Comment Template for: NIST SP 800-63-4 Suite (Initial Public Draft)

Please submit responses to dig-comments@nist.gov by March 24 April 14, 2023

Organization:	Institute for Law, Innovation & Technology (iLIT), Temple University, Beasley School of Law, and the Digital Welfare State & Human Rights Project, Center for Human Rights and Global Justice (CHRGJ), NYU School of Law	***Note: Please see the accompanying Word document for citations and further references.***
Name of Submitter/POC:	Victoria Adelmant	
Email Address of Submitter/POC:	[REMOVED]	

Comment #	Publication (Base, 63A, 63B, 63C)	Section	Page #	Line #	Comment (Include rationale for comment)	Suggested Change
1.a	63-Base	Note to Reviewers, Introduction	ii, 3	148, 155, 353	While SP 800-63-4 may be used by private sector entities, the primary audience is understood to be federal agencies delivering missions in the public interest. References to 'consumers' within the Guidelines reflects a commercial, transactional relationship that does not align with heightened obligations that fall on government agencies delivering essential public services including welfare, education, and healthcare. This may include an obligation to "do no harm;" obligations to ensure accountability and transparency; and obligations to ensure equal treatment and non-discrimination. This does not preclude the protection of consumer rights, including those enumerated under Executive Order 1368; however, the rights held by individual persons affected by digital identity systems are much broader, and this should be reflected consistently throughout the Guidelines.	Adjust language referencing "consumers" to "persons" or "users".
1.a	63A	Note to Reviewers	ii	151, 158	See above comment.	See above suggested change.
1.a	63B	Note to Reviewers	ii	146, 153	See above comment.	See above suggested change.
1.a	63C	Note to Reviewers	ii	144, 151	See above comment.	See above suggested change.
1.b	63-Base	5	23	929–39	The definition of the initial user population, as well as identification of sub-groups within this population who may be particularly vulnerable to inequities, is crucial to the success of the risk management framework. If this population is defined too narrowly, or the agency chooses to focus on the wrong subset of individuals, then the risk management process will fail. NIST should encourage agencies to broadly define this population as all who may be vulnerable to inequities. Agencies should also be obligated to take notice of emerging patterns of inequities and vulnerabilities, which may not always map cleanly onto existing patterns of historical marginalization or social exclusion.	Expand guidance on defining the "overall user population." Clarify that in defining the user population for assessing equity risks, the CSP should consider "groups of users within the population whose shared characteristics may cause them to be subject or vulnerable to inequitable access, treatment, or outcomes when using that service." Further provide guidance that in considering mitigations, any mitigations that result in significant burdens being placed disproportionately on marginalized groups may still give rise to equity concerns, and that the appropriate mitigation may be to reconsider the initial assurance level selected to adopt less onerous requirements.
1.b	63A	10	51	1713–14	See above comment.	See above suggested change.
1.b	63B	1.1	74	2446	See above comment.	See above suggested change.
1.b	63C	11	66	2084	See above comment.	See above suggested change.
1.c	63-Base	2.3.3	8-9	554–586	Some marginalized groups and individuals have genuine safety concerns about participating in any form of digital identity system, and agencies should be encouraged to consider the extensive impacts that inequitable access can have on different aspects of rights. For instance, non-citizens, including asylum seekers and refugees, suffer extreme vulnerabilities in accessing government benefits they are entitled to receive. These vulnerabilities are often exacerbated by the establishment of digital identity systems to deliver those vital benefits. Yet, non-citizens are not identified by name in the definition of equity. Executive Order 14012 of February 2, 2021, on Restoring Faith in Our Legal Immigration Systems and Strengthening Integration and Inclusion Efforts for New Americans, specifically calls for the elimination of "sources of fear and other barriers that prevent immigrants from accessing government services available to them." The omission of non-citizens, including asylum-seekers and refugees, as well as new Americans, fails to give effect to this commitment.	Clarify the stakes of equity considerations by stating that it is the person's ability to be fully included in digital and part-digital services.
1.c	63-Base	2.3.3	8	570–573	See above comment.	Add informative guidance that equity considerations relate not only to the exacerbation of inequities for historically marginalized and underserved groups, but that challenges related to digital access can also create new inequities and new cycles of exclusion for undefined groups, including, inter alia, those with low digital literacy, those without reliable access to the internet, and those who choose to opt-out of using certain forms of biometric authentication
1.c	63-Base	2.3.3	8	562	See above comment.	The category of those who are "otherwise adversely affected by persistent poverty or inequality" should be further expanded and detailed to specifically name vulnerabilities, including explicitly specifying those who are non-citizens.

1.d	63-Base	5	23-24	930, 967, 977, etc	Despite the fact that the "adverse impacts of failures in identity proofing, authentication, and federation" are the sole source of risks covered in the risk management process, these failures are not clearly defined. Even if an individual does not experience a failure in proofing or authentication, for instance, these processes might nonetheless be experienced as very burdensome and may discourage certain groups from accessing services. A definition of risk should therefore be provided within the risk management framework, which should encourage organizations to look beyond questions of technological failures. For instance, an attempt at identity proofing which took over an hour might not represent a failure of the proofing process, but could be considered a failure against the goals and objectives of the digital identity system.	Clearly define what a "failure of each function in the identity system" means. Provide more guidance that "failure" should be understood as more than a technical failure or a failure of proofing or authentication.
1.d	63-Base	5	23	924–927	See above comment.	A definition of risk and clear examples of potential harms should be provided, and organizations should be encouraged to consider all of the possible impacts of each function in the identity system.
1.e	63-Base	5			The selection of assurance levels is the key stage during which organizations' choices about identity proofing and authentication create risks of exclusions and harms. If assurance levels are set too high, this creates additional barriers to access and will be a key mechanism through which marginalized populations will be more likely to be excluded and unable to access key services. Selecting IAL3 and AAL3, for example, requires individuals to submit to a more rigorous identity proofing process and more burdensome authentication requirements each time they access the service. Each assurance level heightens data requirements that will likely act as further obstacles for certain populations. While we welcome the comment that "if a failure to enroll a legitimate applicant could lead to excessive harm, organizations should assess whether lower-assurance identity proofing processes would be appropriate" (Line 1287), we encourage NIST to treat this as a primary part of the entire xAL selection process, and not as a secondary mitigation or tailoring technique.	Equity should be mainstreamed into the initial xAL process rather than concentrated within the tailoring process, with equity explicitly referenced and discussed throughout Section 5 and not only at Section 5.3.1 of SP 800-63-4. Section 5 should clarify that equity impacts shall inform each step in the selection process, including the initial selection of the assurance level. Organizations should not be encouraged to undertake selections solely "based on cybersecurity risk and mission needs"; this current formulation emphasizes cybersecurity and mission needs as the main consideration (i.e. Line 1180) and situates equity as an afterthought.
1.e	63-Base	5.1.1	24		See above comment.	Equity considerations should guide organizations' initial impact assessment process—understanding impacts necessitates an understanding of how impacts are distributed and whether there are differences in different groups' experiences. Section 5.1.1 ("Identify Impacted Entities") currently inadequately addresses these questions. Section 5.1.1 should encourage organizations to identify which groups are most affected, assessing and documenting whether marginalized and historically underserved groups suffer disproportionate impacts from anticipated failures and risks.
