NIST SP 800-63-3 Comments

#	Commenter	Reference	Comment	Category
1	IRS	63-3 - General	Overall this document lacks proper structure & organization. It tends to become very verbose and incoherent. As an example, the Executive Summary takes 5 pages, and it is more of an introduction to authentication than a focus on the guidance for Assurance Level. In fact the Exec Summary and Introduction have both overlapping concepts. The main theme of the guidance in this doc is the Assurance Level, but it has not been formally defined anywhere. The "definition" and usage are repeated all over the document with a new twist each time, and yet leaving it incomplete. Our recommendation would be to have this "Assurance Level" as a whole Section before describing the model in Sec 4.	10. N/A
2	IRS	63-3 - General	The definitions specific to this document should be defined in text, not only in the appendix. This should include standardized definitions for the terms: redress, identity provider/credential service provider.	10. N/A
3	IRS	63-3 - General	Parallels against new NIST documents including the Privacy Framework should be established to align terminology and concepts. At a minimum the Privacy Framework should be referenced as an acceptable set of controls. In particular, more emphasis on attribute referencing during the validation stage should be included.	1. Privacy enhancements
4	IRS	63-3 - General	The risk assessment section should be aligned against the ICAMSC DIRA working group outputs. In general they did a good job aligning their output to this document; but they used a set of terminology, for instance, that may be considered for use.	9. Additional controls
5	IRS	63-3 - General	Agencies still struggle with understanding their abilities and limitations with regards to the risk-based decision. We believe the language is pretty clear, but could this section potentially be moved higher and/or more prominent in the document?	10. N/A
6	IRS	63-3 - 4 Digital Identity Model	4.1 Overview: This not quite an overview but a detailed description of the whole model. The model is weak and does not help to explain how does it support the 3 assurance levels (IAL, AAL, FAL). It uses many paragraphs to describe the authentication concepts , but rarely refer to the model shown in the diagram. There is no graphic to capture the process of authentication or the sequence of basic operations performed by the model.	10. N/A
7	IRS	63-3 - 4.3 Authentication and Lifecycle Management	Not clear how do the various subsections relate to the title of Sec 4.3. There is nowhere life cycle (LC) defined, graphically or otherwise. The companion doc 800-63B (79 pages), exclusively devoted to this functionality , does not capture this definition even in its over 79 pages. The reader still does not know what are the various stages of this LC. 800-63B also has instances of sloppy writing with logical inconsistencies.	10. N/A
8	IRS	63-3 - 4.3.3 Authentication Process	The "Process" does not depict the process as a workflow, but uses four paragraphs only to confuse the reader.	10. N/A
9	IRS	63-3 - Section 5.3.1	Clarify the general expectation that, if the business process requires a signature on a paper form, it needs an authenticated submitter in the electronic transaction. (in IRS context, cf. our e-Signature policy)	1. Privacy enhancements
10	IRS	63-3 - Section 5.4	Section 5.4 describes Risk Acceptance and Compensating Controls. Clarify that, as part of the process of evaluating the process, the assessed xAL should consider all risks prior to determining mitigating factors, such as the examples in Section 5.3.1. We recommend that the assessed xAL consider all data, in both directions of the information exchange, but continue to allow the agency discretion on determining an implementation xAL, based on protections and mitigations.	1. Privacy enhancements

11	IRS	63-3 - Section 6 Selecting Assurance Levels	The process flows should be provided as informative. While these can certainly help to standarize risk assessment across applications their inclusion as normative guidance implies they must be used. Whereas these do not consider additional considerations that may be specific to agency legislative and regulatory environments. These should be labeled as informative models that may be used by agencies to inform their assurance level selection.	10. N/A
12	IRS	63-3 - Section 6 Selecting Assurance Levels	The chart for how to determine an agency's assurance levels should change - most low impact systems are currently going to IAL-2. They should go to IAL-1. See comments in 63A around updating IAL-1 to a more robust set of criteria.	9. Additional controls
13	IRS	63-3 - Appendix A-Definitions and Abbreviations, Page 42, "Authoritative Source".	Agencies need more guidance regarding what would make a source "authoritative". For instance, a source might need to explain: + "chain of custody", showing how they can trace back the data to the actual issuing authority + data refresh rate + security controls to ensure accuracy + privacy controls on the data + authorty by which the information is captured + attestation to the legality of the data capture + potentially more... This is of particular concerns where access to the issuing authority is out of the question. Such guidance could appear in the overview or in the IAL volume (63A), however, the current document set only defines "authoritative source" within the overview document.	10. N/A

