Document	Section	Comment
800-63-3A	5.3.3.2	1. The requirement for a CSP to “have a live operator participate remotely with the applicant” is now obsolete. The legacy assumption that a live operator is the best way to surveil user activity is no longer sustainable. Deepfake technology makes it increasingly low-cost to fabricate imagery that will appear to an operator that the process has integrity, creating a false sense of security. The objective, which is to prevent malicious activity by the remote subject, can be accomplished much better by using a variety of automated means. 2. The requirement for a CSP to “employ physical tamper detection and resistance features appropriate for the environment in which it is located.” has been shown to be unachievable during a pandemic, since access to the location of such units becomes impossible. It should be an option for IAL3 to be achieved also using measures which can be shown to be robust against physical tampering with the biometric collecting device, such as man-in-the-middle attacks against the data path from the sensor. Such methods exist and have been shown to demonstrate such robustness.
800-63-3B	5.2.3	1. The clause “While presentation attack detection (PAD) technologies (e.g., liveness detection) can mitigate the risk of these types of attacks, additional trust in the sensor or biometric processing is required to ensure that PAD is operating in accordance with the needs of the CSP and the subscriber.” is not an accurate reflection of the relative risks. It indicates that sensor and processing trust are the main requirement, rather than PAD. However it is now clear that such trust cannot sustainably be relied on, especially when using BYOD capture devices. There are means to simulate the entire functionality and identity of a user device, providing signals that are indistinguishable from those sourced from genuine devices. Therefore, dependence on the integrity of the device eliminates the value of biometrics as a factor truly independent of the possession factor specified in 5.1. To have value as an independent factor, the integrity of biometrics must be entirely independent of the integrity of the device. This places major dependence on PAD defence, and this should be recognised. 2. The clause “The biometric system SHOULD implement PAD. Testing of the biometric system to be deployed

		SHOULD demonstrate at least 90% resistance to presentation attacks for each relevant attack type (i.e., species), where resistance is defined as the number of thwarted presentation attacks divided by the number of trial presentation attacks. Testing of presentation attack resistance SHALL be in accordance with Clause 12 of ISO/IEC 30107-3. The PAD decision MAY be made either locally on the claimant's device or by a central verifier." is already notified for amendment. We note as follows: 2.1 SiInce a biometric system relies (as noted) on a public credential, it is worthless without assuring the genuine presence of the user. Hence PAD is essential. 2.2 A measure of % resistance to presentation attacks per species is not useful. Species divide into two classes - those whose attack methods are acceptably static in time, and those which are not. Those which are static include photographs, high resolution videos on retina screens and masks. They are static because the technology used to create such forgeries are now developed to such a level that further improvements in technology will not affect the quality of the forgery, with the possible exception of masks. IARPA Project ODIN will highlight the degree to which developments in mask technology represent a dynamic threat. For static threats, it is possible to specify a bounded set of tests which must be undertaken, and to specify a Impostor Attack Presentation Match Rate (IAPMR)). This value cannot be specified without specifying a corresponding False Non-Match Rate (FNMR). Both these values must be specified with attention to the use case and to the statistical confidence ratio achievable. For example, a FNMR of 5% combined with a IAPMR of 0.1% measured over a minimum of 1000 tests would be reasonable. A IAPMR of 10% (as recommended in NIST 800-63-3) is far too high to make biometrics a credible security method. However the second class of attack is non-static: these are attacks based on the theft, modification or synthesis of digital imagery, injected without the involvement of the sensor. This attack type may require its own term, since Presentation to the sensor is not involved. We propose a term such as "Reality Attack Detection " (RAD) to distinguish it from PAD. The technology for the creation of such attacks is evolving extremely fast and the space of possible attacks is very large and expanding. Hence it is not useful to define a static test protocol incorporating a fixed number of fixed attacks. Evaluation of the performance of this type of attack resistance (RAD) must be based on an evaluation of:

		-the effort required to accomplish a successful attack -the lifetime of a successful attack -the reproducibility and transferability of a successful attack These variables cannot be usefully thresholded. A skilled and independent test house (such as a Federal Red Team contractor) may usefully evaluate the robustness of a solution against such criteria, and provide an assessment of fit for purpose. 2.3 The clause "The PAD decision MAY be made either locally on the claimant's device or by a central verifier" should be amended. The security of a biometric system cannot reach high levels if the PAD decision is made on the claimant's device, hence the revised standard should reflect an obligation to make the decision by a central verifier. The reason is that a PAD decision made locally on the claimant's device ensures that the PAD algorithm, software or hardware are wholly available to an attacker and are subject to uncontrolled, unsurveilled reverse engineering. It represents handing to the forger the method of detecting a forgery. The inevitable result will be the rapid development of consistently successful, undetected forgeries. This has been proven in practice by the rapidity with which third parties have broken the PAD on sophisticated consumer devices, such as the Samsung S8 Iris authenticator and the Apple iPhone X FaceID, within a matter of days of launch. A second undesirable consequence is that PAD attacks are not observed and there is no possibility of, observing, learning about and responding to promising attack methodologies. A further undesirable consequence is the difficulty in responding to such breaches rapidly by amending the PAD systems, without making such updates very transparent to attackers. For these reasons, PAD on the claimant's device should never be allowed for level 2 or above.
		3. "Biometric comparison can be performed locally on claimant's device or at a central verifier. Since the potential for attacks on a larger scale is greater at central verifiers, local comparison is preferred." This clause needs to be amended. The location of biometric comparison does not affect the scale of attack, it merely changes the type of attack. If biometric matching is undertaken locally, it will be compromised by an attack on the authenticating device, the same type of attack that will compromise authenticators under 5.1. Hence local comparison eliminates the independence of the factor. If the comparison is done centrally, then the attack potential is determined by the strength of PAD,

		irrespective of scale. Therefore for independence of factor, central comparison may be preferred. However the security of biometric systems does not substantially depend on the biometric comparison but on the strength of PAD. Provided that PAD is undertaken centrally, it does not greatly matter where comparison takes place and should not be mandated or recommended.