Comment #	Publication (Base, 63A, 63B,	Section	Page #	Line #	Comment (Include rationale for comment)	Suggested Change
Socure-63_B	63-Base	general			**THEME: Digital identity model** **RECOMMENDATION: Clarify the role of the agency relative to the CSP. Add a discussion of how agencies can use CSP(s) to manage digital identity risk. Include the notion of an identity orchestrator: orchestrates identity activities, but does not conduct proofing, authentication, or verification itself.** **RATIONALE: Many of us understand this and have no problem operationalizing it, but it's foundational to understanding the digital identity model. An informative explanation would be helpful to set the state for less identity minded folks. This is also an opportunity to discuss the possible models an agency may follow to manage risk, like having multiple CSPs that do different or redundant things. The identity orchestrator model may become more prevalent in the next few years as agencies grapple with determining the best path for a given individual, especially with regards to identity proofing. Not all CSPs will provide all forms of identity proofing, so an entity needs to conduct the orchestration to route the individual appropriately. This can be seen as akin to the process of educating agencies to expect they will need to offer multiple authenticators; that model appears to be expanding to identity proofing approaches and CSPs.**	- Review SP 800-63-4 section 4 and adjust to reflect the role of an identity orchestrator. - Update the figures in SP 800-63-4, perhaps adding a new figure to demonstrate an identity orchestrator managing the individuals flow to and between multiple CSPs. - Update figures or add a new figure to show the agency's role. This may require multiple permutations showing the agency acting as the CSP, the agency outsourcing to one or more CSPs, and the agency brokering user interactions with CSPs such as in the case where a user might be redirected during an identity proofing event to a CSP that provides proofing methods that better suits their individual needs. - Review all requirements for accuracy in their application to Agencies, CSPs, the identity orchestrator, or other roles as appropriate.
Socure-63_B	63-Base	2.3.3	8	586	**THEME: Equity** **RECOMMENDATION: Consider additional language regarding the accessibility of identity systems to those with accessibility needs.** **RATIONALE: In the IPD, the only explicit references to accessibility in terms of disabled communities are in are a consultative one in 63A 5.1.5(5), an informative one in the usability sections of 63A and 63B, and in passing regarding trusted referees in 63A. While the 800-63 suite should not set requirements, it should be clear about the intent for identity solutions to serve communities with accessibility needs as part of the "normal" workflow wherever possible and not just as part of the trusted referee process. We believe the best approach to this is to expand the equity section in 63-4 to be more inclusive of accessibility for persons with disabilities and a stated preference for designing workflows that accommodate these individuals. In addition to the proposed language, we recommend including references to applicable law outside of the usability sections. There may be room for additional language in 63A 5.1.3.**	[added to end of 2nd to last paragraph of 2.3.3] In considering the design of, and workflows within, identity systems, preference should be given to including accessibility for individuals with disabilities within the normal workflow wherever possible. This includes support for assistive technologies and accessible design patterns such as screen readers, speech recognition software, and alternative keyboard inputs within the basic workflow as preferential relative to alternative or "failover" workflows that often have higher likelihood of wait times or disruptions of the session in which the individual is engaged. As a part of the primary workflows, testing should include that for equity to ensure that identity services are accessible and usable by all users, including those with disabilities. Additionally, identity system design should consider equity and accessibility in all phases and should implement relevant standards and guidance, such as Section 508 of the Rehabilitation Act and the Web Content Accessibility Guidelines, as appropriate.