NIST SP 800-63A Comments

#	Commenter	Reference	Comment	Category
1	IRS	63A - General	Consideration for international documents should be included in the description for how to determine the strength of different evidence types.	9. Additional controls
2	IRS	63A - 4.2.10 General Requirements	While 63A lists several fraud mitigation measures (4.2.10) - there is an opportunity for CSPs and RPs to reap more of the benefits of technical innovations in this regard. Over the past few years vendors have delivered continued innovation on for instance device fingerprinting and behavorial biometrics, feeding into an overall transaction risk score. And while the FAQ (QA-B02) acknowledges both the innovation as well as the issue with defining requirements in the context of Authentication, our suggestion is to include more firm language that allows CSPs and RPs to deploy fraud mitigation measures as part of their Acceptance Statements (63 5.4 and 5.5) , for instance through the introduction of the concept of risk scoring.	8. Verifier impersonation resistance
3	IRS	63A - 4.3 Identity Assurance Level 1	NIST should reconsider the Identity Assurance Level Requirements. 63A was written and published in a time when the natural "goldilocks" options were: Self-Asserted; Online proofed; or In person proofed. However, especially with the advent of fully remote government services, the new goldilocks as represented by the three identity assurance levels needs to shift to inlude a low risk online or in person option, a moderate risk online or in person option, and a high risk online or in person option. Currently, the first item is lacking - there is no true low-risk option either online or in person. We suggest heightening the security of IAL-1 as an opportunity to create meaningful low level of security. This could potentially include resolution and verification of evidence without the validation/PAD requirement; or collection of more evidence of lesser strength. Self-asserted, non-verified attributes could either be an IAL-0 or not included in the standard.	9. Additional controls
4	IRS	63A - 4.4.1.2 Evidence Collection Requirements Implementation Resources	The concept of a "Strong Plus" piece of identity evidence was included in the Implementation Resources. This concept should be codified in modifications to the SP documents themselves, with clear inclusion of descriptions. Examples should also be provided, since there are very few documents that meet the requriement of *"If the identity proofing process for issuance of the STRONG evidence confrmed the claimed identity by collecting two of more forms of SUPERIOR or STRONG evidence"* This is not even required or guaranteed by RealID compliant documentation. As REAL ID and mDL become more popular, recommend deleting the clause requiring validating with the issuing source, which would then allow for use of AAMVA validation as an authoritative source.	4. Remote Identity Proofing
5	IRS	63A - 4.4.1.4 Verification Requirements	"No KBV" over the phone is an issue for the IRS because the Taxpayer Protection Program, which identity proofs potential victims of identity theft, uses phone verification for a large segment of users. We contend that having the supervised remote worker proofed to the same level is a mitigating factor. Recommend either making this a SHOULD NOT or adding language around minimizing PII in these situations, or ensuring an NDA for phone operators.	6. Knowledge-based information for verification
6	IRS	63A - 4.4.1.5 Presence Requirements	The recommendation ("SHOULD") for CSPs to support in-person proofing is burdensome for vendors. Recommend removing the second clause. If this section is aiming to get at helping different segments of the population, recommend adding language around the CSP SHOULD support multiple types of identity evidence to cater to different segments of the population.	3. Security and performance capabilities
7	IRS	63A - 4.4.1.6 Address Confirmation	The requirement for verification of address on record is burdensome and expensive for vendors, driving up the price of a proofing event. In addition, this may go against attribute minimization principles; and also can prove difficult due enact to unhoused users or users who have recently moved. Recommend either limiting it to IAL-3, or adding a clause that says this is only required if the RP needs the address, and refocusing this section to telephone or email address on record. Same goes for item f.	3. Security and performance capabilities