1.e	63-Base	5.1.2	25-26		See above comment.	Section 5.1.2 ("Identifying Impact Categories and Potential Harms") should include a specific reference to the harms felt by marginalized communities. Currently, the harms to individuals unable to access government services are encompassed in "damage to mission delivery" (Line 1070), but the harm involved when individuals are unable to access government services should be treated as a category of its own.
1.f	63-Base	Note to Reviewers	ii	148–155	The current emphasis on "optionality and choice," including supporting "multiple authenticator options to address diverse consumer needs," for example, is an important step to advance equity, reduce some risks of exclusion, and minimize frictions that result from limited options. But optionality should not obscure the importance of minimizing barriers in the first place. The crucial determinant of the barriers and exclusion caused through proofing and authentication is the level of assurance selected. If proofing or authentication assurance for a service is set at a high level, this will create barriers to access. The onus should therefore be on the organization to determine the least invasive means necessary for proofing and authentication.	Emphasize that providing for optionality and choice is important but not sufficient to mitigate the risks of harm which arise from higher assurance levels. Entities should carefully consider opting for a high IAL or AAL while providing for alternate options, as this approach does not completely mitigate the barriers which result from the increased proofing and authentication burdens. Entities should be encouraged to determine and apply the "least restrictive means necessary for proofing and authentication" to balance the equity risks presented by such barriers and exclusionary effects with security risks.

1.g	63-Base	Introduction	3	351	The Guidelines make infrequent reference to physical structures and in-person activities, although in practice these components significantly impact the equitability of a digital identity system. The existence of a digital identity system independent of the physical world is not inevitable. We lack empirical evidence suggesting that the need for physical structures and in-person support to users of digital identity systems will wane in the near future, yet, the Guidelines make oblique statements about the physical world without acknowledging that the persistent need for physical assets should be a planned-for eventuality and be incorporated throughout the Guidelines (see further below at 2(a) and 3(f)). The need to retain in-person channels within digital identity systems has been recognized in many contexts. For example, in the European Union, which is currently considering a new digital identity regulation (eIDAS 2.0), independent experts are calling for strong non-discrimination protections to recognize and respect the rights of EU citizens and residents who do not wish to use the online digital identity model and would prefer to exercise their rights and receive entitlements through alternative avenues. The European Parliament adopted this position in its most recent proposal in the negotiations, affirming that "[u]sing the EU wallet will always be voluntary. MEPs also want to ensure that citizens who choose not to adopt it are not treated differently to those who do." In the United States, amidst emerging evidence of exclusions arising from remote identity proofing services, the Office of Inspector General for the U.S. Postal Service (USPS) released a 2022 report on the potential role of the vast physical network of USPS locations throughout the country, including serving as "a fallback option for government customers who have failed remote identification verification or prefer in-person interaction." Meanwhile, the White House OSTP Blueprint for an AI Bill of Rights calls for "mechanisms for human consideration and fallback, whether in-person, on paper, by phone" as an essential way of ensuring that services remain accessible. And in March 2023, Pennsylvania's Department of Labor and Industry indefinitely extended a popular program offering unemployment compensation applicants in-person appointments, initially launched in May 2022. The program has served nearly 34,000 claimants during that time.	Delete the reference to "blur" between virtual and physical worlds. Add clearer language that emphasizes the equity benefits of in-person, offline support. Include physical assets and trained in-person personnel, alternative in-person offline identity proofing and authentication options, and similar "physical world" components as foundational, permanent, valid options for establishing and asserting identity and among the mitigation measures that should be integrated in risk assessment impact analysis. Add a requirement that "Entities SHOULD research and consider how the use of offline or alternative identity proofing and authentication support (including in federated systems) can be integrated into digital identity systems, including how these features of the broader identity documentation ecosystem can mitigate identified risks, particularly risks to individual users, taking into account their specific and diverse needs."
1.h	63-Base	5	23	Line 922 et seq.	In order to better integrate equity considerations into the digital identity risk management model (see Lines 204–05), an abundance of caution with respect to the application of digital identity models in specific sectors is warranted. A similar approach is currently under consideration in the EU's proposed Artificial Intelligence (AI) Act, which classifies certain sectors and applications of AI tools as high risk, including in education and law enforcement. The Guidelines already make reference to heightened risk considerations for other purposes, for instance with respect to "high-risk actions" and the associated need for heightened assurance in identity proofing (SP 800-63A-4, Lines 371–72). While it is welcome that the Guidelines include normative guidance on the inclusion of individuals using the system within the consideration of "impacted entities" in initial impact analysis (Lines 988–89), leaving the assessment of the vulnerability of user populations to the sole discretion of agencies (see Line 930) is a missed opportunity to provide heightened protection for inherently vulnerable user populations such as immigrants or in sectors like social security and health that meet critical survival needs of user populations. Taking into account the benefits of a normative goal to scale the Guidelines to find wide application in federal agencies and other state, municipal, tribal and private entities, realizing this aim should not come at the expense of reckoning with the heightened vulnerability of user populations for specific service delivery sectors.	Include a definition of "high-risk sector" for the purposes of digital identity models within which individual users face heightened risks of harm. High-risk sectors are considered "critical" or "essential" where a disruption in service would result in injury to health, safety, security or economic well-being of individuals. The list of high-risk sectors may fluctuate based on external environmental, economic, social or political factors, and the Guidelines should reflect this reality. Lines 957–959 list several reasons why an organization might revisit certain steps in the risk management process, but do not reference user feedback or events, such as a pandemic, that would make access to specific organizational services within particular sectors (in this case health or labor, for instance) acutely needed. Guidance on the risk management process as a dynamic enterprise which can diverge from the "stepwise" approach should reference high-risk sectors, and the iterative process should explicitly incorporate user feedback and complaints (see below at 5(i)), aligned with guidance on consultation methodology and access to remedies (see below at 6), to assess the risks that are inherent to the sector or field of application for a digital identity system.
1.h	63C	5.5	31	1130–1133	See above comment.	Furthermore, following the initial impact assessment, analysis, and xAL selection, the Guidelines over rely on the Senior Agency Official for Privacy (SAOP) to identify and mitigate sector- or agency-specific risks dynamically (and only in relation to privacy risks, without consideration of the intersection between privacy and equity in many cases) (e.g. SP 800-63C-4 at Lines 1130–1133 and at Section 9.4), without differentiating the qualifications, approach, capacities, resourcing or documentation requirements for actors in these crucial roles in different sectors (like immigration, health or education).
1.h	63C	9.4	58		See above comment.	See above suggested change.
1.h	63C	5.5 & 6.2.5.2	30, 45		See above comment.	In federated systems, IdPs and RPs with a role in the immigration system specifically should be required to adhere strictly to anti-tracking and anti-profiling technical measures in SP 800-63C-4, Sections 5.5 and 6.2.5.2 (covering PPI). The Guidelines recognize the risk that IdPs and colluding RPs will build tracking profiles of subscribers, but the risks associated with tracking vary depending on the particularities of the sector. (See further below at 4.)

