[redacted]

Hey Campbell,

The intent of the requirement text was to provide greater clarity on the “periodic” nature of testing matching algorithms and what would trigger the need for “re-testing” to confirm performance has not changed substantially.

As the current requirement constituted, I think you proposed approach is reasonable, though not precisely conformant. Fortunately, this is why we do public comment periods. We would be interested in suggested alternative text that is reasonable and meets the need to ensure that algorithmic updates to not result in serious performance deviations, to include between different demographics.

Happy to grab time to discuss if you want.

Ryan

From: Campbell Cowie [redacted]
Date: Wednesday, September 4, 2024 at 5:12 AM
To: Galluzzo, Ryan J. (Fed) [redacted]
Subject: Digital Identity Draft Guidelines Query

Ryan- I wanted to start by saying how useful the workshop on the draft Digital Identity Guidelines was - as someone with a global remit, I can only wish that other authorities were as open and consultative.

Reading through the draft on identity proofing - nodding in agreement to the vast majority - and wanted to check something with you for clarity. I hope you dont mind.

On line 1238 there is a requirement for algorithms to be retested after it is updated. I wanted to just check your thinking on that. We update our algorithm 3 or 4 times each week on average, reflecting how we respond to the rapidly accelerating changes in the threat landscape. There is not the testing capacity on earth to have each updated algorithm externally retested. We work with external ISO certified labs and are subject to regular testing (including for injection attacks). Testing can take months and consume the resources of the entire lab. What we do is combine periodic external testing with internal testing and independent auditing of our processes (including our approach to testing). We are certified at Level of Assurance: High under the EU's eIDAS framework, with accreditation done regularly by certified authorities.

Does this sort of approach - external testing, internal testing and independent audit of processes - fall under your intended meaning?

As the same threats impact non-biometric solutions (in-person and human examiner) I would struggle to see how their performance is retested every time a new threat is identified (3 or 4 new threats are identified each week).

I would welcome the chance to discuss if you are free.

Thanks,
Campbell

--

Campbell Cowie
Head of Policy, Standards and Regulatory Affairs

[redacted]