Socure-63_B	63-Base	2.3	9	601	**THEME: Fraud mitigation measures** **RECOMMENDATION: Add a subsection 2.3.x on the use of fraud, transaction, and behavioral analytic capabilities.** **RATIONALE: This language is used throughout the suite but isn't clearly defined. For instance, 63A 5.1.1.2(1) provides three valuable examples (device, behavioral, and the DMF) but more context is needed on the breadth of these capabilities and how they should be used. This is true in several section of 63A. 63B provides slightly more information on this. Rather than add bulk to each of these sections, it may be best to include a section in 63 on the expected use. Given the large and increasing role of these measures in the digital identity enterprise risk management, it's worthy of a role this early in the base document. It received, for instance, substantially more attention than usability--for better or worse!**	Fraud mitigation measures seek to lower the risk of fraudulent activity in digital identity processes. The ability to conduct and continually evolve reasonable fraud mitigation measures is a fundamental component of any modern digital identity solution. Capabilities for fraud mitigation commonly include: - correlation of location of IP address and device location, - evaluating data freshness/recency, - efforts to correlate data to determine if it belongs together, - performance for difficult to identify demographics, - fraud capture performance, - ability to confirm fraud capture performance by using feedback to confirm false positives, false negatives, true positives, and true negatives - characteristics from 63B such as device swap, SIM change, ISP porting, etc - presence of a trusted compute module (if seen before with good behavior) - velocity measures to limit rapid reuse of evidence used to perpetuate fraud
Socure-63_B	63-Base	5	23	922	**THEME: Clarity of language** **RECOMMENDATION: Change the name of the section title to reflect that it's about risk assessment and not management writ large** **RATIONALE: This section addresses only risk assessment: what categories of risk are there, how do they impact my final risk categorization, and do I do anything special before coming to my final determination. This is a small aspect of risk management, which is the intent of the suite as a whole.**	5. Assessing Risk for Applications that Leverage Digital Identity

Socure-63_B	63-Base	5.3	36	1375	**THEME: Risk Assessment** **RECOMMENDATION: Adjust the language in the Assurance level tailoring section to be about tailoring controls within an xAL rather than tailoring to create an xAL.** **RATIONALE: Tailoring is extremely difficult. Tailoring individual controls allows for flexibility without relying on (often unjustifiable) claims that the underlying risk has changed from the initial assessment which, presumable, just occurred. The difference between the two (control tailoring within xAL and tailoring of the xAL itself) is that tailoring controls is like saying "I removed my deadbolt because I lock the handle and have a security system" vs "I removed the deadbolt because I haven't seen any burglars around this neighborhood lately." For an agency or IG, the former may have reasonable comparative measures. For the latter, it requires a comprehensive analysis of risk on the internet (the neighborhood) and attackers' intent. NIST should not be promoting adaptation of already subjective risk assessments for convenience, which tailoring of the xALs themselves is prone to result in. Tailoring of the xAL also effectively eliminates all requirements for the entirety of the xAL when in most cases it is just one or two controls presenting the problems for the agency.**	[changes underlined] 5.3. Tailor and Document Assurance Levels Tailoring provides a process to modify the controls within an application's assessed assurance level, implementing compensating controls based on ongoing detailed impact and risk assessments. Organizations SHALL NOT alter the assessed xAL, and organizations SHOULD implement the assessed assurance level as defined in these guidelines. However, these guidelines provide flexibility to allow for organizations to meet specific mission needs and address unique risk appetites and considerations. Therefore, organizations SHALL establish and document an xAL tailoring process to facilitate adjustments of the requirements within the assess xAL. At a minimum this process: 1. SHALL include a structured governance approach to allow for decision-making and conflict resolution. 2. SHALL document all decisions in the tailoring process, including the assessed xALs, modifications to controls within the xALs, and compensating controls in the Digital Identity Acceptance Statement (see Sec. 5.3.4). 3. SHALL justify and document all risk-based decisions or modifications to the initially assessed xALs in the Digital Identity Acceptance Statement (see Sec. 5.3.4). 4. SHOULD establish across-functional capability to support subject matter analysis of xAL selection impacts in the tailoring process. 5. SHOULD be a continuous process that incorporates real world operational data to evaluate the impacts of xAL tailoring. [additional changes may be necessary flowing from these above changes]
Socure-63_B	63-Base	5.4	39	1479	THEME: Monitoring and evaluation RECOMMENDATION: Make a monitoring and improvement program mandatory for agencies. RATIONALE: Consistent with an overall theme of these comments, NIST should move agencies to be better risk managers even where it cannot specify the precise approach to that risk management. While it may be premature to specify the exact nature of the monitoring and the associated metrics, the need to do so should not wait until the next revision. Include language on appropriate metrics.	...organizations SHALL implement a continuous evaluation and improvement program that leverages input from people interacting with the identity system and performance data about the system. Performance monitoring SHALL: - include collection of data on how the performance of deployed identity proofing solutions changes over time, accounting for changes in identity proofing processes. - use these data to evaluate degradation of identity proofing events over time. - evaluate the value of additional identity proofing activities to incremental increase the risk of initial identity proofing errors [NOTE: this is akin to doing step-up authN but for proofing]