2.a	63A	4.3	9		People who live in poverty, people who are formerly incarcerated, immigrants, and people of color are less likely to have up-to-date forms of official ID. In any document verification step that may restrict access to government services, individuals should always be able to easily access an alternative method for proving their identity. In particular, in-person options for enrollment and identity proofing processes are crucial to ensure that people who are unable to use digital remote options (e.g., people who have low levels of digital literacy, lack reliable access to the internet, etc.) are able to access services. As the Office of Inspector General of USPS notes, on-site in-person proofing can "provide a fallback option for government customers who have failed remote identification verification or prefer in-person interaction. It would also help vulnerable citizens with no or limited credit history, or without access to broadband Internet, verify their identity." The United Kingdom Government's recent experience with a federated digital identity system provides a cautionary tale as to the importance of retaining in-person proofing options. Gov.Verify (known as "Verify"), the government's now defunct flagship identity verification and authentication platform, allowed people to choose from a list of five identity providers (commercial organizations, such as a bank, or the Post Office) who would undertake identity proofing using a variety of evidence and methods. The Verify system was used by several government agencies, including by the welfare agency to provide LOA2 verification for online claims for unemployment benefits. Despite the options open to users, only 29% of welfare claimants were successful in creating an account. Navigating the Verify system through an app or browser, entering personal information, finding the required documents, and successfully scanning the required documents, were often insurmountable obstacles; this was repeatedly seen as the most challenging step in the process of claiming welfare benefits and resulted in millions of claimants facing significant delays—thereby exacerbating inequities. Systems relying on smartphone or computer usage and remote scanning of official documents will necessarily continue to exclude groups at the margins; this is a key risk which must be avoided in the introduction of remote verification systems in government programs. The Guidelines should therefore emphasize the need to retain in-person alternatives	Add a requirement that the CSP shall provide clear alternative methods for individuals who are unable to provide the physical or digital evidence outlined throughout Section 4.3.
2.a	63A	4	6	440, 444	See above comment.	In-person identity proofing options must always be provided and must be meaningfully accessible to all. Beyond including in-person proofing as "possible mitigations" in Section 10.3, the normative information in Section 4, SP 800-63A-4 should also require that organizations always maintain meaningful in-person options for identity proofing. Specifically, at Line 440, change "SHOULD" to "SHALL," and at Line 444 add: "Organizations SHALL ensure that in-person, offline proofing channels remain available for individuals to verify their identity in a face-to-face interaction."
2.a	63A	5.5.7	31		See above comment.	In Section 5.5.7 (In-Person Proofing Requirements), SP 800-63A-4 should emphasize that the suggested "remote interaction with the applicant, supervised by an operator" should not replace the option of face-to-face interaction. An in-person interaction should always be available, and those who choose to use in-person options should not be subject to differential treatment.
2.b	63A	5.1.9.1	24	994	If the Trusted Referee system is to adequately address equity concerns, then it needs to be accessible. Many of the same equity concerns that will affect enrollment and identity proofing may lead to exclusion through the Trusted Referee system—for instance, requiring individuals seeking recourse to Trusted Referees to use a smartphone and selfie camera function and have access to reliable internet will create risks of exclusions among groups who lack internet access or who do no have a smartphone. Ensuring the availability of in-person options for Trusted Referees can help ensure that those impacted by the digital divide are still able to access services offered by the CSP. Delays in accessing Trusted Referees may also lead to significant harm, leaving individuals without access to crucial services while they wait. Reports have emerged that, in many U.S. states that had contracted with ID.me to provide identity verification services for unemployment insurance applications, applicants were left waiting days and, in some instances, weeks to have their identity verified through Trusted Referees. This caused delays to unemployment insurance applications, leaving people without crucial income. Some states moved away from using the technology after it was clear that it was slowing down the distribution of benefits to eligible residents. Trusted Referee services must therefore be accessible without undue delays.	Add: "CSPs SHALL provide the option for the use of trusted referees for remote and in-person identity proofing at IALs 1 and 2." Add a requirement that "The CSP shall ensure that trusted referees, when offered, are accessible to the public, and that there are accessible, in-person options for Trusted Referees."
2.b	63A	10.2	52	1774	See above comment.	Add: "Reliance on Trusted Referees and Applicant references must be accessible without undue delays."

2.c	63A	5.1.9.2	25		In the UK, a "vouch" system is in place whereby a declaration from someone who knows the individual can be accepted as proof of a user's identity. The UK Government Digital Service published specific guidance in 2020 on how this "vouch" can be accepted as evidence of identity, including guidance on channels through which the "vouch" can be accepted, how recent the evidence must be, who can vouch for a user, and the information that must be recorded during a "face-to-face vouch" process. Guidance of this kind provides both specific requirements ("who cannot vouch for someone's identity;" "rules for face-to-face vouches") as well as general guidance on best practices. An "Introducer" system has been used for over a decade in India to enroll in the Aadhaar digital ID system. This system was intended to allow those who were unable to complete the initial enrollment process have a certified person act as a witness and officially confirm the person's identity. It was modeled on a procedure already used by banks in India, where existing customers could introduce new customers. "Introducers" must be enrolled into Aadhaar and are persons with "high credibility" such as social workers, teachers, or postal workers, who must be vetted by India's Identification Agency. However, according to right to information request responses released in 2016, only 0.03% of Aadhaar numbers were issued through the Introducer system. The Introducer system has also been criticized for its design, as Introducers were not required to personally know the individual to whom they were providing the service. Further, concerns about the potential legal liability of Introducers made some organizations reluctant to continue playing this role within the ecosystem.	Include additional guidance about possible requirements and standards that should be in place regarding the use of applicant references, to provide more information to CSPs as they establish their written policies and procedures for the use of applicant references.
2.c	63A	5.1.9	24		See above comment.	Include successful examples of the implementation of applicant reference systems, to provide a clearer sense of how these systems should be designed and implemented. NIST should also continue to monitor examples of experimental applicant reference systems to distill lessons learned.
2.d	63A	10.1	51-52	1721-42	The current Guidelines refer to changes in attributes that result in a mismatch, but some attribute provider databases are indirectly (de facto, or unintentionally) or deliberately exclusionary based on political factors. Patterns of exclusion and discrimination can therefore lead to attribute verifier databases that are over- or under-inclusive. These patterns can also lead to a reluctance to provide personal information in certain contexts, which can exacerbate the problem of under-inclusion. Databases may be over-inclusive, such as in Kenya when the distribution of food aid was linked to a refugee database. This led individuals who were Kenyan citizens, predominantly of Somali descent, to be listed in a refugee database, and subsequently denied the right to nationality and associated benefits, leaving many at risk of statelessness. Similarly, along the U.S. Southern Border, passport denial and revocation is a frequent issue for binational families. In some cases, U.S. citizen children, born in the US, have also been registered in the Mexican civil registry in order to access services including the education system in Mexico. Later in life, these inaccuracies caused by widely known cultural patterns among border communities result in fraud-based passport denials and revocations by U.S. federal authorities, embroiling families in years of costly legal struggles and insecure legal status in the United States. In the Rio Grande Valley, many of those families who are able to afford legal challenges to passport denials ultimately correct the information and confirm their U.S. citizenship. Additionally, some databases contain high levels of errors and gaps caused by human error or technical challenges in identity resolution processes, as in India where wrong names, ages, and addresses collected during the initial data collection process for the Aadhaar card have meant that subsequent identity resolution processes in pensions, food distribution and banking have led to false allegations of fraud.	Add "Description: The identity service relies on attribute verifiers that have known exclusions and gaps in the information they hold, leading to difficulties in the identity resolution process."
