## 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:*** | *iProov* |
| ***Name of Submitter/POC*** | *Campbell Cowie* |
| ***Email Address of Submi*** | [redacted] |

| Comment # | (Base, 63A, | Section | Page # | Line # | Comment (Include rationale for comment) | Suggested Change |
|---|---|---|---|---|---|---|
| 1 | **63-Base** | 1 | 1 | 373 | The Guidlines should make explicity reference to obligations on publicly funded organizations to explicitly consider the cost efficiency of their approach to identity solutions. There are several Executive Orders which place requirements on Federal Agencies to demonstrate prudence with public funds and to undertake full cost-benefit analyses of decisions. (See for example, https://crsreports.congress.gov/product/pdf/IF/IF12058). Total lifetime costs of a solution should be explicitly included within the cost-benefit analysus which underpins the decision making process. The declining performance of human operators relative to biometric systems creates additional (and increasing) costs (over the solution lifetime) due to the need to remedy declining confidence in human operators and reduce risks, for example through increased training costs (although research shows that training has little positive impact on human performance (see Klaire Somoray, Dan J. Miller, Providing detection strategies to improve human detection of deepfakes: An experimental study, Computers in Human Behavior, Volume 149, 2023, 107917, ISSN 0747-5632, ttps://doi.org/10.1016/j.chb.2023.107917. (https://www.sciencedirect.com/science/article/pii/S0747563223002686)), higher wages to attract more effective examiners and through employing additional human operators to provide additional scrutiny of the primary human operator's decision. Cost estimates would also have to include computer system and IT costs as human operators would have to capture decision data required for subsequent reviews. These systems would require maintenance and regular development to enable the human operator to capture and store data (for processing) on new and evolving threats. The logging of decisions creates another process component subject to human error. Cost ciomparisons must be done between solutions delivering equivalent levels of security, equity and usability. The threat landscape is changing at pace, with the sophistication of threats increasing at an accelerating rate. The amount of training (and therefore | Organizations should reflect the lifetime cost implications of alternative identity solutions in cost-benefit analysis and be accountable for those decisions through their compliance with requirements to demonstrate prudence with public funds. |
| 2 | **63-Base** | 1 | 2 | 382 | As above, the lifetime cost of a solution is an important matter for organizations. | ...secure, private, usable, cost effective, and equitable services to ..... (bold text is suggested addition) |
| 3 | **63-Base** | 1.3.3 | 7 | 570 | Bias is a challenge that impacts both human examiners and biometric solutions, so performance requires in the Guidelines should apply equally to both. Human bias in image examination is well known. For example, See Emily Pronin, Perception and misperception of bias in human judgment, Trends in Cognitive Sciences, Volume 11, Issue 1, 2007 (https://www.sciencedirect.com/science/article/pii/S1364661306002993) and Heyer, Rebecca & Semmler, Carolyn. (2013). Forensic confirmation bias: The case of facial image comparison. Journal of Applied Research in Memory and Cognition. 2. 68-70. 10.1016/j.jarmac.2013.01.008. Unlike human systems, bias in biometric solutions can be tested for and processes put in place to continually reduce bias levels. This research shows that humans perceive their own judgement to be less influenced by bias than the judgement of others. This makes objective | ...operation of human, biometric or hybrid digital identity systems. (bold text is suggested addition) |

| | | | | | | |
|---|---|---|---|---|---|---|
| 4 | **63-Base** | 2.3.1 | 12 | 698-702 | The rationale for requiring multi-factor authentication to draw on factors from different factor types is based on the presumption that should one be breached then then the other is also vulnerable if from the same factor channel. However, this is a challengable presumption in the case of biometrics. It is not technically challenging to maintain systems such that should data on (for example) fingerprint biometrics be breached, face biomtric data can still be secure. Moreovever, the application of Liveness testing in biometric solutions mean that even were a malicious actor somehow able to steal a copy of fingerprints or attempt to use a photo, a robust solution would identity the spoof attempt. If a malicious actor was to, for example, steal a device and threaten the device owner, then the two factors of "something you have" and "something you know" could be readily compromised. In such circumstances it need to be recognised that humans are not inherently skilled at spotting whether another is being coerced. Malicious actors will design coercion efforts to minimise the risk of their being caught. To presume that human operators are uniquely capable of identifying anomalies is simply incorrect. The effectiveness of the human will depend on the operational environment, the quality of the training and the performance of the human at that point in time. For example, if they are distracted, tired, not sufficiently well trained or simply not focussed on identifying anomalies then they are unlikely to be effective at this task.