Socure-63_B	63-Base	5.4	39	1483	THEME: Monitoring and evaluation and fraud mitigation measures RECOMMENDATION: Include additional language in 5.4 about adjusting to threats at they emerge. RATIONALE: While the existing language provides some examples of the type of monitoring that should be conducted, it would benefit from more robust language to establish expectations based on what we know to be good practices for monitoring and improvement.	In addition, agencies and others involved in the identity proofing process SHOULD: - Regularly review industry sources, such as NIST and other reputable organizations, to stay informed on the latest trends and threats in the cybersecurity landscape. - Conduct ongoing risk assessments: Rather than using periodic assessments, continuously monitor the organization's systems and networks to identify vulnerabilities and determine the level of risk associated with them. This information should be used to prioritize and implement security measures to mitigate risks. - Adopt a proactive security posture: Implement security measures that are proactive rather than reactive, such as firewalls, intrusion detection systems, and network segmentation, to prevent threats from entering the network. - Evaluate and implement new technologies: New technologies and methodologies can provide enhanced security and protection against emerging threats. - Assess the effectiveness of these technologies and implement them where appropriate. - Regularly monitor the effectiveness of security measures and assess the threat landscape to ensure that security measures remain relevant and up-to-date. - Adjust to a changing threat landscape, especially by improving fraud detection capabilities to better account for the threat at any given time
Socure-63_B	63-Base	A.1	43	1589	**THEME: Fraud mitigation measures** **RECOMMENDATION: Include a definition(s) for fraud, transaction, and behavioral analysis capabilities.** **RATIONALE: These are critical concepts but are currently only defined with reference to biometrics**	The process of collecting and analyzing data from actions performed by users of the digital identity system in order to understand patterns of valid use and misuse.

Socure-63A-	63A	5.3, 5.4, 5.5	multip	multiple	THEME: Fraud mitigation measures RECOMMENDATION: Add a subsection requiring a baseline of specific fraud mitigation measures and establishing a baseline. RATIONALE: Fraud mitigation measures, as described in 800-63, are now at the heart of most identity proofing solutions. Some are sufficiently common that CSPs should be deploying a baseline at each IAL and encouraged to do more. Note the requirements placed on IAL1 are substantial. Our understanding of the motivation for the new IAL1 is to create a lower-friction path for users. The approach taken in this comment is to shift the burden from the applicant to the CSP, rather than simply dramatically lowering the bar. The 800-63-4 suite must include baselines for fraud mitigation measures such as these. Failing to include baselines creates too high a risk of technical sufficiency being undermined in procurements. They serve as a signal to procurement officers on how to define minimum technical viability for identity solutions. Absent baselines, the incentives too strong for a race to the bottom.	5.3.x Fraud mitigation measures The CSP SHALL employ a data-driven fraud mitigation model designed to predict the likelihood that a given identity is being used fraudulently at any given time and includes the following fraud mitigation measures that check for: 1. known historical fraudulent use of personal information AND 2. fraud risk indicators for: a. email OR b. phone OR c. address AND 3. associations between collected personal information, such as known associations between email, phone number, and IP address AND 4. risk associated with devices including use of proxy servers, geolocation or spoofed geolocation, and similar attributes; AND 5. measures of velocity in use of information and devices AND The CSP SHALL update the fraud mitigation model at least quarterly based on performance data about the identity solution. CSPs SHOULD use these models to allow decisions based on the totality of evidence that may not be clear based on binary indicators of pass or failure. CSPs SHOULD use behavioral biometrics to additionally lower risk. Agencies SHOULD monitor the efficacy of deploying behavioral biometrics as these technologies evolve. For each of these measures, the CSP SHALL employ equity protections as described elsewhere in this document. ----- 5.4.x Fraud mitigation measures
Socure-63A-	63A	4	6	440	THEME: Digital identity model and identity proofing RECOMMENDATION: Include additional language about how to offer multiple identity proofing workflows and the goals for managing these flows. RATIONALE: We strongly approve of NIST setting an expectation for multiple types and combinations of identity evidence and methods for identity verification. That said, the parenthetical undermines the intent. We believe identity proofing should look more like authentication: offer many and allow user choice. We understand the approaches to identity proofing, especially verification at IAL2, are limited, but NIST should set the expectation that trusted referees is much more of a failover approach and not an approach of choice.	[added to the end of the subsection] Wherever possible, CSPs and organizations SHOULD offer multiple approaches to identity proofing, including identity verification, as part of the default workflow. "Failover" methods that typically have longer wait times and higher friction, such as most trusted referee approaches, should be rare and considered only after other options, as chosen by the applicant, have been exhausted.
