Comment #	Publication (Base, 63A, 63B, 63C)	Section	Page #	Line #	Comment (Include rationale for comment)	Suggested Change
	63-Base	4. Digital Identity Model	24	637, Figure 1.	Suggest readability improvements for Figure 1. The steps are out of order on the graphic which makes it difficult to follow.	Suggest having the CSP at the top of the graphic, RP, then Verifier; or at least have the steps in order for ease of use.
	63-Base	4. Digital Identity Model	25	657, Figure 2.	Suggest readability improvements for Figure 2. The steps are out of order on the graphic which makes it difficult to follow.	Suggest having the CSP at the top of the graphic, RP, then Verifier; or at least have the steps in order for ease of use.
	63-Base	4. Digital Identity Model	27	706 & 707	"The CSP then establishes a subscriber account to uniquely identify each subscriber and record any authenticators registered (bound) to that subscriber account." How does a subscriber differ from an identity at this point? Are these terms interchangeable in this scenario? The IAM community is familiar with multiple authenticators being bound to a single identity.	Explain the difference between a Subject (Applicant, Subscriber, and Claimant) and an Identity. The document is entitled 'Digital Identity Guidelines' but utilizes the CSP terminology (i.e. Subscriber/Claimant) throughout.
	63-Base	5. Digital Identity Risk Management	35	943	GSA created the Digital Identity Risk Assessment (DIRA) Playbook as a method of applying Digital Identity Risk Management. The Digital Identity Acceptance Statement is a product of this assessment; thus we suggest referrencing DIRA or explaining how this serves as a companion document to 800-63-4.	Suggest incorporating DIRA into Section 5. Digital Identity Risk Management OR referencing the DIRA Playbook as complimentary guidance.
	63A	5.6 Summary of Requirements	45	1234, Table 1.	The IAL Requirements Summary is signifcantly different from the previous revision. Based on this table, are we to takeaway that that only difference between IAL1 and IAL2 is the Verification piece? The rest of the requirements for IAL1 and IAL2 in this table are the same verbiage.	The document states "IAL2 adds additional rigor to the identity proofing process by requiring the collection of stronger types of evidence and a more rigorous process for validating the evidence and verifying the identity." but the evidence requirements are the same. Suggest verifying this is accurate and provide reasoning for the significant variance from 800-63-3 requirements.
	63A	Appendix A. Change Log	72	1933	"Adds requirements for a new IAL1 for lower-risk applications" Should this say IAL0 or IALx?	IAL0 was added to the latest revision, suggest this addition to the change log.
	63B	6.1.1. Binding at Enrollment	54	1598-1600	"The CSP SHALL bind at least one — and SHOULD bind at least two — physical (something you have) authenticators to the subscriber account..." What would be an example of this if the subject has a PIV card? For agencies that are considering FIDO2 authentication would the laptop or mobile device suffice? FIDO2 authentication is designed to work with existing infrastructure and should not require special hardware.	Most federal employees and contractors already have one physical authenticator. Suggest providing clarity on what second physical authenticator should be used to bind to.
	63B	5.1.1.1. Memorized Secret Authenticators	26	676 & 684	Currently in USAccess, the software used to activate the PIV card, only a 6 digit pin is required/enforced by the application. How will this be addressed for current card holders?	No change in documentation required; just wanted to bring awareness of PIV issuance software current state.