Department of Education Comments for: NIST SP 800-157

Please submit responses internally by 2/17/2023

#	Section	Page #	Line #	**Comment** (Include rationale for comment)	Suggested Change
1	1.6	4	362	The term subscriber - aligns with most NIST publications but there may be a few instances of confusion, for example in the glossary of 800-72 ("An individual applying for a Derived PIV Credential") versus someone who already has the derived PIV credential in hand.	
2	2	5	380	In Figure 1, is there a way to indicate that non-voluntary termination of a DPC may get flagged for a review of the PIV as well? This could be in instances of suspected fraud or misuse of the DPC; the PIV account may wish to be monitored as well.	
3	2.1	6	395	When a non-PKI authenticator is lost, stolen, or damaged, does the credential being invalidated on the issuer side remove the DPC altogether similar to a re-key event, or could it be revalidated without having to undergo the issuance process again?	
4	2.2	7	436	It may be good to provide examples of how to notify the PIV holder that a DPC has been issued; and are there requirements around this process, e.g. it would have to go to a validated address of record?	
5	2.2.1	8	461	It's implied, but at AAL2, it might be good to specify that the public/private keypair for the DPC is different than the keypair created for the PIV itself.	
6	2.2.2	8	476	Including the FIPS 140 requirements may rule out non-certified FIDO authenticators.	

7	N/A	N/A	N/A	General - are there special requirements or guidance around the use of DPCs for physical access? Is this up to the issuing agency?	
8	2.3.1	9	513	In the event of a name change, does the subscriber need to undergo the binding process again, or is the certificate just updated?	
9	2.4	10	538	Tracking the termination status of a PIV card is indeed a large challenge for PKI management. Maybe include a line to indicate that agencies should have processes in place to routinely cross-check for expired, revoked, or invalidated accounts with active PKI-based DPCs attached.	