NIST SP 800-63-4(Draft) Digital Identity Guidelines
DoD Response to PRE-DRAFT Call for Comments

#	Organization/ POC	Document/ Section	Issue	Recommendation
1.	DoD Rebecca Nielsen	General	Federal agencies have an increasing number of policy requirements they must address that are related to ICAM. Currently, these documents and requirements are not well aligned, requiring agencies to either create their own alignment or perform multiple assessments to ensure they are compliant with all of the various publications. While each document has its own distinct focus, ICAM is a critical element of all of them. Some examples include: • OMB – M-19-17 and FISMA • NIST – SP 800-63, SP 800-53, FIPS 201, Cybersecurity Framework • DHS – CDM	NIST should provide an appendix or other mechanism to align the requirements in SP 800-63 with other NIST publications, and should coordinate with other agencies to simplify assessments for ICAM related requirements.
2.	DoD Rebecca Nielsen	General	This document provides requirements for identity proofing, authenticator, and federated assertions for person entities, but it explicitly does not address non-person entities such as robotic process automation or endpoints, nor does it address requirements for organizational entities such as businesses or government offices. Implementing ICAM requires consistent approach to all types of entities, not just person entities.	Either expand this document to include non-person entities and organizational entities, or develop additional guidance that does address these entities.
3.	DoD Rebecca Nielsen	General	The document talks to relying parties in general, but does not differentiate between different types of transactions. In practice, most information systems will have general users, functional privileged users, and IT privileged users, and the IAL, AAL, and FAL will likely be different depending on the type of user. For example, a web site that is designed to provide agency information to the general public will not require authentication for general users, but functional privileged users who can update the content of the site would need to authenticate, and system administrators may have additional authentication requirements.	Focus the document on the type of transaction, not just the general users of a system.

#	Organization/ POC	Document/ Section	Issue	Recommendation
4.	DoD CIO Rebecca Nielsen	800-63 Section 4, 800-63A General	The definitions and requirements for the IAL levels need to be redone to be more useful and usable. As currently written, IAL1 has no assurance, as it allows for self-assertion of identities, and IAL3 requirements cannot realistically be implemented. IAL2 essentially includes everything in the middle, which leaves processes that meet IAL2 with very different actual assurance. For example, in-person identity proofing of an entity using breeder documents that contain a photo provides a very different assurance than unmonitored remote proofing, but both of these processes may be IAL2. Furthermore, descriptions of how identity proofing is performed narrowly focus on the presentation of breeder documents, which does not fully address mechanisms for performing identity proofing such as the concept of a known entity vouching for the identity of a new entity,	Consider the following: • Replace the "self-asserted" definition of IAL1 (which is essentially no assurance) with a definition of basic identity proofing, such as on-line database checks or assertion of identity by a known entity • Increase the total number of IALs described to account for the broad range of identity proofing mechanisms • Redefine IAL3 so that it can be met by other providers external to the government • Use a different process for describing assurance of identity proofing – the current definition of "fair" "good" types of breeder documents is confusing and doesn't accommodate all types of identity proofing
5.	DoD CIO Rebecca Nielsen	800-63 Section 4, 800-63A General	Although discussions on updates to FIPS-201 have stated that the requirements for issuing PIV cards are IAL3, a comparison of the identity proofing processes described in FIPS 201 do not fully meet the requirements specified in SP 800-63. The background investigation process required by FIPS 201 provides additional proof that an identity exists in the real world, but is not part of the process to prove that a given real world individual is the person whose background was checked. These are separate processes, and should not be equated together in FIPS 201 to claim that the IAL3 requirements as currently stated in SP 800-63 have been met.	• Align the identity proofing requirements in SP 800-63 so that the processes in FIPS 201 meet IAL3
6.	DoD CIO Rebecca Nielsen	800-63 Section 4, 800-63B General	The requirements for AAL focus on the authenticators themselves, but do not address the assurance of the system used by the	Either include key credential service provider requirements as part of the

#	Organization/ POC	Document/ Section	Issue	Recommendation
			credential service provider to manage those authenticators. Without adequate protections implemented by the credential service provider, an attacker can generate credentials claiming any identity, bypassing identity proofing and negating the strength of the authenticator. The Federal PKI provides a baseline set of requirements for Public Key Infrastructure (PKI) based credentials through the Federal Bridge Certificate Policy and the Federal Common Policy Certificate Policy, but there are no equivalent requirements for non-PKI credentials, and there is no references to certificate policies or any other standards for credential service provider operations in the document.	definition of authenticator assurance levels, or provide references to standards where these requirements are defined. Without operational protections, authenticator assurance levels are not meaningful.
7.	DoD Rebecca Nielsen	800-63 Section 4, 800-63C General	The requirements for FAL focus on the assertions themselves, but do not address the assurance of the identity provider system that performs authentication and generates assertions. Without adequate protections implemented by the identity provider, an attacker can generate assertions claiming any identity without authenticating first, negating the strength of the assertion. As an example, an IdP that authenticates AAL3 credentials should meet the same requirements for protection of its own private signing key as those for the credentials themselves.	Either include key identity provider requirements as part of the definition of federation assurance levels or provide references to where these requirements are defined. Without operational protections, federation assurance levels are not meaningful.
8.	DoD Rebecca Nielsen	800-63 Section 4, 800-63C General	The requirements for FAL3 are not currently commercially available for identity providers or well supported by commercial off the shelf software. However, as written, FAL3 is required for certain types of transactions. Having documented requirements that are not supported creates significant issues with implementing the policy.	Either redefine the requirements for FAL3 so that they are supported, or change the flowcharts to indicate that FAL3 is aspirational but not required today.
9.	DoD Rebecca Nielsen	800-63 Section 5 and 6	Although SP 800-63-3 split out the requirements for IAL, AAL, and FAL into different categories rather than the single assurance level defined in SP 800-62-2, the flow charts describing the requirements are essentially identical for each of the three elements. So AL-1 from version two became IAL1/AAL1/FAL1 in version 3, AL-2 and AL-3 from version two became IAL2/AAL2/FAL2 in version 3, and AL-4 from version two became IAL3/AAL3/FAL3 in version 3. So version three actually provides fewer distinctions in the implementation of authentication than version two since AL-2 and AL-3 were merged. If	Reconsider the flow charts and implementation requirements for the various assurance levels to better align them with usability, scalability, and security goals.

#	Organization/ POC	Document/ Section	Issue	Recommendation
			there are no distinctions in the implementation of the various levels, having more levels adds unnecessary complexity.	
10.				
11.				
12.				
13.				
14.				
15.				
16.				
17.				
18.				
19.				
20.				
21.				
22.				
23.				
24.				
25.				
26.				
27.				
28.				
29.				
30.				