<br>There is a sizable body of widely available, peer-reviewed and generally accepted research evidence which shows how even well trained human observers fail to spot significant anomalies. By way of example, see The invisible gorilla strikes again: Sustained inattentional blindness in expert observers, Drew et al, Psychol Sci. 2013 September ; 24(9): 1848–1853. (https://www.ncbi.nlm.nih.gov/pmc/articles/PMC3964612/pdf/nihms563995.pdf). In this research, an anomaly was added to a standard scroll of axial slices of a lung. 100% of the untrained examiners failed to spot it, whilst 83% of trained | Multiple instances of the same factor may be accepted where the organization has confidence that the security of each factor is such that should one be compromised the other is still secure. |
| 5 | **63-Base** | 3 | 22 | 926-928 | As above, it is important that organizations (in particular those in receipt of taxpayer funding) take account of the lifetime costs involved in securing equivalent performance from the alternative systems (human, biometric/automated and hybrid) and make decisions which take explicit account of those cost impacts.<br>Organizations have a duty to provide value for money for taxpayers, and Federal Agencies are requireed under several Executive Orders (12866 and 13771 for example) to undertake cost-benefit analysis and to be "prudent and financially responsible" with public funds. The Guidelines should make these requirements explicit as they are relevant to the approach of organizations to selecting between | Risk assessments are not a stand-alone exercise and should be a component element of the organization's cost-benefit analysis, with the effectiveness of alternative identity systems forming part of of the benefits estimations. The lifetime costs of securing a specific level of risk mitigation should be considered by the organization. |
| 6 | **63-Base** | 3.3.3 | 37 | 1407-1409 | As above, it is important that organizations (in particular those in receipt of taxpayer funding) take account of the lifetime costs involved in securing equivalent performance from the alternative systems (human, biometric/automated and hybrid) and make decisions which take explicit account of those cost impacts.<br>Organizations have a duty to provide value for money for taxpayers, and Federal Agencies are requireed under several Executive Orders (12866 and 13771 for example) to undertake cost-benefit analysis and to be "prudent and financially responsible" with public funds. The Guidelines should make these requirements explicit as they are relevant to the approach of organizations to selecting between | ...controls based on the potential impact of failures in the digital identity approach, as well as the lifetime costs of the identity system (bold text is added suggestion) |
| 7 | **63-Base** | 3.4.1 | 41 | 1596-1599 | As above, it is important that organizations (in particular those in receipt of taxpayer funding) take account of the lifetime costs involved in securing equivalent performance from the alternative systems (human, biometric/automated and hybrid) and make decisions which take explicit account of those cost impacts. Organizations have a duty to provide value for money for taxpayers, and Federal Agencies are requireed under several Executive Orders (12866 and 13771 for example) to undertake cost-benefit analysis and to be "prudent and financially responsible" with public funds. The Guidelines should make these requirements explicit as they are relevant to the approach of | These assessments shall include a formal cost-benefit analysis, taking into account the lifetime costs of the considered identity systems. (bold text is added suggestion) |

| | | | | | | |
|---|---|---|---|---|---|---|