8	IRS	63A - 4.4.1.7 Biometric Collection, 5.3.1 Identity Verification Methods, 5.3.3.1 General Requirements	The current Biometrics Collection requirements for Identity Proofing simply points to SP 800-63B, Section 5.2.3. The conclusion one could draw from this is that the Biometric requirements for Identity Proofing and Authentication are exactly the same. Given implementation experiences, there are several suggestions for improvement to make here. 1) Provide a dedicated biometrics section in 63A, in particular around the common implementation practice of "selfie matching". NIST should more clearly define what constitutes good "selfie matching" during Identity Proofing, in particular with regards to the False Match Rate (FMR) and Presentation Attack Detection (PAD) using liveness. 2) Since the vast majority of applicants use their own personal devices (cell phones, webcams), NIST should more clearly define quality conditions, acceptable vendors and tresholds, for instance using the ongoing Facial Recognition Vendor Test Project. Ideally (a group within) NIST will establish metrics and acceptable pass/fail rates at different assurance levels for biometrics algorithms. 3) Biometric guidance for identity proofing specific contexts needs to be provided in order ensure solutions are appopriately defined, measured, and evaluated to ensure appropriate risk mitigation when collecting and verifying biometric information. 4) Liveness detection should be included as an explicit requirement for verification processes that include any form of "biometric" matching. Additionally, greater information on how to perform testing of liveness and performance of liveness should be considered for inclusion that is specific to identity proofing scenarios. 5) Presentation Attack Detection should be codified as part of SUPERIOR and possibly also STRONG verification requirements.	8. Verifier impersonation resistance
9	IRS	63A - Table 5-2	The guidance of using the smallest set of attributes necessary to resolve to a unique individual seems to conflict with the guidance in the SUPERIOR validation requirements: *"All personal details and evidence details from the evidence have been confirmed as valid by comparison with information held or published by the issuing source or authoritative source(s)."* We contend that it is not necessary to validate all information but rather the minimum necessary.	1. Privacy enhancements
10	IRS	63A - Table 5-3, strong verification.	The definitions for both "physical verification done remotely" and biometric verification reference the same biometrics in NIST SP 800-63B, so it would be helpful to clarify the distinction. Based on context it could be implied that the "physical comparison" is of a picture to picture - since no existing "template" can be used for the matching. Where as a "biometric" match is to a specific stored template on a piece of evidence (e.g., a finger print template stored on a PIV card). Regardless this section should clarify and provide clear examples of each.	4. Remote Identity Proofing
11	IRS	63A - 4.5.5 Presence Requirements	Clarify in-person or supervised remote for presence requirements	4. Remote Identity Proofing
12	IRS	63A - 5.3.4 Trusted Referee Requirements	The provided examples of what constitutes a Trusted Referee (TR) - *"notaries, legal guardians, medical professionals, conservators, persons with power of attorney, or some other form of trained and approved or certified individuals"* - provide a broad range of options to designate such a role. Some of these options (for instance the legal guardian) suggest that a TR is someone who intimately knows the applicant and can act on their behalf, while the notion of *"trained and approved or certified individuals"* seems to suggest that TRs could be part of the CSP workforce in the field. The FAQ on TRs (QA-A01) provides a more narrow definition, but does not definitively define and/or limit the usage of TRs. We also know that some CSPs have built IAL2 offerings on the TR concept. The suggestion here is to clear up any remaining confusion around the concept of TRs, in particular on whether or how CSPs may offer TR proofing services, and under which conditions RPs may accept TR assisted proofings.	9. Additional controls