Socure-63A-	63A	4.4.1.	14	672, 673	THEME: Fraud Mitigation Measures RECOMMENDATIONS: Clarify "(unattended) using a captured video or photograph and the uploaded copy" means the video is captured by the CSP, not the applicant. Photograph should be removed as all comparisons should be via video or multiframe capture. Also clarify consent conditions. RATIONAL: All capture for comparison should be video or multiframe; single frame captures are too easy to spoof. All capture must be done live within the session and not allowing upload (other than of the evidence). Consent must be conducted in the same session as the capture.	"The CSP operator may interact directly with the applicant during some or all of the identity proofing event (attended) or may conduct the comparison at a later time (unattended) using the copy of the evidence provided by the user and a video or other multiframe capture obtained and maintained by the CSP during the session. If the comparison is performed at a later time, steps are taken to ensure the captured video was taken from the live applicant present during the identity proofing event and that consent for the capture and storage was obtained by the CSP during that session."
Socure-63A-	63A	5.1	16	694	THEME: Monitoring and evaluation RECOMMENDATION: Add a subsection to this section to address monitoring and evaluation of the identity proofing solution. RATIONALE: While 63-4 5.4 contains some language on monitoring and improving, the document would benefit from additional explicit information on monitoring and evaluation of the identity proofing solution. Knowing the performance of solutions typically degrades over time, measuring this performance is the only way to ensure it continues to meet the expected service levels and risk mitigation. Moreover, many of these solutions are outsourced, and without appropriate evaluation and performance measurement, good procurement decisions cannot be made. Note this deserves its own subsection because it is not just about security (nor privacy, equity, etc.) but is about the service as a whole. In addition, defining and labeling fraud to provide feedback to fraud detection models is critical to stopping fraud as discussed the white paper: Fraud Definitions and Rigorous Labeling are Vital to the Public Sector (https://offers.socure.com/fraud-definitions-and-rigorous-labeling-are-vital-to-the-public-sector.html)	5.1.x Identity Service Auditing and Performance Monitoring Organizations SHALL implement a monitoring and evaluation program that leverages input from people interacting with the identity system and performance data about the system. To conduct proper monitoring and evaluation of identity solutions, the Agency: 1. SHALL implement monitoring and evaluation procedures for the identity service to identify any potential weaknesses or vulnerabilities. 2. SHALL use quantitative performance metrics as decision criteria in selecting identity solutions, particularly in procurements. 3. SHALL retrospectively study the benefits and cost associated with chosen identity proofing solutions, including quantitative analysis of the costs associated with both false accepts and false rejects. 4. SHALL shall clearly and accurately define and label fraudulent transactions to understand fraud within the environment and provide feedback to fraud detection models 5. SHOULD conduct testing as follows: a. Whenever possible, the Agency SHOULD conduct tests using historical data as part of procurements to approximate real-world results of prospective CSPs based on the agency's own populations. b. Whenever possible, the Agency SHOULD conduct tests in production to determine real-world results of prospective CSPs based on the agency's own populations. Ideally, these can be part of multi-stage procurements. c. the Agency SHOULD only use simulated tests only when tests based on historical data and live tests are not possible. To assist in appropriate performance monitoring, CSPs: 1. SHALL maintain a record of the adjudication of any identity proofing, authentication, or federation event, subject to system data retention requirements 2. SHALL maintain a label on all such records, through monitoring and evaluation, of whether such an adjudication was