| 8 | **63-Base** | 3.5 | 44 | 1689 | The accelerating sophistication of attacks means that human are increasingly challenged and their vulnerabilities in being able to distibguish between fake and genuine images will become ever more apparent. As such, humanoperator led systems will require an increasing amount of specialised training and particularly testing- whenever new attacks are developed (i.e. 3 or 4 times per week at the current rate of threat detection). Reesearch makes clear that it should not be presumed that a human operator cannot be tricked by a fake image. Available research provides evidence that human operators have a high failure rate in identifying AI generated images. For example, see Michoel L. Moshel, Amanda K. Robinson, Thomas A. Carlson, Tijl Grootswagers, Are you for real? Decoding realistic AIgenerated faces from neural activity, Vision Research, Volume 199, 2022, 108079, ISSN 0042-6989, https://doi. org/10.1016/j.visres.2022.108079. https://www.sciencedirect.com/science/article/abs/pii/S0042698922000852. See also Nils C. Kobis, Barbora Dolezalová , Ivan Soraperra, Fooled twice: People cannot detect deepfakes but think they can, iScience 24, 103364, November 19, 2021, https://www.ncbi.nlm.nih.gov/pmc/articles/PMC8602050/pdf/main.pdf. The authors show how people cannot reliably detect deepfakes, whilst raising awareness and financial incentives do not improve people's detection accuracy. The authors show that People tend to mistake deepfakes as authentic videos (rather than vice versa) and that people overestimate their own deepfake | Organizations shall ensure that the training for proofing agents is updated and refreshed whenever new threats are identified by effective intelligence and agents are retrained and their performance tested when there are material updates in the threat landscape. This is particularly important where identity systems use a combination of automated solutions and human operators |
| 9 | **63-Base** | 3.5.2 | 46 | | Table 4 should include operating costs as a performance metric and subject to regular review | Identity system operating costs should be captured and reported. |
| 10 | **63-Base** | 3.8 | 50 | 1826 | Most computer applications today use AI (eg predictive text to web search) so to require the documentation of all uses of AI and ML is disproptionate and is likely to lead to crifical/relevant uses being masked or lost amongst a long list of irrelevant AI/ML use. The requirement should be narrowed to uses of AI and ML which are directly relevant to the identity system | All uses of AI and ML directly relevant to the identity system shall be documented.... |
| 11 | **63A** | 2.1.3 | 9 | 616 | When discussing hybrid solutions, where a human opertor is involved as well as an automated stage, the draft Guidelines have not captured the importance of how the ultimate decision is taken in practice. The degree to which the ultimate decision rests with the human operator is critically important. The term "hybrid" captures a wide range of operating models, from 99.99% human operator controlled through to 99.99% automated system controlled. Care needs to be taken to clarify how the relationship between the human operator and the automated solution works in practice. Whenever the term "hybrid solution" is used, clarity is required on the nature of the interaction between the human operator and the automated system. If the human operator does not interact with the automated system (for example, by not being required to take into account the output of the automated system) then it is in effect a manual system. If the human operator has to interact with the automated system to reach a decision then it is of critical importance that the human operator understands the automated system and how it functions to deliver a decision.The importance of this interaction is often missed in discussions. Research shows how the performance of even highly trained human operators declines when used as part of a hybrid system. See, for example Nightingale, Sophie & Farid, Hany. (2022). AI-synthesized faces are indistinguishable from real faces and more trustworthy. Proceedings of the National Academy of Sciences. 119. e2120481119. 10.1073/pnas.2120481119. (Available at https: //pubmed.ncbi.nlm.nih.gov/35165187/ ) It is not the case that all hybrid systems are better than all automated solutions in all circumstances (see, Prof. John Daugman's excellent explanation of why combining modalities can lead to a reduction in performance (https://www.cl.cam.ac.uk/~jgd1000/combine/combine.html#:~:text=If%20two% 20biometri c%20tests%20of,the%20net%20equal%2Derror%20rate.)). If you are combining an automated solution with a human operator then it is important to | Organizations shall ensure that the training for proofing agents is updated and refreshed whenever new threats are identified by effective intelligence and agents are retrained and their performance tested when there are material updates in the threat landscape. This is particularly important where identity systems use a combination of automated solutions and human operators. |

| | | | | | | |
|---|---|---|---|---|---|---|