2.d	63A	10.1	51-52	1721-42	In some instances, the collection of identity attributes has been shown to create opportunities to surveil, harass, and exploit marginalized groups and individuals and groups owing to their political opinions or activities, including human rights defenders. Examples include communities who have experienced over-policing and surveillance, and who may perceive a heightened risk in providing certain identity attributes such as fingerprints or in linking their digital identities to certain services. For instance, in India, the linking of the Aadhaar number with health records of those accessing HIV medication led many to discontinue such medication in fear that there would be a breach of Aadhaar data. Often, migrants may associate the collection of personal and biometric data with law enforcement, the possibility of placing themselves or their family members at risk of losing status or benefits, and facing increased surveillance and/or immigration detention and deportation. There may therefore be reluctance to engage with digital identity systems, leading to self-exclusion.	Add "Description: Individuals may self-exclude from the identity service, or from identity services offered by back-end attribute providers, which leads to an inability to validate their identity by the CSP."

2.f	63A	10.2	52	1743-74	The records against which identity evidence and core attributes are validated will generally reflect discrimination and barriers faced. For example, many systems display English language bias and are unsuited to entering longer names, non-Roman characters, or names which do not follow the American convention of First-Middle-Last name structure. A first or last name that is "too long" might be truncated in government or commercial databases; names may have been Anglicized on some identity documents and not others—these will complicate automatic name-matching exercises. Meanwhile, groups such as formerly incarcerated people may be deliberately excluded from some sources deemed to be authoritative and credible. Many of these exclusions are created by structural discrimination and patterns of exclusion that may cause errors at the initial identity resolution stage, as above at 2(d)).	Add: "Description: Records held by authoritative and credible sources may reflect existing patterns of discrimination and exclusion."
2.g	63A	10.3	53-54	1775-1817	The guidance gives several examples of bias in facial comparison algorithms and also in human bias and inconsistencies. However, there may also be significant technological and operational errors in the use of biometric technologies that can lead to inequities. Fingerprint scanning, for instance, varies in reliability based on environmental factors such as heat, moisture, and sweat. These problems are further discussed in the context of authentication and lifecycle management (below, Section 3.)	In addition to the discussion of facial image capture, add discussion of possible inequities which can arise from other biometric technologies, such as fingerprint-scanning technologies.
2.h	63A	10.4	54		As identity proofing processes can be burdensome or challenging for some groups, organizations should be encouraged to avoid creating multiple instances of identity resolution, validation, and verification. Many enrollment and identity proofing steps assume a certain level of digital and administrative skill. This can place high burdens on individuals, who need to either develop or source specialized knowledge in order to access the identity system. This is not only a usability issue, but also an equity concern as those with limited literacy or digital literacy skills, or those without access to resources and support, might experience exclusion and differential treatment as a result.	Entities should minimize the amount of administrative burden and consider factors such as minimum literacy levels required, time and resources, and duplication in submitting information.
3.a	63B	5.2.3	33	1280-81	While the requirement in SP 800-63B-4 that any biometric system used for authentication "shall operate with a false-match rate of 1 in 10000 or better" provides a good starting point regarding accuracy, this insufficiently addresses crucial equity issues. The use of a blanket rate fails to address the disparate impacts of false matches. A system might, for example, have a FMR which falls within the performance requirements but where every false match recorded was experienced by a person of color or a person with a disability. The lack of guidance on these disparate impacts in SP 800-63B-4 suggests that entities can, under these Guidelines, use biometric systems which disproportionately create exclusions for people of color. Organizations should require data on false rejection rates by demographic group, and should not implement systems which display disparities across groups.	Require the documentation and transmission of performance measures by skin type classifications and require that no biometric system with varying levels of accuracy for different demographic groups be deployed.
3.b	63B	5.2.3	32	1278	Equity requires that biometric authentication never be a mandatory precondition for accessing services, given the disproportionate challenges and disparate risks faced by certain communities in authenticating biometrically. While SP 800-63B-4 mentions the need to provide alternatives in the context of biometrics usability considerations, a requirement that biometric-based authentication only ever be optional and the consistent availability of non-biometric alternatives should be included as a normative requirement.	Add: "Biometrics SHALL be used only as part of multi-factor authentication with a physical authenticator (something you have) and SHALL only ever be provided as an optional choice of authenticator. Other, non-biometric options SHALL always be meaningfully provided." This issue of non-mandatory biometric-based authentication should be centrally addressed throughout SP 800-63B-4 rather than only mentioned in passing.
3.c	63B	10.4	73	2426	The current formulation regarding alternatives to biometric authentication is unnecessarily narrow. An alternative authentication method must be available not only as a fallback when biometrics do not work, as individuals should always have the option of not using biometric authenticators at all. An older person whose fingerprints never successfully scan should not be required to try to scan her fingerprint every time before having access to an alternative method, for example.	The usability consideration that "An alternative authentication method must be available and functioning. In cases where biometrics do not work, allow users to use a memorized secret as an alternative second factor" should be changed to: "An alternative authentication method must be functioning, readily-available, and clearly-communicated. Users should never be required to attempt biometric authentication."
3.d	63B	11	74	2452-68	Section 10.4 of SP 800-63B-4 lists the amount of moisture on a finger, age, gender, and occupation as well as injuries to fingers as "Biometrics Usability Considerations." But these should also, or even primarily, be seen as equity issues. If certain groups—older persons, people with damaged fingertips or disabilities affecting their hands, and people who work extensively with their hands in manual occupations—face more difficulties using fingerprint authenticators and experience frequent fingerprint authentication failures, this goes beyond questions of usability and risks creating indirectly discriminatory exclusions affecting specific groups, many of whom belong to protected classes under anti-discrimination laws. If the Guidelines do not discuss fingerprint scanning in the Equity Considerations section, organizations may interpret the document as encouraging fingerprint-based authentication.	Add examples relating to fingerprint-based authentication. For example, add: "older persons or people who have undertaken manual labor may not be able to use fingerprint scanning technologies."