Socure-63A-	63A	5.1	~~16~~	695	**THEME: Monitoring and evaluation** **RECOMMENDATION: Add a subsection (or include in new performance monitoring subsection) to address baselining of performance** **RATIONALE: Too often agencies attempt to measure performance but don't have sufficient baseline to understand how various solutions affect outcomes. Providing guidance around how to establish a baseline (and regularly measuring against that baseline regularly) can help manage risk more effectively over time**	Agencies SHALL understand and document the existing performance and fraud rates in current systems to create a baseline before making significant changes to identity solutions. While many methods may be deployed to achieve this, baselining for a specific identity solution SHOULD: - categorize the population or history of transactions based on how much risk is present relative to rest of the population over time; that is, divide the total history of transactions into groups based on how likely they are to be fraudulent - analyze these categories to understand performance of the solution, both against fraud and effectiveness of methods that introduce friction - determine the extent to which fraud is captured in the riskiest categories CSPs shall then determine thresholds for performance and fraud within the context of business objectives and tolerance for risk and establish whether friction is being placed on the appropriate subset of transactions. CSPs SHALL ensure equity within identity solutions by using model governance methods, such as the FTC's Algorithmic Impact Assessment, to determine whether protected classes may be inequitably impacted by the employed methods CSPs SHALL ensure reasonable methods are used to establish the protected classes against which equity is measures, such as the CFPB's implementation of the BISG methodology
Socure-63A-	63A	5.1	16	695	THEME: AI/ML RECOMMENDATION: Add a subsection to this section to address the use of AI and ML in identity proofing solutions. RATIONALE: Over the next 5 years AI/ML are the most of all fraud mitigation methods to grow and establish themselves as the norm. With an expected reduced reliance on biometrics, it is very likely that AI/ML will fill this gap to attempt to appropriately mitigate risk. While the field may be too immature to apply SHALL statements, it is reasonable to impose SHOULD statements on agencies to address this growing field.	5.1.x Requirements for use of artificial intelligence and machine learning Artificial intelligence and machine learning systems are engineered or machine-based systems that can, for a given set of objectives, generate outputs such as predictions, recommendations, or decisions influencing real or virtual environments. [AI RMF] AI/ML are increasingly used in common applications involving human behavior, including in identity systems. If AI/ML is used, the CSP SHALL evaluate use of AI/ML systems in its identity systems. In doing so, the CSP SHOULD use the NIST AI RMF as a guide to understanding and managing risk in implementing AI/ML systems and the CSP SHOULD monitor for additional NIST and related publications on AI/ML (such as the FTC's Algorithmic Impact Assessment), including for information on measurement and evaluation and technical standards. Furthermore, the CSP SHOULD: - Assess the quality of the data used for AI/ML models for accuracy and effectiveness. Organizations should ensure that the data they use is relevant, up-to-date, and unbiased. - Conduct model validation to ensure they are accurate and effective. This may include testing the models using real-world data, evaluating their performance against established metrics, and verifying their results with manual review. - Incorporate security and privacy. AI/ML models can store and process large amounts of sensitive data. It is important to ensure that the privacy and security of this data are protected by implementing appropriate data protection measures, such as encryption and access controls. - Review for and expect explainability, as AI/ML models can make complex decisions that may not be immediately apparent to users. These models must be transparent and explainable, so that users can understand how and why decisions are made. - Consider integration with other systems to ensure their effectiveness and efficiency. This may include integrating the models with existing identity proofing systems, biometric authentication systems, and other relevant systems.
Socure-63A-	63A	5.1.1.2(1)	17	733	THEME: Fraud mitigation measures RECOMMENDATION: Make deployment of fraud mitigation measures mandatory RATIONALE: At this point in the maturation of identity proofing solutions, all systems should use at least some fraud mitigation measures. Any solution that doesn't is likely under-mitigating risk. While this market may not be mature enough to specify the exact set of mitigations, using them should be mandatory. Additional information is in a later comment proposing a new subsection in section 7. Note there is more here than the mention of behavioral analytics under the automated attack prevention subsections and is in a different class of protection than web application firewalls and the like.	"...Agencies SHALL employ additional fraud mitigation measures to understand and reduce the impact of fraud from identity proofing errors. Agencies SHALL collect data on the performance of additional fraud mitigation measures. At least annually, Agencies SHALL evaluate the performance of additional fraud mitigation measures using quantitative methods and update the set of measures based on quantitative performance. and, at end of the list item, "For more information on fraud mitigations, see section 7.3."
