4 Federation Assurance Levels	Additional clarity that RP should be able to request a certain level of FAL to IdP and if not presented in the response, the RP can make the decision to grant lower privileges.	**Add text: "IdPs SHOULD support a mechanism for RPs to specify a particular FAL either at runtime as part of the request, or statically when the RP is registered with the IdP.** Regardless of what the RP requests or what the protocol requires, the RP can easily detect the FAL in use by observing the nature of the assertion as it is presented as part of the federation protocol."
26	Google	ge	6	63C	4.2 Runtime Decisions	Define the references before they are used, for readability and clarity.	**Add text "See Authorizing Party in Section 5.1.2":** "...the IdP without a runtime decision from the subscriber - **see Authorizing Party in Section 5.1.2** ."
27	Google	te	6	63C	4.2 Runtime Decisions	In order to target, suggest having this triggered by a subscriber request.	**Modify:** "IdPs **SHALL** make whitelists available to subscribers..." **To:** ""IdPs **SHALL upon request** make whitelists available to subscribers..."
28	Google	te	14	63C	5.3 Reauthentication and Session Requirements in Federated Environments	IdP's only share time of authentication events when the RP request includes a max age parameter.	**Modify:** "The IdP SHALL communicate any information it has regarding the time of the latest authentication event at the IdP**, and the RP MAY use this information in determining its access policies**." **To:** "Modify: "The IdP SHALL communicate any information it has regarding the time of the latest authentication event at the IdP **when the RP requests information as part of the authentication**."
29	Google	ed	15	63C	6. Assertions	Add normative language since just adding a value identifying the assertion doesn't prevent replay unless the RP actually checks it.	**Modify:** "6. Identifier: A value uniquely identifying this assertion, **used to prevent attackers from replaying prior assertions**." **To:** "6. Identifier: A value uniquely identifying this assertion, **which RPs MAY use to prevent attackers from replaying prior assertions**."
30	Google	te	15	63C	6. Assertions	IdP's only share time of authentication events when the RP request includes a max age parameter.	**Delete bullet:** "All assertions SHALL include the following assertion metadata:... ~~**8. Authentication Time: A timestamp indicating when the IdP last verified the presence of the subscriber at the IdP through a primary authentication event (if available)**~~." **Add bullet: "**Assertions MAY also include the following information:... **8. Authentication Time: A timestamp indicating when the IdP last verified the presence of the subscriber at the IdP through a primary authentication event (if available)**."
31	Google	ed	18	63C	6.2.3. Encrypted Assertion	Add text as the current sentence contradicts the definition of FAL1 by not excluding it. This is more appropriate for a SHOULD clause given that FAL1 has been excluded.	**Modify:** "When assertions are passed through third parties, such as a browser, the actual assertion **SHALL** be encrypted. **To:** "At FAL2 and FAL3, assertions passed through third parties, such as a browser, **SHOULD** be encrypted.

32	Google	ed	18	63C	6.2.3. Encrypted Assertion	Add text as the current sentence contradicts the definition of FAL1 by not excluding it. This note is not required if this is a SHOULD clause.	**Delete text: "~~Note: Assertion encryption is required at FAL2 and FAL3~~."**
33	Google	ge	19	63C	6.3.2 Pairwise Pseudonymous Identifier Generation	Add additional text to account for situations that have not been covered for Section 6.3.2	The following situations will arise in pseudonymous identifier generation. These situations have not been accounted for in the current text and should be included. Please add text for these areas, and recommendations are below: **Case 1:** Is the IdP allowed to return the pseudonymous subscriber ID to the RP if the RP authenticates itself and presents the global subscriber ID? **Case 2:** If case 1 is allowed, this would be an important tool for use in things like account recovery and support cases which are initiated by the subscriber at the RP. Subscribers will not typically know their own pseudonymous IDs and wouldn't want to re-identify using psuedonymous IDs (i.e. that could be hazardous). The system has a deliberate feature where identity reversal is not possible and users desire the impossibility of pseudonymous ID being re-identified (undesired re-association to an individual) **Case 3:** Illegitimate account recovery. Malicious or uncalled account recovery
34	Google	ge	19	63C	6.3.2 Pairwise Pseudonymous Identifier Generation	Add additional text to account for situations that have not been covered for Section 6.3.2.	Please add additional text to provide clarity on the following: • Merging of user IDs may be beneficial • However, that is not always what users desire • Users should be aware of well intentioned unification of user IDs For example, when a new relationship arises between RPs, the IdP MAY provide a mapping between both RPs' pseudonymous identifiers. These aspects have not been addressed in the current text.
35	Google	te	20	63C	7. Assertion Presentation	To provide clarity that the risk assessments are not required at runtime on every identity check.	**Modify:** "RPs SHALL conduct a privacy risk assessment when **determining which attributes to request**." **To:** "**During design,** RPs SHALL conduct a privacy risk assessment when determining which attributes to request."
36	Google	ed	23	63C	7.3. Protecting Information	SHOULD is a better fit here. All IdPs don't support attribute references across the board. Providers have support for some references, not all. Therefore recommendation to turn this into a should clause.	**Modify:** "The RP **SHALL, where feasible, request attribute** references rather than full attribute values as described in Section 9.3. The IdP **SHALL** support attribute references." **To:** "The RP **SHOULD request attribute** references rather than full attribute values as described in Section 9.3, **when the IdP supports attributes via references**. The IdP **SHOULD** support attribute references."
37	Google	te	29	63C	9.4. Agency-Specific Privacy Compliance	Understanding the main overall building blocks and how they fit together is reasonable and should be sufficient.	**Modify:** "**Due to the many components** of digital authentication, it is important for the SAOP to have an awareness and understanding of each individual component." **To:** "**each high level component** of digital authentication, it is important for the SAOP to have an awareness and understanding of each individual component."
38	Google	te	34	63C	10.2.2 User Perspectives of Trust and Benefits	Dialog and alerts should be used with care, users that are trained to click through any dialogue box reduce or eliminate the efficacy of a control.	**Add text "or click training":** "...and frequency of notifications is necessary to avoid thoughtless user **click-through or click training**."
39	Google	ed	34	63C	10.2.2 User Perspectives of Trust and Benefits	Added the term easily to make the update a user friendly process.	**Add text "easily":** "o Allow users to **easily** update their consent to their list of shared attributes."
40	Google	te	38	63C	11.3. OpenID Connect	Change including to may include but not limited to since returning this information depends on the permissions granted by the user, and the IdP is not required to implement support for all of these scopes.	**Modify:** "...representing a set of attributes about the subscriber, **including** but not limited to their name,..." **To:** ""...representing a set of attributes about the subscriber, **which may include** but not limited to their name,..."