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:	*Cloudflare, Inc.*
Name of Submitter/POC:	*Ellie Durling*
Email Address of Submitter/P	[redacted]

Comment #	Publication (Base, 63A, 63B, 63C)	Section	Page #	Line #	Comment (Include rationale for comment)	Suggested Change
1	63A	4.3.1 Proofing Types	44	1794	The requirement for IAL3 identity proofing to be conducted exclusively via in-person, onsite attended sessions poses significant challenges for companies like Cloudflare that rely heavily on a globally distributed remote workforce. Many of our employees are located in countries around the world, making it extremely burdensome and impractical to conduct in-person identity proofing for all IAL3 use cases. This limitation would hinder Cloudflare's ability to provide high assurance identity services to our customers and secure access for our own remote employees.	We suggest that NIST consider allowing alternative secure remote identity proofing methods that can achieve an equivalent level of assurance as in-person proofing for IAL3. This could include a combination of secure video conferencing, document verification, and biometric collection that meets the requirements outlined in Section 4.3.8 for remote attended proofing. Enabling secure remote IAL3 proofing options would provide more flexibility for globally distributed organizations while still maintaining the necessary level of identity assurance.
2	63A	4.3.1 Proofing Types	44	1794	We understand that we need to collect a biometric sample at the time of verification, however we want to highlight potential privacy concerns. In particular, this could pose a significant challenge for companies with employees in countries where there are limitations on the collection of this type of information.	We suggest that NIST provide additional guidance on acceptable methods for securely collecting, processing, storing and disposing of biometric samples in a manner that respects applicable privacy regulations and user concerns. This could include specifying requirements for obtaining explicit user consent, minimizing data retention, protecting biometric data both in transit and at rest, and allowing users to easily request deletion of their biometric information. Additionally, in cases where employees are located in countries that prohibit the collection of biometric data, NIST should consider allowing alternative non-biometric methods for identity verification that can still meet the IAL3 assurance level. This would provide flexibility for global organizations while ensuring compliance with local laws and regulations.