| 12 | **63A** | 2.5.1 | 14 | 811 | To be efffective, a biometric comparison must include a liveness test. This is the only way to have confidence against a PAD or digital injection attack. | ...biometric comparison, incorporating liveness detection,.... |
| 13 | **63A** | 3.1.2.1 | 18 | 903 | Date of death records are not comprehensive. For example, they typically do not contain full information on expats. As there is no single comprehensive source the requirement will add complexity, time and cost to processing applications. A biometric liveness check can determine if the individual is a real person, is present at the time of the biometric capture and is a match for the identity in presented authoritiative documents. For organizations using biometrics incorporating liveness the requirement for a Date of Death check adds an avoidable cost for a secondary check which may not be accurate. The Guidelines should require either a biometric liveness test OR a Date of Death check. | Either a biometric check incorporting liveness or a Date of Death Check.... |
| 14 | **63A** | 3.1.2.1 | 19 | 936-938 | The research paper from David White , Richard I. Kemp, Rob Jenkins, Michael Matheson, A. Mike Burton is noteworthy for explaining that even expert examiners can be spoofed with a high rate of success in the attended use case (see White D, Kemp RI, Jenkins R, Matheson M, Burton AM (2014) Passport Officers' Errors in Face Matching. PLoS ONE 9(8): e103510. https://doi.org/10.1371/journal.pone.0103510.) It was found that on 15% of trials the officers decided that the photograph on their screen matched the face of the person standing in front of them, when in fact, the photograph showed an entirely different person. In a second test, the passport officers were asked to match current face photos to images taken 2 years ago or to genuine photo-ID documents including passports and driving licences. Error rates on this task rose to 20% - a level of performance that was no different to a group of untrained student volunteers who were also tested.When commenting on this paper, Professor Mike Burton, Sixth Century Chair in Psychology at the University of Aberdeen said: "Psychologists identified around a decade ago that in general people are not very good at matching a person to an image on a security document. Familiar faces trigger special processes in our brain - we would recognise a member of our family, a friend or a famous face within a crowd, in a multitude of guises, venues, angles or lighting conditions. But when it comes to identifying a stranger it's another story." (https://www.abdn.ac.uk/news/6590/). It should also be noted that evidence suggests that even expert examiners can be fooled by fake documents and images when prevelence of fake documents being presented is low. See Weatherford, D.R., Roberson, D. & Erickson, W.B. When experience does not promote expertise: security professionals fail to detect low prevalence fake IDs. Cogn. Research 6, 25 (2021). (available from https://rdcu.be/dUCbQ). The same research also shows that expert examiners who are supported by digital tools make a higher number of errors, with reliance of digital tools having a deleterious effect on their learning. In addition, the | CSPs shall train proofing agents to detect indicators of fraud and test for performance at an equivalent level to that expected in biometric systems. CSPs shall make available sufficient resources such that agents' performance is not undermined by working conditions. |
| 15 | **63A** | 3.1.5 | 23 | 1093 | A biometric test, incorporating liveness is a high assurance approach to preventing attacks on the identity proofigng process | ...not limited to: biometric testing with liveness,… |
| 16 | **63A** | 3.1.7 | 24 | 1125 | Federal Agencies are required to be prudent with public finannces and to undertake cost-benefit analyses, by EOs. This requirement should be made | The agency shall complete a cost-benefit analysis in order to demonstrate that selected identity system represents a prudent use of public funds. |
| 17 | **63A** | 3.1.11 | 28 | 1235-1239 | Independent testing is importat, but NIST should appreciate that the best in class algorithms are upated 3 or 4 times each week. Testing every update through a lab takes typically 30 days and requires that the algorithm is stable for the duration of the test. As such, the requirement is not practicable and would serve only to reduce security if it meant that updates could only be introduced to align with available lab testing schedules. NIST should also recognise that lab testing is only a point in time test and does not relate well to the real world environment. External testing is important, but it must be in place together with internal testing and the independent auditing by an approved certification body of related | Replace 1238-1239 with: At a minimum, algorithms shall be subject to internal testing following every update. Relevant processes and procedures for that testng shall be subject to exterenal independent auditing by an recognised expert body. External lab testing may be employed where there is a material change to a system. |