3.e	63B	11	74	2454	The examples of authenticator suitability problems outlined in Section 11 point only to a limited set of equity considerations which focus especially on disabilities. Examples from a wider spectrum should be included to better capture the ways in which authenticator options will disproportionately create difficulties for certain populations, thereby introducing barriers and creating harms. Further contextual issues relating to immigration status, literacy and digital skills, and the day-to-day impacts of life on a low income, among others, should therefore inform the discussion of equity considerations.	At Line 2454 onwards, add: The types of devices people use influence their ability to input certain authentication methods. People on lower incomes and marginalized groups are less likely to have the latest devices and may face more difficulties using certain features, such as manually entering an OTP on a smaller onscreen keyboard. Americans with lower incomes rely more on smartphones and are less likely to have broadband internet at home: in early 2021, 27% of adults earning less than $30,000 a year were “smartphone-only” internet users who did not have broadband at home. As a result, authenticator options which require a hardware connection such as needing to be plugged into a device via a USB port, will be unavailable to lower-income groups. Low-income groups may be more likely to lack internet access or run out of data on their phones; offline alternatives must therefore always be available. The use of many authenticator types may be difficult for persons lacking in technological skills. For example, many older persons without experience using OTP devices may struggle to enter codes from one device into another. Many older persons in the United States struggle to use 2FA security tokens as they have very small form factors. A 2019 study of Americans’ digital literacy by the Pew Research Center found that only 28% of Americans understood two-factor authentication. Individuals who are experiencing trauma, addiction, or sexual exploitation will often struggle to remember details about passwords or other memorized secrets. (As above in 3d) older persons may not be able to use fingerprint scanning technologies.
3.f	63B				Just as the provision of on-site in-person identity proofing is necessary to prevent the exclusion of any individuals who are unable to or prefer not to have their identity verified remotely, offline in-person authentication is also critical in preventing the exclusion of marginalized groups. As some groups will be unable to use any digital authentication methods, agencies must maintain meaningful access to in-person authentication options, whereby individuals can have a face-to-face interaction to access a service. The failure to provide such alternatives has been a major source of exclusion in the implementation of digital identity systems in many contexts, including India, the United Kingdom, and Uganda. The approach in the Guidelines has been to equate the focus on digital identity with a focus on digital authentication, such that SP 800-63B-4 addresses only digital authentication. But as U.S. government agencies themselves note, offline in-person authentication methods form a part of digital identity systems, and should be treated as within scope of the Guidelines.	SP 800-63B-4 should address the importance of maintaining offline in-person authentication options, particularly given the equity impacts of the mandatory introduction of any digital authentication methods.
4.a	63C	Introduction	3	337 et. seq.	It is critical that the Guidelines acknowledge that federation is considered a facilitator of interoperability, and federated digital identity architectures are increasingly popular solutions to provide efficiency and convenience within enterprises and for subscribers. This reality is not captured in the Introduction to 800-63C (Lines 390–391), which only states that Federation and Assertion requirements “build on the requirements of other volumes.” The scaling of risk through federation is not adequately captured in the Introduction to the concept, leaving the Volume and the Guidelines largely silent on this feature of federated identity architecture. The Guidelines do acknowledge the “more nascent” character of federated identity generally (Line 1873) and the “lack of depth and conclusiveness of research findings” (Line 1875), with respect to usability. However, this should be highlighted in the Introduction and more appropriately centered there, to signal the caution with which these new, unfamiliar and experimental approaches to identity should be adopted and applied.	(i) Elevate and highlight the limited research available on usability, equity and privacy risks associated with federated identity. (ii) Explicitly reference the fact that any risks to usability, privacy and equity posed by a single IdP scale along with federation in digital identity, with compounding effects for subscribers across multiple services. (iii) Refer back to initial risk assessment requirements in other volumes in light of the scope and complexity and experimental nature of federated identity architectures. Specifically, recall the need for “iterative” and dynamic risk assessment (800-63-4), with entering into a federated identity scheme as a trigger for full off-cycle review (800-63A, Line 721) of risk assessment across the entire digital identity system subject to federation, not only FAL selection and other federation-specific elements of the Guidelines.

4.b	63C				While the Guidelines provide both normative requirements and informative guidance on tracking and profiling in federated systems, they fail to explain how the risks to privacy and Privacy Considerations in SP 800-63C-4 intersect with equity in unique and acute fashion in federated digital identity systems. For users of the Guidelines to fully appreciate these intersecting risks between privacy and equity, the relationship between biometric identity proofing and verification, biometric authentication, federation, interoperability and persistent surveillance using biometrics should be explicitly set out. The Guidelines, as currently structured, do not sufficiently guard against the creation of centralized biometric databases as foundational digital identity infrastructure, operating through a federated architecture. While centralization of biometric data for authentication through a central identifier is discouraged (800-63B-4, Line 1306 et seq.), federal agencies, states, territories and private entities could establish large biometric databases for digital identity verification and authentication and still be in compliance with the requirements and normative guidance in the Guidelines. Similarly, although the Guidelines acknowledge that there are significant usability considerations and open questions about user understanding and trust with respect to federated identity (800-63C, Section 10), limited information is provided on the varying incentives that different actors in a federated ecosystem, particularly financial incentives for private sector (for-profit) IdPs and colluding RPs, may have for building tracking and profiling datasets on subscriber behavior.	Draw together in one section (e.g. within Privacy Considerations, 800-63C-4 at Line 1713 et seq.) the elements of the Guidelines that allow for the establishment of large (e.g. national or state-wide), centralized biometric identification databases and include, at minimum, informative guidance concerning the privacy and equity risks that would flow from this approach. Reiterate concerns about building profiles of subscribers using transaction information, currently covered in an informative section on Privacy Considerations (Section 9), in Section 11 (Equity Considerations). Note that profiling and surveillance are not neutral or evenly experienced in any society and it is often people in low-income earning brackets, the unemployed, people of color, non-citizens, and those living in neighborhoods already subject to heightened surveillance who are most likely to be affected by tracking and profiling through federated identity and biometric identification data. The Guidelines must adequately reflect the substantial intersectional privacy and equity risks of a federated, highly interoperable digital identity ecosystem premised on a centralized biometric database. These wide scale impacts are well-documented through research and monitoring on the experimentation with this approach in the United States and other countries.
4.c	63C	5.5	30	1108	While the Privacy Requirements in Section 5.5 acknowledge the risk of IdPs and "colluding RPs" accumulating knowledge about a subscriber's conduct and movement (Line 1099), the normative requirements should be binding and not suggested, due to the absence of any suitable and legitimate purpose for engaging in tracking and profiling.	Replace MAY with SHALL in relation to requiring "clear notice, obtaining subscriber consent": "Measures SHALL include providing clear notice and obtaining subscriber consent. Measures MAY also include enabling selective use or disclosure of attributes."
4.c	63C	5.5	30	1114	See above comment.	Replace SHOULD with SHALL (regarding disassociability) in light of the equity concerns for these vulnerable groups.
4.c	63C	5.5	30	1124	See above comment.	Replace SHOULD with SHALL (regarding account termination) in light of the equity concerns for these vulnerable groups.