Socure-63A-	63A	5.1.1.2	17	742	THEME: Fraud mitigation measures RECOMMENDATION: Include recency of data as a factor in how fraud mitigation measures are used. RATIONALE: The trend in fraud mitigation has been to leverage fraud mitigation measures and increasing the use of real-time or near-real time data sources, such as through signals sharing. This can help eliminate fraud much earlier and should receive a call out. In addition, this should involve agencies providing feedback on identified fraud (and false negatives) and fraud trends to incorporate into the CSP or other providers' processes.	Agencies and CSPs SHALL consider the recency of data in assessing their value in the identity proofing process. Agencies SHALL consider data recency for fraud mitigation in evaluating identity solutions. Agencies SHOULD give a greater weight to solutions that can leverage real-time or near real-time known status for fraud data, identity attributes and identity evidence, like phone records. Agencies SHOULD provide feedback on identified fraud (and false negatives) and fraud trends to CSPs to incorporate into modeling and other decision making. Generally, CSPs should assign more weight to attributes and other data within models when they have been confirmed more recently and less weight to use of data as it ages without updated confirmation of that data.

Socure-63A-	63A	5.1.3	19	793	THEME: Equity and fraud mitigation measures RECOMMENDATION: The draft places the burden of assessing whether "the elements of [an] identity service" are either inequitable or not, without clearly defined standards or definitions of key words such as "equity", "groups," "access," "treatment," and "outcomes." CSPs should be held accountable to the same, objective, measureable standards so that agencies may have assurance in their assessments. In comparison, the well-established fair lending and fair housing legal frameworks both define protected classes and types of overt and inadvertent discrimination. There are expectations that businesses subject to these laws not only pro-actively design their products and processes for fairness, but also retrospectively test them for equitable results across the defined classes. Also, the draft does not distinguish between inequities that stem from agency actions, meaning how they may use the identity service. Agencies will still control aspects of identity proofing that may impact effectiveness of an identity service. For example, the digital user experience may be more difficult for certain types of users, from inaccessible language for less educated persons to prejudicial or unfriendly language to visual designs that are harder for the elderly to comprehend. If a CSP is to assess the outcomes of the use of its service, it may need to reflect upon the context in which its services are deployed. This requires a feedback loop from the agency. Finally, the expectation of mitigation measures could be narrowly construed to mean singular, post hoc measures. In comparison, the financial services sector has a mature, lifecycle approach called model risk management ("MRM"). Entities using quantitative models to make decisions must develop governance spanning all stakeholders, processes to document and validate methodologies, control framework, and clear risk quantification. The fulsome expectations of MRM are not only useful to regulated entities, but they also minimize the possibilities of wide variance and gaps in how entities interpret the standard. RATIONALE: This approach will prevent up front rejection of edge populations and reduce friction in the flow while still detecting fraud. For instance, name translated for transliterated from other alphabets often have spelling discrepancies	5.1.3(x). The CSP SHALL consider equity in making determinations of fraud mitigation measures. The CSP SHOULD establish categories of users in edge populations and measure performance of those categories against established baselines to determine and monitor impacts and bias within the system and maximize inclusivity. The CSP SHOULD consider established frameworks that define protected classes and types of overt and inadvertent discrimination, such as those used in fair lending and fair housing legal frameworks and the model risk management ("MRM") lifefcycle approach used in the financial services sector.
Socure-63A-	63A	5.1.4	20	830	THEME: Clarity of language RECOMMENDATION: Provide additional context to make clear the expectation of applying the appropriate baseline. RATIONALE: While agencies are likely to understand what applying the baseline means, many of those implementing this guidance will not and may believe that the 800-63 suite does not properly address underlying security. This should not change the requirement, but signal to those less versed in NIST guidance what this requirement is trying to achieve.	"The CSP SHALL assess the risks associated with operating its identity service, according to the NIST risk management framework [NIST-RMF], and apply an appropriate baseline security controls, including, but not limited to, those involving privacy impact assessments, data protection measures, access controls, logging, encryption, and retention."
