Comment #	Publication (Base, 63A, 63B, 63C)	Section	Page #	Line #	Comment (Include rationale for comment)	Suggested Change
1	63A	2.2	4	408	EPA supports the inclusion of a no identity proofing (IAL0) assurance level and changing the IAL1 assurance level to be a verification standard than IAL2. While EPA routinely interacts with external users the identity proofing needs vary significantly. Adding the additional assurance level provides EPA with a broader foundation to support programmatic functions.	N/A
2	Base	5.1.1	24	982	A significant gap in the impact assessment process is how to appropriately assess digitial identity risk for situations when multiple non-organizational users have shared responsibility for entering and viewing data that is then submitted to the federal government. In most scenarios EPA regulates activities and does not regulate individuals. But it is individuals that interact with EPA to license/permit the activity or otherwise submit compliance reports for the activity. When individuals transact with EPA there is a general need for EPA to know the digital identity of the individual (e.g. for electronic signature processes) that is representing the activity. For many regulated activities there are multiple non-EPA users that may be involved in entering, reviewing, granting access to, and ultimately submitting information for a given activity to EPA. For digitally signed documents EPA generally focuses on the identity of the individual who ultimately submitted the document or individuals who manage access to the acitivty. EPA typically does not have an interest in knowing the identity of individuals who prepare data for submission, but EPA may collect self asserted information (e.g. name, email) to facilitate that function. Historically EPA identifies different types of roles/permissions for non-organizational users and identity proofs as appropriate. While some programs may require identity proofing for all users, for others it is deemed too high burden and only users that must be identify verified are. In practice it becomes very challenging to reconcile what has been historically done with a modern impact assessment framework. In theory email addresses/user names can be used as account indentifiers that are sufficiently secured and identity assurance can be performed by non-organizational users without need to engage EPA. While EPA can tailor the identity assurance process to account for this scenario, the pervasivity of it would be beneficial to be acknowledged in 800-63 to identify recommendations on how to address the identity assurance needs for individuals who support but are not directly transacting with EPA.	Add examples for how impact assessments would be completed for regulated entities or companies.
3	Base	5.1.3	27	1063	In identifying impact levels a note is provided that says "if a failure in the identity system causes no measurable consquences for a category, there is no impact". However in Table 1. Impact Categories there is no category specific option for none. If there is no impact for a category it is not clear if it should be left blank or if low should be selected for the category. If the intent was to categorize no impacts under the low impact level, which would result in IAL1, then this should be explicitly stated. If no impact results in IAL1 then clarity should be provided for situations it would be appropriate to use IAL0.	Add "None" to Table 1 in addition to L/M/H.
4	63B	4	6	439-440	The AAL2 requirement resulting from the online availability of PII is confusing and should be clarified. It is not clear if it is the availability of the PII to the account holder, the availability of the account PII to other users (e.g. anonymous users on a public website), or if it is the general ability to view any PII at all (e.g. names on a public websites) that triggers the AAL2 requirement. The intent appears to be that if PII is viewable by the respective user after they authenticate then it would trigger AAL2. However that would imply that if any type of PII (including basic self asserted information such as name and email) are visible, then it would require AAL2. Such a strict interpration is challenging and would seem to preclude use of AAL1 even for cases that assess no impact. In practice no impact use cases are not often assessed for an ATO as they would be excluded as part of the RMF process. If this is intended to be a global intended then greater clarity should be provided.	