4.d	63C	10	61		The draft Guidelines address the role of private sector IdPs primarily in Section 10, an informative section on Usability Considerations (see, e.g., Lines 1917-29, focused on users' comfort level with social network providers as IdPs in light of concerns about their "broadcasting nature"). The ample review of existing literature on user behavior, beliefs and perceptions is welcome and provides valuable insight for RPs and IdPs contemplating or operating in federated identity systems. Yet, unfortunately, the Guidelines are silent as to the expectations, obligations, and behavior of private sector IdPs. For example, Section 10 currently differentiates between perspectives of users and implementers (see, e.g., Lines 1944–50), pointing to a "disconnect" in conceptions of identity, and focuses on measures to encourage user adoption, primarily through providing clarity on benefits and risks to users in federated systems. This is an important distinction. However, Section 10 omits any consideration of the possibility of a "disconnect" between RPs in the public sector, and particularly in high-risk sectors, and IdPs operating for-profit enterprises in the private sector. An important case in point is the UK's "Verify" system, launched in 2016 (see above at 2(a)). The UK Government Digital Service (GDS) conceived of Verify as a public sector-facilitated, private sector-led solution that would establish a marketplace for identity services, within a wider "government as a platform" framework, where government provides "supportive infrastructure" and private sector builds out the implementation of government functions through innovation. The experiment failed. When government subsidies ended in 2020, five out of seven accredited IdPs dropped out. The National Audit Office (NAO) investigated Verify, and in a 2019 report highlighted the "optimism bias" driving decisions about its uptake by the public, cost savings, and the overall commercial model. The Guidelines should also go beyond elaborating the usability considerations associated with public-private partnerships in federated identity systems, and set out the important equity considerations that flow from these same schemes due to the unique incentives and motives of private sector firms involved in identity marketplaces. Private sector partnerships in multilateral federated digital identity schemes for service delivery in other countries have resulted in disproportionate impacts for specific groups. This is an equity consideration that the Guidelines should highlight. As discussed throughout these comments, the success or failure in equitable operation of digital identity cannot be understood by implementers (public or private) as chiefly a question of technical architecture. In the case of public-private partnerships in federated identity systems, intrinsic factors in competitive marketplaces must be taken into account as drivers of access and	Differentiate between public and private sector IdPs, particularly where federated identity models encourage private sector IdPs to compete, or otherwise explicitly or implicitly rely on private sector markets to facilitate efficiency and convenience for RPs and users.
4.d	63C	11	67-68		See above comment.	Advise caution with respect to private sector involvement in public sector services as IdPs, particularly in high-risk sectors (see 1(h)), given the poor track record of such arrangements in reaching and successfully delivering essential services to vulnerable populations.
4.e	63C	5.1	14	640, 647	The disclosure provisions relating to Trust Agreements are unclear as to the transparency and accessibility of Trust Agreement terms to subscribers. In light of the extensive informative treatment of user perspectives in Usability Considerations, the Guidelines should include strict, comprehensive transparency and accessibility requirements so that the public and to users have full information about Trust Agreements between actors in a federated identity system. Disclosure requirements are especially important given the complexity of federated systems and lack of research as to their operation and effects in practice. Strengthened normative language in this section will also enhance transparency relating to public-private partnerships in federated systems, discussed immediately above.	At Line 640 (static) and 647 (dynamic): use "full parameters" or "full terms" instead of "parameters."

4.f	63C	6.2.5.2	45	1530-31		Make a privacy risk assessment required for RPs using a common identifier as a mandatory requirement: "SHALL be made available to subscribers and potential subscribers."
5.a	63-Base	5.4	39	1477	We appreciate NIST's acknowledgment that "Threat actors adapt, user expectations and needs shift, and missions evolve" and that "risk assessments and identity solutions are not to be set and forgotten." We encourage NIST to strengthen the requirement for organizations to conduct continuous evaluation and improvement to be able to re-assess.	"To maintain pace with the constantly shifting environment in which they operate, organizations SHALL implement a continuous evaluation and improvement program that leverages input from people interacting with the identity system. These programs SHALL consider feedback from application performance metrics, threat intelligence, fraud analytics, assessments of equity impacts, privacy impact analysis, and user inputs."
5.b	63-Base	5	23-24	922-64	NIST asks, at line 236 of SP 800-63-4, what equity assessment methods could be referenced to "better support organizations in preventing or detecting disparate impacts that could arise as a result of identity verification technologies or processes." A key method in preventing and detecting such impacts is to meaningfully consult with affected communities ex ante. Decision-making surrounding the design and adoption of digital identity systems must be based on the realities experienced by beneficiary populations. Beyond initial decisions about adoption and design, the methodology for assessing digital identity risks for each xAL in Section 5 of SP 800-63-4 currently provides for organizations' assessments of risk with very little mention of consultation and participation—the envisaged process appears to be top-down rather than consultative. Beyond "evaluating their user population" when conducting their initial impact assessment, organizations should consult diverse communities of users and prospective users throughout the risk management process. The lack of consultation of user populations has been specifically pointed to as a key reason for failure in the UK's Gov.Verify digital identity system (see above at 2(a)). The UK's Major Projects Authority found that the system was failing in part because "assumptions based on insight work into customer journey are not at all aligning with reality." To avoid making assumptions that lead to inequities and harms when implementing a digital identity system, federal agencies and all organizations must design with many different populations in mind and with an understanding of the kinds of technologies that certain communities are unable to use. This understanding is best acquired through inclusive consultations. As reports in the U.S. context have found, involving users throughout critical junctures would help mitigate many of the exclusions that have arisen from public sector initiatives to introduce digital systems into services. Organizations should create ample opportunities throughout the design process for user feedback from a broad range of stakeholders, including conducting their own user testing on a representative sample of their user population.	Bring reference to consultation into each of the 4 Volumes, ensuring that the individuals who will be using these digital identity systems are consistently consulted by decision-makers and providers of services. In particular, consultation with diverse user populations should be brought more centrally into each of the 4 steps of the digital identity risk management process outlined in SP 800-63-4, Section 5. This should be brought into the initial description of the model at lines 922–964.
5.b	63-Base	5	23	953	See above comment.	Add: "Throughout each of these 4 steps, organizations SHALL ensure that the views, preferences, and needs of diverse user populations are taken into account. At line 960–64, add: "Organizations SHOULD adapt and modify this overall approach to meet organizational processes, governance, and integration with enterprise risk management practices. At a minimum, organizations SHALL ensure that each step is executed, that their existing and intended user populations have been meaningfully consulted throughout each step, and the normative mandates and outcomes of each step are completed and documented regardless of operational approach and enabling tools."
5.c	63-Base	5	23	930	Impact assessments within stage 1 of the Digital Identity Risk Management process should not only assess the impact of a failure of proofing, authentication, or federation, but should rather take a more holistic approach to assessing how diverse communities are affected by these systems. Proofing or authentication might, for example, be experienced as stressful, burdensome, and may discourage certain groups from accessing services–the current orientation of impact assessment towards failure will not adequately capture these broader impacts arising from digital identity systems. Consultations within this process of identifying impact categories and potential harms should also take a broader starting point than contained in SP 800-63-4 such that, instead of asking "what would be the impact of a failure," organizations should ask, "what kinds of identity proofing methods work for some communities and not others; what kinds of authenticators are preferred or least preferred", and so forth.	Instead of referring to organizations' assessment of "the impact of a failure of each function in the identity system", the Guidelines should refer to "the impacts of each function in the identity system."