Socure-63A-	63A	5.1.6	21	869	THEME: Evidence validation and fraud mitigation measures RECOMMENDATION: Add a clause to allow a telephone number to be used for validation when it can be shown to have low risk via application of fraud mitigation measures. RATIONALE: Provide options to reduce friction on the identity proofing process if certain additional fraud mitigation measures are employed. This can be a boon to edge case users that often cannot have their phones validated by standard means but still present low risk. It can improve equity without an increase in risk.	In the event an applicant does not have a phone number that can be validated in records, an enrollment code can still be sent the phone number provided by the applicant if ALL of the following hold: - The CSP has determined through fraud mitigation measures that the supplied phone number has a low risk - The CSP has, through fraud measures, determined with high likelihood that the applicant has current possession of the device associated with the supplied phone number.
Socure-63A-	63A	5.1.6(3)(b)	21	877	THEME: Clarity of language RECOMMENDATION: Avoid putting normative requirements in parentheticals. RATIONALE: While a minor detail, parentheticals are often read as asides or afterthoughts	"...containing an appropriately constructed session ID of at least 64 bits of entropy;"
Socure-63A-	63A	5.1.8	23	929	THEME: Biometrics RECOMMENDATIONS: Clarify biometric deletion request allowance RATIONALE: The current language states only that the CSPs allow a request, does not account for the attack vector in which an attacker can continually delete their image and immediately reuse it	CSPs SHALL allow individuals to request deletion of their biometric information at any time, except where otherwise restricted by regulation, law, or statute. The CSP MAY deny this request if the biometric information is known to have been used in attempts to commit fraud.
Socure-63A-	63A	5.1.8	23	943	THEME: Biometrics RECOMMENDATIONS: Narrow requirement on public availability of all biometric system testing (#10) RATIONAL: The current language is overbroad and risks unintended consequences. For instance, testing may occur daily for new clients or potential new model parameterization, creating a flood of testing results that do not provide additional insight into the biometric system performance. Note also that #12 is a repeat of #10.	[NIST should either remove this requirement or specify a testing program to which it applies. As written, it would apply to a developer debugging at their desk and running a test. There is no definition of what such a "performance and operational test" would be, making it a problematic requirement that gives little guidance to Agencies, CSPs, or other identity solution providers."]
Socure-63A-	63A	5.1.8	23	955	THEME: Biometrics RECOMMENDATIONS: Disallow single frame capture for liveness RATIONAL: The current language does not prohibit liveness testing with single frame comparison	Add to #2 "The CSP SHALL NOT use single frame capture methods to establishing liveness detection."

Socure-63A-	63A	5.1.8	23	958	THEME: Biometrics RECOMMENDATIONS: Require facial matching to known fraudsters RATIONALE: Understanding this has been a contentious topic, comparing the captured biometric of an applicant to that of those with known fraudulent use is the single most effective fraud mitigation strategy available. NIST should be requiring this, but should put extremely tight constraints on the matching sensitivity to ensure equity and minimal false positive matches.	4. CSP SHALL compare the collected biometric to a corpus of known fraudulent of attempts or biometric information connected to other personal information. The CSP SHALL meet a performance threshold for biometric usage of 1:100,000 for false match rate.