NIST SP 800-63B Comments

#	Commenter	Reference	Comment	Category
1	IRS	63B - General	KBA is not acceptable as any form of authentication - this concept should be explicit in the next revision. See also note about permissable KBV over the phone in our 63A comments	6. Knowledge-based information for verification
2	IRS	63B - General	Email should be removed as a permissable channel for higher assurance levels	8. Verifier impersonation resistance
3	IRS	63B - General	Access control is a huge aspect of system security - suggest to include a recommendation that agencies SHOULD practice robust access control in accordance with the AC family in 800-53	9. Additional controls
4	IRS	63B - General / Electronic Signature Certification/St	"Authentication" is generally related with the identity/identities of a person. Sometimes there is something "weaker" than authentication (as some sort of its subsets for "one time") needed, e.g. the "certification"/authenticity-guaranteeing of an "electronic signature" of a person. If feasible, some corresponding standard would be needed for "Signature Certification" or "Certificate Authority" or something alike. Without the authentication of the person per se, the "Signature Certification" would guarantee the authenticity for a particular electronic signature for a particular electronic document, trusted by all the parties/entities involved, and could be served as the basis of responsibilities in legal, business and financial aspects etc., and the "Signature Certification" could be federated similar to "Identity Federation" (some partial aspects in "Blockchain"?). Currently one of the implementation for electronic signature is "Click-Wrap" and an electronic signature is usually associated with a particular electronic document, where the digital signature (NIST standard: https://www.nist.gov/publications/digital-signature-standard-dss-2) is for being never altered since the signing of the document	9. Additional controls
5	IRS	63B - 6.1.2.3 Replacement of a Lost Authentication Factor	This section allows for the CSP to conduct an "abbreviated" proofing to help recover accounts. However, it provides no guidance on how to abbreviate that process. At a minumum either NIST SP 800-63A or NIST SP 800-63B should provide a minumum expectation for this abbreviated process. For example, at a minimum, this process should include the revalidation and verification of the user's strongest piece of evidence, or something similar. We have observed a CSP's weak "abreviated" process undermine both proofing and MFA.	9. Additional controls
6	IRS	63B - 5.1.3.1 OOOB Authenticators and 5.1.3.3 Authentication using the PTSN	The splitting of requirements across both of these sections, with the verifier section in between makes fully understanding an complete implementation of a use case leveraging PTSN hard to follow. The application of "restricted" to PTSN is also confusing. Is it restricted if it follows the defined requirements, or only if it does not? Are the requirements part of the restriction or not? Additionally, if risk indicators are included (e.g., porting or simswap detection) can these be used to avoid the "restricted status?"	9. Additional controls
7	IRS	63B - 5.2.3 Use of Biometrics, bullet 4	While Bullet 4 applies to physical features (e.g., facial recognition), the listed concerns are not applicable to behavioral biometics.	5. Behavioral characteristics as an authentication factor

NIST SP 800-63C Comments

#	Commenter	Reference	Comment	Category
1	IRS	63C - 2 Introduction (and other Sections)	The differences between "almost-but-not-quite-interchangeable" terms CSP and IdP should be revisited. We understand there is a federation-specific scenario for RP/IdP but we believe just the CSP term may work just as well here and provide additional clarity.	9. Additional controls
2	IRS	63C - 2 Introduction (and other Sections) and 63C - 8 Security	This volume clearly scopes itself to providing guidance to CSPs. We believe there to be value in adding select requirements for the RP as well, to encourage agencies to enhance their own security when setting up a federation; similar to the information around whitelists/blacklists in Section 4.2. For instance, consider the RP's role in enhancing assertion security and fraud mitigation on top of what the CSP provides. In addition, could the RP have a role in enhancing security across the entire ecosystem, e.g. through reporting incidents to the CSP, who then in turn notifies other RPs? (*see also our comment on 63C - 8 Security, incident reporting*)	9. Additional controls
3	IRS	63C - 4.2 Runtime Decisions	Suggest to update the terms whitelist/blacklist, for instance to allowlist/denylist	9. Additional controls
4	IRS	63C - 8 Security	Recommend some notation around incident reporting - not just to the RP but to network of other entities consuming the assertion- and encourage the use of automated security reporting e.g. using OSCAL.	9. Additional controls