5.c	63-Base	5.1	24	967, 977, 986, etc.	See above comment.	Instead of "adverse impacts of failures in identity proofing, authentication, and federation," use language such as "adverse impacts arising from identity proofing, authentication, and federation."

5.d	63-Base	5.1.4	29	1144-58	Equity considerations relating to AALs go beyond the binary issue of whether an individual is able to access a service or not. In considering risks when determining AALs, organizations should also consider that choices about authentication also shape individuals' day-to-day experience of accessing a service. A higher AAL can impose additional burdens and frictions for an individual accessing a service, even if that individual is not excluded from the service. If an agency introduces 2FA, for example, requiring individuals to enter a username, password, and a One Time Passcode (OTP) every time they access an online service, this addition of the OTP into the process introduces an additional potential source of stress and difficulty. Some groups may experience the required OTP as a significant hurdle. An individual whose phone is shared between several members of the family for cost reasons, or a houseless person who faces barriers in keeping a phone charged, for example, may not be excluded from accessing a service, but they will experience more burdens and friction each time they access the service. The current approach to understanding and analyzing impacts on individuals under the risk management framework set out in SP 800-63-4 focuses only on whether individuals can or cannot access a service, and does not adequately address the experiences of individuals who ultimately succeed in authenticating each time, but feel intense stress or experience significant delays every time they need to access the service. The higher the AAL, the more significant this friction may be.	NIST should encourage organizations to take into account not only the possibility of certain users failing to authenticate and therefore failing to access a service, but also the burdens, frustrations, and frictions experienced by certain groups as a result of authentication requirements. For example, at line 1144–1158, NIST should not only include a normative requirement that "Entities SHOULD consider the impact of specific modes of failures [including …] the impact of failing to authenticate the correct subject due to barriers" when conducting impact analysis, but also add: "the impacts of imposing new and potentially burdensome authentication requirements on user populations." NIST should encourage organizations to take into account the impacts of authentication requirements on users' everyday lives throughout the process by which organizations assess impacts and select assurance levels.
5.e	63-Base	5.5	39		NIST should explicitly suggest to organizations that it is insufficient to measure when applications fail. Instead, evaluation programs should measure instances in which individuals have begun a verification process and then stopped, to gain some understanding of the number of attempted verifications which have not been completed and how difficult it may be for some users to complete the process. Organizations should also put in place analytics to identify the points at which individuals abandon processes, to identify key friction points.	Organizations' continuous evaluation programs SHOULD consider "application performance metrics, including measuring verification and authentication attempts and time taken…"
5.f	63-Base	5.1.2	25	1005	Organizations will be unable to properly ascertain the full range of possible impacts without conducting comprehensive consultative processes.	Add: "Organizations SHOULD include additional impact categories based on their mission and the additional impacts identified through consultations with their user population."
5.g	63-Base	5.1.3	27	1066	Organizations will only be able to gain an adequate understanding of the potential impacts (low, moderate, or high) on users through listening to users and thereby gaining an understanding of how they experience proofing, authentication, and federation.	Add: "Each assurance level … SHALL be evaluated separately and SHALL take into account consultations with user populations."
5.h	63-Base	5.3.1	37	1402-04	When assessing privacy, equity, and usability within the Digital Identity Risk Management process (Section 5.3.1), in addition to emphasizing consultations, NIST should also emphasize the need to seek input and feedback from civil society organizations, particularly those which work closely with the most marginalized and vulnerable groups of users. This, in addition to direct consultations with users, is a crucial way of gaining a better understanding of how marginalized individuals may experience a digital identity system and to ascertain potential inequities and disparate impacts.	Add: "organizations SHALL conduct detailed assessments of the controls defined at the assurance level to determine potential impacts in their operational environment. Organizations SHOULD establish mechanisms through which civil society organizations working with marginalized groups can provide input on the impacts felt or likely to be felt."
5.i	63-Base	5.3.1	37		Every consideration should be given to how to treat users as agents with knowledge and expertise that is vital to the risk assessment process. The Guidelines should encourage organizations to see users as holding specialized knowledge, as recommended in the context of EU digital policy by AI expert Lilian Edwards: "users as activists and complainants are as crucial to post-launch enforcement as regulators." Data and inputs from redress mechanisms should therefore feed into the continuous evaluation and improvement stage of the digital identity risk management framework.	
5.i	63-Base	5.4	39	1483	See above comment.	Add: "User inputs should include information collected from grievance and feedback mechanisms."
5.i	63-Base	5	23	945-52	See above comment.	Add: "Information collected about complaints and grievances should be used to feed into this continuous evaluation and improvement process. Organizations should ensure complaints and problems users experience are swiftly addressed in the continuous improvement process".
5.j	63-Base	5.1	24		Qualitative data collection through focus groups, surveys, and in-depth interviews will allow organizations to better understand how the digital identity system is impacting users. Methods should be informed by experts, and should include open-ended questions relating to users' experiences.	Add: "Organizations SHOULD collect and analyze qualitative data as well as quantitative data, conduct focus groups with diverse populations, surveys, and interviews."
5.j	63-Base	5.4	39	1483	See above comment.	Add: "Organizations' continuous evaluation of equity impacts and user inputs should draw on in-depth information collected through regular surveys and interviews to gain a holistic understanding of how the system is being experienced by users."
6.a	63-Base				While redress is currently mentioned in greatest detail in SP 800-63A-4 and SP-800-63C-4, the base document (SP 800-63-4) says very little about redress and does not comprehensively set out requirements. As individuals' ability to file grievances and seek redress should be seen as a central part of a digital identity risk management process, SP 800-63-4 should clearly address this issue.	Add a section on redress, including normative requirements and informative information.

6.a	63B				See above comment.	Requirements surrounding redress for authentication failures should also be brought into SP 800-63B-4.
6.b	63-Base	2.3.3	9	586	Throughout the Guidelines, sections on equity considerations rarely include a reference to redress. But redress mechanisms are crucial in achieving equity—not only because the reporting of inequities allows organizations to improve their processes and fix problems, but also because they provide an avenue to remedy errors and exclusions which disproportionately fall on marginalized groups. While SP 800-63A-4 helpfully requires CSPs to provide redress options to individuals affected by biometric technologies with differing performance across demographic groups, this requirement is not mentioned again within sections concerning equity. As these risks disproportionately affect some groups, redress is a key equity issue and should also come under equity considerations.	Include discussion of redress within sections on equity considerations in each document. Here, add: "Organizations should also ensure that appropriate and adequate avenues for redress are provided, and that these are meaningfully accessible to the most vulnerable user populations."
6.b	63A	10.3	53	1783-91	See above comment.	Reiterate the requirement to provide redress. Add: "In instances where image capture technologies have failed to capture certain skin tones or facial features, CSPs SHALL act expeditiously to provide redress."
