Comment Template for: NIST SP 800-157r1 (Initial Public Draft)

Please submit responses to piv_comments@nist.gov by ~~March 24~~ April 21, 2023

Organization:	*Department of Veterans Affairs, Information Security Engineering, Identity and Access Management*
Name of Submitter/POC:	
Email Address of Submitter/POC:	

Comment #	Section	Page #	Line #	Comment (Include rationale for comment)	Suggested Change
1	2.3 Maintenance; 2.4 Invalidation	19, 20	488, 489 & 528-530	These lines state "Derived PIV credentials are unaffected when the subscriber replaces their PIV Card with a new one (reissuance) or when the PIV Card is lost, stolen, or damaged." However, this is contradicted on the next page where it states "When an authenticator associated with a derived PIV credential is compromised (e.g., lost, stolen, or damaged), that derived PIV credential SHALL be invalidated as described below. All derived PIV credentials associated with a given PIV Card SHALL be invalidated when the associated PIV identity account is terminated.	There needs to be clear, consistent language on what happens to a derived credential in the instances of a lost, stolen, or damaged PIV card. The PIV card is terminated when it is lost, stolen, expired, etc. during the reissuance process.
2	3.2.1 Allowable Authenticator Types	23	632	This section focuses on phishing-resistant multi-factor or single-factor cryptographic authenticators, but does not provide a list of examples of commonly used authenticators.	Suggest providing examples of both types of authenticators that can be used to meet these requirements.
3	B.1.2. Derived PIV Application Data Model Elements	28	829	The CHUID was deprecated per FIPS-201-3 "Removal of the previously deprecated Cardholder Unique Identifier (CHUID) authentication mechanism and deprecation of the symmetric card authentication key and visual authentication mechanisms (VIS)" Does this still apply for derived PIV credentials?	Provide update on whether the CHUID is used for Derived PIV or remove reference.
4	2.2 Initial Issuance	17	433	The statement reads as if associating the derived PIV credential with the identity account is optional? I don't think that is correct and should be re-phrased.	Suggest changing to -- : "After the applicant has been authenticated, a derived PIV credential MAY be issued and **SHALL** be associated with the cardholder's PIV identity account. The newly issued derived PIV credential SHALL be represented in the cardholder's PIV identity account."
5	2.2. Initial Issuance	18	449-451	Line states "Accordingly, issuers MAY place a limit on the number of active derived PIV credentials that a subscriber may have." What is the recommended number of derived credentials that are considered to be at a secure level?	Suggest providing guidance on secure level of derived credential assignments.