Socure-63A-	63A	5.3.3	27	1068	THEME: Evidence Validation RECOMMENDATIONS: Clarify that automated methods can be used to validate FAIR evidence RATIONAL: The current language suggests that human intervention is required to validate FAIR evidence ("by visual inspection by trained personnel")	The CSP SHALL validate the genuineness of each piece of FAIR evidence by one of the following: 1. Visual inspection by trained personnel 2. The use of technologies that can confirm the integrity of physical security features or detect if the evidence is fraudulent or has been inappropriately modified
Socure-63A-	63A	5.3.4(2)	27	1084	THEME: Verification and fraud mitigation measures RECOMMENDATION: Eliminate this IAL1 option for verification OR strengthen it through additional fraud mitigation measures. RATIONALE: Control of a poorly protected social media account seems far too weak to accept as successful verification without additional controls. For instance, many individuals have, for one reason or another, emailed a photo of their driver's license to someone. Losing control of an AAL1 email account would then provide an attacker all they needed to assert the photo of the STRONG evidence, self-assert core attributes regarding a piece of FAIR evidence (such information is almost assuredly contained in an personal email account), and verify via the same AAL1 email account that was taken over. The goal here is to reduce the burden on the user while raising the burden on the CSP in the background to compensate for the additional risk. This account being evidence (that is, validated in records) does not seem to be a significant improvement	[Remove 5.3.4(2) or increase the strength by requiring additional fraud mitigation measures, such as:] 5.3.4(2) Demonstrated...protocol. If verifying via this method the CSP SHALL also implement additional fraud mitigation measures. These measures SHALL include: - success and reject rates, including initial and final adjudications if additional or reprocessing occurred - pass rates, including for each process step - fail rates, including for each process step - dropoff, including for each process step - time to resolution - false positive and negatives - correlation of location of IP address and device location, - checks/metrics for velocity, - evaluating data freshness/recency, - characteristics from 63B such as device swap, SIM change, ISP porting, etc These measures SHOULD also include: - performance for difficult to identify demographics, - presence of a trusted compute module (if seen before with good behavior)
Socure-63A-	63A	5.3	27	1089	**THEME: Risk Assessment** **RECOMMENDATION: Add a subsection on protecting IAL1 accounts with AAL2.** **RATIONALE: The new IAL1 creates a misalignment between the xAL# mappings. IAL1 accounts can have personal information, which needs to be protected at AAL2. This must be made explicit. This should likely be stated in both 63A-4 and 63B-4, and perhaps 63C-4.**	5.3.x. Binding of IAL1 accounts to authenticators If the IAL1 identity proofing session results in the retention of any personal information or other information that might be considered sensitive, whether provided or self-asserted, it SHALL be protected by] AAL2 authentication to allow a return to the service.
Socure-63A-	63A	5.4.3, 5.5.3	28, 30	1118, 11	THEME: Evidence Validation RECOMMENDATIONS: Require validation of FAIR evidence RATIONAL: The current language does not require validation of FAIR evidence	The CSP SHALL validate the genuineness of each piece of FAIR evidence by one of the following: 1. Visual inspection by trained personnel 2. The use of technologies that can confirm the integrity of physical security features or detect if the evidence is fraudulent or has been inappropriately modified
Socure-63A-	63A	10	5193	1703	THEME: Equity RECOMMENDATIONS: Describe the importance of testing for equity and provide examples of successful testing regimes RATIONALE: The current description-mitigation approach is important but provides little practical guidance for addressing equity outside of the limited set of examples. Guidance toward additional resources can help build competence in testing models for equity impacts. This includes testing for correlation effects relative to information value in the model. For example, ensuring that a model breaks correlation of zip code with race to avoid zip code unintentionally serving as a proxy for race and driving inequitable outcomes.	[add language] Ensuring equitable treatment in identity solutions has proven a complex challenge, but significant research has gone into this problem, to include continuing efforts from the Consumer Financial Protection Bureau on defining a methodology for establishing a proxy for vulnerable populations and how to test for impacts to those individuals. At minimum, classes should be defined, and models should be tested with each released iteration to ensure that being a member of a subgroup is not a significant driver in a modeling decision. To ensure successful implementation, CSP must continually update methods and conduct research to keep pace with this evolving area of digital identity work.
Socure-63A-	63A	7	39	1334	THEME: Threat Mitigation RECOMMENDATIONS: Include a new subsection 7.x to address the emerging threat mitigation technique of behavioral characteristics RATIONAL: While behavioral characteristics are lightly deployed thus far, by the time of the next revision, they will be mainstream. This revision should include some discussion of their appropriate use.	7.x Behavioral Biometrics Behavioral biometrics are increasingly part of identity solutions and are likely to provide substantial threat mitigation value in the coming years. Behavioral characteristics look at session interactions and assess risk based on the behavior of the user in the session. For example, mouse movement, bot detection. Typically, none of the behavioral characteristics on their own will binarily trigger a failure, but many may contribute to an assessment that flags a transaction as likely fraud, either failing the transaction or triggering additional friction. Agencies should be aware of when CSPs are using these messages and incorporate performance measures for them into procurements, conduct continual testing, and assess how behavioral biometric approaches impact performance metrics described elsewhere in this document.