6.c	63A	5.1.2	17	789	Where identity proofing processes create delays, people are left waiting to access services. As outlined above (at 2(b)), some unemployment insurance applicants in states which had contracted with ID.me for identity proofing services were left waiting weeks to have their identity verified by "trusted referees" when facial scanning failed, which caused delays to their unemployment insurance applications and left them without crucial income to which they were entitled. Individuals affected by delays and the consequences of these delays must be able to file grievances and claim redress for the impacts they experience. Redress for such delays is especially important from an equity perspective, given that people of color, people with disabilities, and those living in poverty, among others, are more likely to be affected.	Add: "The CSP SHALL provide mechanisms for redress for applicant complaints and for problems arising from identity proofing, including but not limited to: proofing failures, delays, and difficulties."
6.c	63A	8.4	42	1417-25	See above comment.	Add a reference to the need to provide redress for delays in identity proofing processes.
6.d	63C	10.1	62	1923	Clearly communicating information about redress entails understanding user populations and tailoring communication accordingly, such as for people without consistent access to the internet, lower digital literacy, or without English language skills. Ineffective communication about helplines and mechanisms for assistance which fails to reach more vulnerable populations will affect communities' ability to seek help, further exacerbating inequities.	Add: "Clearly communicate how and where to acquire technical assistance and redress. Ensure information about technical assistance and redress is available in multiple languages, stated in plain language, provided in-person at government offices, and clearly communicated to community organizations working with vulnerable populations."
6.e	63C	10.1	62	1928	Providing meaningful assistance and redress for people who are less able to navigate digital systems requires the maintenance of phone-based and in-person channels. Help desks should be well-staffed to avoid long delays.	Add: "Provide assistance and grievance mechanisms in multiple languages, via an online system and phone number for help desk support. Maintain in-person channels through which individuals can seek assistance and file complaints."
6.f	63A	8.4	41-42	1407-25	Currently, the Guidelines place much responsibility on CSPs to communicate with users about assistance and redress. Responsibility should also be placed on the agencies providing government services to provide clear information about redress, because users accessing services will be most familiar with the agency and this will be their port of call. Individuals who are struggling to use a digital identity system to access a government service should be able to access clear information about redress from the agency, and not immediately sent to the CSP to find information.	Add: "Agencies should also provide clearly-accessible and clearly-communicated information about how users can access assistance and redress when problems arise from identity proofing."
6.f	63B				See above comment.	Add a requirement that both agencies and CSPs provide coherent, clear information on how to access assistance in the case of problems with authentication.
6.f	63C				See above comment.	Add a requirement that, to avoid redirecting users back and forth among RPs, IdPs, and brokers to receive technical assistance, the RP should have a responsibility to provide clear information about avenues for assistance when problems arise.
6.g	63-Base				If staff are not provided with a clear understanding of redress mechanisms and alternatives, this raises the risk that "officers will be unequipped to respond [to failures in the digital identity system] without denying citizens constitutionally protected rights and services." In Kenya, for example, though social security recipients can use alternatives to fingerprint scans to authenticate their identity at government offices, less than 10% of beneficiaries have been offered alternatives, leading to exclusions. To avoid such situations, agencies should provide staff with training and clear processes about alternatives and avenues for assistance. If a user applying for unemployment benefits from their state is struggling to verify or authenticate their identity and goes to the state unemployment office for help, there should be a process and dedicated staff members in place who can help applicants. Agencies should also provide staff with opportunities to share major barriers that users face and commonly expressed grievances, as well as a mechanism to feed these concerns into continuous evaluation and improvement of the digital identity system.	Across the documents, emphasize that staff in organizations providing services should have an understanding of the avenues for redress, the alternatives available, and the complaints procedures, within the digital identity system. Public officials and agency staff should receive training and have access to clear information about how users struggling with the digital identity system can gain access to services.
6.g	63A				See above comment.	See above suggestion.
6.g	63B				See above comment.	See above suggestion.
6.g	63C				See above comment.	See above suggestion.

6.h	63C	11	68	2115-17	There may be a risk of fragmentation in avenues for redress across a digital identity system, as the Guidelines include some requirements for CSPs to provide redress in relation to identity proofing (in 63A-4), some requirements on IdPs to redress problems such as inaccurate attribute value (in 63C-4), and separately provide for mechanisms for subscribers to report inequitable authentication requirements (in 63C-4). Requiring each CSP to create its own redress mechanism without clearly setting minimum standards could also lead to increased complexity for users. Clarifying and expanding the requirements placed on organizations providing services (state and federal agencies) would mitigate this risk. Agencies could, for example, have a holistic complaint mechanism through which users can file complaints about any stage of the digital identity system, including its overall design. This would be easier for users, and would also enable organizations to obtain information about problems with their implemented digital identity system.	Elaborate further on the requirement that RPs "provide mechanisms for subscribers to report inequitable authentication requirements and to advise them on potential alternative authentication strategies." Beyond this, NIST could require agencies to maintain an accessible avenue for users to file complaints about problems arising from the digital identity system.
6.i	63A	5.1.2.2	19	791	The Guidelines appear to envisage only CSPs' self-assessment of redress mechanisms—such as by requiring CSPs to "assess the mechanisms for their efficacy in achieving resolution of complaints or problems" in SP 800-63A-4 at Line 791—but do not provide for any centralized oversight of how redress mechanisms are functioning. Centralized oversight of redress mechanisms, rather than self-assessment, is necessary to ensure that they are functioning and adequate, as well as to ensure continual improvement in the digital identity system. The UK's Digital identity and attributes trust framework, though still in progress, could provide inspiration. It requires identity providers to have a process in place to deal with incidents, including fraud, data breach, and "service delivery, for example if users cannot use your product or service because it's temporarily unavailable". Providers "must have a process for managing and responding to service delivery incidents" which must follow industry good practice service management processes and the process should cover how the provider will "log, categorise, prioritise and assign incidents" as well as "resolve and close incidents". It establishes a governing body, which will ensure that organizations within the trust framework follow the applicable rules, ascertain where organizations have broken the rules, and will be involved in ensuring redress.	NIST should encourage external (and preferably harmonized or centralized) assessment of the redress mechanisms within digital identity systems.
6.j					Independent review of complaints will allow for the identification of varying standards of accessibility in digital identity systems, common points of failure and friction, and varying adequacy in rectifying problems. For the UK's Digital identity and attributes trust framework, the proposed oversight body will investigate and handle complaints concerning digital identity and will oversee identity providers and relying parties. Identity service providers must have a process in place for dealing with complaints and disputes, but the governing body will likely be responsible for deciding how users' complaints must be handled. Providers "might be asked to provide specific information as part of an investigation into an incident" by the governing body. Identity service providers are also required to submit an exclusion report to the governing body every year, which must include which demographics have been excluded (or are likely to be excluded) from using the service or product, why the exclusion happened (or could happen), and what the identity service provider will do to improve inclusion of its product or service. In the European Union, the EU Parliament has proposed the establishment of a European Digital Identity Framework Board, which will play an oversight role, as well as a complaint mechanism with a supervisory body.	A separate, independent body should be established which reviews the complaints submitted and the redress provided in relation to digital identity systems.