| 18 | **63A** | 3.1.11 | 28 | 1246-1249 | With regards the FMR and FNMR, for equivalence, these need to be set at the same level in the testing of humanoperators<br>and also for hybrid systems. Otherwise, NIST is accepted a different level of assurance according to<br>whether the system us human or uses biometrics, exposing end users of human systems to increased risk and<br>unfairly skewing the decision making process for organisations by not ensuring that selection decisions are based on<br>equivalent performance levels. | |

| | | | | | | |
|---|---|---|---|---|---|---|
| 19 | **63A** | 3.1.11 | 29 | 1273-1276 | Not all PAD test methods will distibguish between a genuine and fake image presented for biometric capture. For example, the use of injection attacks can even provide for the live presentation of a moving face such that an active challenge-response test (randomly asking for head or face movements) can be spoofed. At the very least, the CSP needs to include a liveness test. | ...presentation attack detection (PAD) capabilities and a robust liveness test… |
| 20 | **63A** | 3.1.12 | 30 | 1315 | As a minimum human operators must be retrained and tested whenever there is a change in the threat landscape. For information, we identify 3 or 4 new threats each week, based on out threat intelligence. If a human operator is not trained and retested there can be no confidence in their ability to adapt to the new threat, exposing the organization to risk. Similarly, research shows how the performance of even highly trained expert examiners declines due to the working evironment (fatique and distraction are the most commonly cited factors). For evidence, see Josh P. Davis, Tim Valentine, Human Verification of Identity from Photographic Images, available from https: //onlinelibrary.wiley.com/doi/epdf/10.1002/9781118469538.ch9#accessDenialLayo | ...shall be trained and retested when new threats are identified, and provided resources, and a suitable working environment.... |
| 21 | **63A** | 3.1.12 | 31 | 1336 | The proposed approach is too passive to be effective. Agents need to be trained and retested each time a new threat is detected. Otherwise, the organization is at risk. Additionally, the proposed approach is materially different from that proposed for biometric solutions, thereby undermining equivalent treatment of competing systems. Training and retesting can be undertaken internally, but the relevant processes and procedures supporting that should be subject to independent external audit and certification by a recognised expert body. The current proposals are not sufficient given the nature of the threat landscape. | ...shall be reviewed, trained and retested regarding their ability...whenever a new threat is identified. Retesting may be internal, but the processes and procedures relevant shall be subject to periodic external independent audit by an recognised certification body. |
| 22 | **63A** | 4.1.1 | 36 | 1512 | The Guidelines should reflect the increased vulnerability that comes from a hybrid system. See an excellent note from Professor John Daugman - available at https://www.cl.cam.ac.uk/~jgd1000/combine/combine.html#:~:text=If%20two%20biometric%20tests%20of,the%20net%20equal%2Derror%20rate. When two modalities are combined, one of the resulting error rates (False Accept or False Reject rate) becomes better than that of the stronger of the two tests, while the other error rate becomes worse even than that of the weaker of the tests. If the two biometric tests differ significantly in their power, and each operates at its own cross-over point, then combining them gives significantly worse performance than relying solely on the stronger biometric. | ...each proofing type that is applied. CISPs shall recognise the additional security risks from a hybrid approach and incorporate this into their risk-assessment process. |
| 23 | **63A** | 4.1.6 | 37 | 1549 | The Guidelines should acknowledge that processes 1,2 & 3 provide posssion of a device or account, but do not provide proof as to the identity of the individual. Accounts can be hacked and devices can be stolen or cloned. These process weaknesses should be reflected in a risk assessment for systems using such measures, Processes 4 & 5 are vulnernable to injection attacks (or even PAD attacks) where they do not incorporate a biometric liveness check. Again, this vulnerability risk should be recognised in the Guidelines and incorporated into the risk assessment for systems using these processes. We have shared above links to independent academic research which illustrates the vulnerabilities of human operator models when faced with the increasingly sophisticated threat landscape. The research shows how even expert examiners under lab conditions can be regularly spoofed. As a general point, those processes relying on human agents should be reflecting these well known vulnerabilities in their risk assessments. We would ask that NIST acknowlegde this research in the Guidelines and require that the vulnerabiities be incorporated in the assessments made by organisations. | |

