Comment Template for: NIST SP 800-63-4 Suite (Second Public Draft)

Please submit responses to dig-comments@nist.gov by October 7, 2024.

Organization:	*Forrester Research*
Name of Submitter/POC:	*Conor McCormick, Account Director - Department of Commerce*
Email Address of Submitter/POC:	[redacted]

Comment #	Publication (Base, 63A, 63B, 63C)	Section	Page #	Line #	Comment (Include rationale for comment)	Suggested Change
1	63-Base				This new version does not reference the role of Idenitity as part of a Zero Trust Architecture.	As appropriate throughout the document, include the ties between digital identity and Zero Trust Architecture. In Section 1, include a discussion about Zero Trust Identity pillar requirements from EO 14028 and M-22-09 and its relation to NIST SP 800-207 (Zero Trust Architecture). Specifically see SP 800-207, Section 3.1.1 ZTA Using Enhanced Identity Governance. The CISA Zero Trust Maturity Model (ZTMM) states numerous identity-related functions and capabilities as a part of an organization's maturity. This also needs to be included throughout the series. Agencies rely on this mapping as they leverage NIST standards.
2	63-Base	Glossary			The glossary lacks digital identity-related terms from NIST SP800-207, Zero Trust Architecture.	Add digital identity-related terms such as Policy Engine (PE), Policy Administration Point (PAP), Policy Enforcement Point (PEP), and Policy Decision Point (PDP), etc.
3	63C				OMB M-22-09 requires, "Agency staff use enterprise-managed identities to access the applications they use in their work."	Include a reference to M-22-09 and a discussion about enterprise-managed identities.
4	63B				OMB M-22-09 requires, " Phishing-resistant MFA protects those personnel from sophisticated online attacks."	Include a reference to M-22-09 and how it applies to meeting the OMB requirement.
5	63-Base	Section 2			NIST SP 800-63-4 2pd : Section 8.3 of 800-63-3 calls out authenticator recovery as a weak point in many authenticator mechanisms.	Consider adding statements to highlight this in section 2 on digital identity model. Emphasis on authenticator lifecycle management/recovery should be added and/or reference to 800-63B and cover in more details there.