| | | | | | | |
|---|---|---|---|---|---|---|
| 24 | **63A** | 4.1.7 | 38 | 1568 | Video-ident models (video sessions) are easily spoofed using off-the-shelf technologies. This has been well documented, for example see the demonstration by the Chaos Computer Club - https://www.ccc. de/en/updates/2022/chaos-computer-club-hackt-video-ident. As a consequence of this vulnerability being identified several organisations in Germany (notably in healthcare) ceased reliance on video identity solutions. That NIST is accepting of the approach as one which is secure is at odds with the readily available evidence. Where NIST refers to training for proofing agents, the available evidence on difficulties faced by even expert examiners in identifying anomalies should be reflected. The effectiveness of the human will depend on the operational environment, the quality of the training and the performance of the human at that point in time. For example, if they are distracted, tired, not sufficiently well trained or simply not focussed on identifying anomalies then they are unlikely to be effective at this task. There is a sizable body of widely available, peer-reviewed and generally accepted research evidence which shows how even well trained human observers fail to spot significant anomalies. By way of example, see The invisible gorilla strikes again: Sustained inattentional blindness in expert observers, Drew et al, Psychol Sci. 2013 September ; 24(9): 1848–1853. | |
| 25 | **63A** | 4.1.7 | 38 | 1587 | Challenge response systems are increasingly obselete when faced with widely available live injection attack solutions. Youtube offers readily accessible guides to using these solutions to spoof live video systems. The best of these systems will today fool most human examiners over a video connection and the very best will spoof the weakest biometric solutions (thosw which dont incpororate liveness). Challenge response based on random actions provides organisations with a false sense of security and so should not be accepted in the Guidelines. Only passive challenge systems, based on liveness are effective against these solutions. When combined with a voice spoofing tool (AI solutions casn generated effective spooks with 10 seconds or less of an indivual's voice), they will spoof challenges based on questions as well. Additionally, challenge response approaches based on facial moves or head movements may be exclusionary for those with physical challenges. | The CSP shall not rely upon the outcome of a challenge response feature that does not inclide a biometric liveness check. |
| 26 | **63A** | 4.2.1 | 40 | 1661 | The Guidelines should reflect the increased vulnerability that comes from a hybrid system. In effect, when a second subsystem is added this increases the vulnerabilities in the system as a whole. It increases the range of weaknesses which can be exploited by a malicious actor. See an excellent note from Professor John Daugman - available at https: //www.cl.cam.ac.uk/~jgd1000/combine/combine.html. When two modalities are combined, one of the resulting error rates (False Accept or False Reject rate) becomes better than that of the stronger of the two tests, while the other error rate becomes worse even than that of the weaker of the tests. If the two biometric tests differ significantly in their power, and each operates at its own cross-over point, then combining them gives significantly worse performance than relying solely on the stronger biometric. | If a CSP employs a hybrid process, the associated risks shall be incorporated into the risk assessment and effective mitigations will be adopted. |

| | | | | | | |
|---|---|---|---|---|---|---|
| 27 | **63A** | 4.3.7 | 47 | 1866 | Research shows that humans are not automatically effective at identifying signs of coercion or anomalies. As explained above, there is a well kown concept of incidental blindness that impacts human's ability to see low prevalence anomalies. See, for example -https://www.ncbi.nlm.nih.gov/pmc/articles/PMC3964612/pdf/nihms563995.pdf In this research, 83% of expert examiners fail to spot a significant anomaly. This finding is common across research papers. Even under optimal viewing conditions, ID matching performance has a surprisingly high number of errors (e.g., Burton, 2013). Errors further increase with additional real-world challenges such as time pressure (e.g.,Bindemann et al., 2016) and vigilance (e.g., Alenezіet al., 2015). Among a host of challenges to successful ID screening, the Low Prevalence Efect (LPE; e.g., Wolfeet al., 2007) also increases error rates. As we would expect coercion to a rare incident, the evidence would suggest that exen expert examiners will be vulnerable. Training is not suficient, so must be supported by regular testing against specified performance metrics. | ...shall be trained and regularly tested.... |
| 28 | **63A** | 4.3.8 | 47 | 1881 | This is the same as the German Videoldent solution which has been repeatedly shown to be vulnerable to low-skill attacks. See, for example the work of the Chaos Computer Club - https://www.ccc.de/en/updates/2022/chaoscomputer-club-hackt-video-ident. NIST may know that the German Finance Ministry has recently proposed a Bill that would authorise the use of remote biometric automated enrollment for KYC and AML checks in regulated financial markets. This is in response to criticisms from the securoty community of the ease by which remote in person (attended) processes can be spoofed. See https://technologyquotient.freshfields.com/post/102j8r4/a-chance-for-aigermany-greenlights-fully-automated-customer-identification for coverage of the Bill. | The CSP shall undertake a risk assessment of this system and adopt mitigating meaures, including regular training and testing, including against spoofing (penetration testing). |
| 29 | **63B** | 2.2.1 | 6 | 563 | The factors - something you have and something you know are vulnerable to attack. Posession of a device does not verify that the identity of the holder of the device is the legitimate owner - just that they have the device in their possession. Similarly, a password (even a complext one) or OTP simply porves possession of that fact - it not not prove the identity of the possessor of that fact. Biometrics is crucially different. When combined with a robust liveness test a biometric face capture can prove that the person presenting themselves is a real person, that they are present at the time of capture and that their idenity is matched with a trusted authoritative source. Of the three, something you are is the most exacting and robusy against spoofiing and the application of a biometric capture with liveness is the most secure means currently available. Addiing something you have does not increase the level of assurance against spoofing as it is more vulnerable to attack. Logically, the postion proposed in the Guidelines does not hold. Moreover, it increaseds the costs to organisaations without any additional assurance. From the perspective of a cost benefit analysis and the requirement to be able to demonstrate prudence wth public funds, the addition of a requirement for a physical authenticator is contrary to best practice as it adds nothing to the assurance level provided by the biometric (with liveness). | A biometric is recognised as an authenticator when captured using a robust liveness solution. (the remainder of that paragraph can be removed) |
| 30 | **63B** | 3.2.3 | 29 | 1248 | All authentication factors are probablistic. Given the ease by which the other factors can be spoofed (stolen devices, shared passwords etc) possession of either (and both) does not provide for 100% confidence as to the identity of the applicant. Biometric solutions can and are tested against performance requirements, so the probabilities can be known and mitigation taken. However, this is not the case fot the other factors. | Remove this challenge to biometrics as it is common to all factors and in fact it can be more easily managed for biometrics than for other factors. |

| | | | | | | |
|---|---|---|---|---|---|---|
| 31 | **63B** | 3.2.3 | 30 | 1253 | There can be no confidence that possession and knowledge factors constitute secrets either. Possession and knowledge factors are proof only of possession (either device or knowledge) and not identity. There is no certainty that the password or possession based factor are held by the applicant they claim to be. Unlinke possession or knowldge, biometrics does not depend on it remaining a secret. What makes biometrcs so powerful as a method for identity proofing is that an image or a picture can be stolen or scraped from social media, but this does not undermine the strength of an effective biometric capture incorporating a robust liveness test. The concern raised by NIST in the draft is one which relates to confidence in the liveness solution, rather than to biometrics itself. Rather than discriminate against the use of biometrics in this way, it would be wiser for NIST to require that the CSP only deploy biometric solutions with tested and certified liveness incorporated. | Remove this challenge to biometrics as it is not a weakness of biometrics but of the liveness solution. This weakness can be tested for, documented and mitigated, unlike the weaknesses for possession and knowledge based factors. |