CENTER FOR HUMAN RIGHTS & GLOBAL JUSTICE
NYU SCHOOL OF LAW

NYU LAW

Temple University
Beasley School of Law

Institute for Law, Innovation and Technology

SHAPING DIGITAL IDENTITY STANDARDS

AN EXPLAINER AND RECOMMENDATIONS ON TECHNICAL STANDARD-SETTING FOR DIGITAL IDENTITY SYSTEMS

JUNE 2023

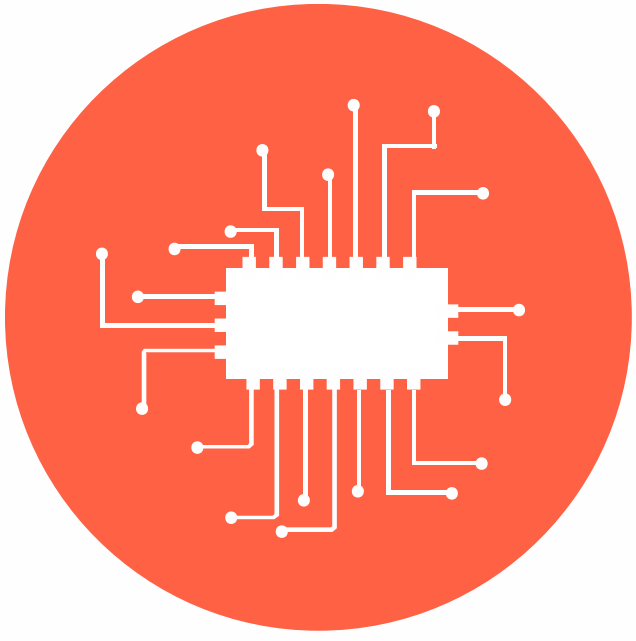


TABLE OF CONTENTS

THE IMPORTANCE OF STANDARDS ORGANIZATIONS FOR THOSE WORKING ON DIGITAL IDENTITY

There are now many civil society organizations, grassroots groups and frontline practitioners who work on issues relating to digital identity systems, or provide advice and assistance directly to users of digital identity systems. Many of these practitioners may not have previously engaged with technical standards or the standards organizations who create them. But technical standards are fundamentally shaping the digital systems that these practitioners confront in their work. Some basic background on what standards are—and why they matter for safeguarding rights—will help actors in the field who are not technical experts to engage with standards in the context of their own work.

Scientific and technical standards promote standardization: repeat technical tasks or measurements being performed in the same way in different organizations, geographies or sectors (such as healthcare, education, or human resources). A wide range of organizations create and develop technical standards; they are composed of technical experts, and many are industry-led. Standards bodies exist at national, regional and international levels. They may be generalized, developing standards for a wide range of technologies impacting public life, like the International Standards Organization (ISO), or specialized, such as a national telecommunications standards body. Trade and competition in international markets are major drivers for governments and private standards organizations to adopt and disseminate technical standards.

In the context of digital technologies, technical standard setting bodies warrant critical attention. These standards bodies are key sites at which vital decisions are made to shape the development of technologies and digital infrastructures. Especially in contexts where regulation of digital technologies is lacking, standards bodies often play a crucial role in determining what technological systems can or cannot do, and more importantly what they should and should not do, effectively setting the rules governing digital technologies.[1] Technical standards guide the design and performance levels of biometric technologies, for example, and standards bodies are promulgating standards concerning the reliability and safety of artificial intelligence systems.

It is therefore important to understand the mission, structure, and priorities of different bodies responsible for creating technical standards. Furthermore, the work of standards bodies based in the United States and Europe has relevance well beyond these geographies, given the significant role that they play in exporting many digital technologies.

1 See Carolina Caeiro, Kate Jones and Emily Taylor, 'Technical Standards and Human Rights: The case of New IP' in Christopher Sabatini (ed.), Reclaiming Human Rights in a Changing World Order (Chatham House, 2022); CDT response to the Office of the High Commissioner for Human Rights call for inputs on the relationship between human rights and technical standard-setting processes for new and emerging digital technologies, March 2023

THE ROLE OF THE NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST) IN SHAPING DIGITAL IDENTITY SYSTEMS

This explainer and recommendations emerged during a public participation and comment period for a particular set of standards on digital identity produced by a prominent standards body, the National Institute of Standards and Technology (NIST), which is part of the U.S. Department of Commerce. NIST sees itself as a world leader in promoting equitable standards. It is currently in the process of updating its Guidelines on Digital Identity (Guidelines), which "present the process and technical requirements for meeting digital identity management assurance levels ... including requirements for security and privacy as well as considerations for fostering equity and the usability of digital identity solutions and technology."[2] The primary audiences for the Guidelines are IT professionals and senior administrators in U.S. federal agencies that utilize, maintain, or develop digital identity technologies to advance their mission. The Guidelines fall under a wider NIST initiative to design a Roadmap on Identity Access and Management that explores topics like accelerating adoption of mobile drivers licenses, expanding biometric measurement programs, promoting interoperability, and modernizing identity management for U.S. federal government employees and contractors.

This technical guidance is particularly influential, as it shapes decision-making surrounding the design and architecture of digital identity systems. Biometrics and identity and security companies frequently cite their compliance with NIST standards to promote their technology and to convince governments to purchase their hardware and software products to build digital identity systems. Other technical standards bodies look to NIST and cite NIST standards. For many digital identity users (individuals) and civil society groups working on digital identity in the United States and other countries, the use of standards to promote technology that has been associated with discrimination, denial of services, violations of privacy and data protection, surveillance and other human rights violations presents a real challenge to the public interest.

The NIST Guidelines set out a framework for enterprises, targeted at government agencies but also applicable to private companies, to work through how digital identity technology can contribute to the delivery of their missions. For civil society organizations familiar with concepts of data protection impact assessments, privacy impact assessments, or human rights impact assessments, the Guidelines follow a similar basic approach in that they provide guidance on how to identify and evaluate risks. The infographic below (Figure 1) shows a high-level overview of the Guidelines, which are divided into four volumes: a main volume that walks through risk assessment considerations, and three volumes with specific guidance on three core elements of digital identity systems: identity enrollment and proofing (including collecting, validating and verifying documentation of identity), identity authentication (confirming identity of an enrolled individual), and federation (networking digital identity functions across different organizations). Throughout the documents, normative requirements are set out, noting what organizations "shall" or "should" do in creating and rolling out digital identity systems.

2 See National Institute of Standards and Technology, Digital Identity Guidelines (Draft), SP 800-63-4, published December 16, 2022, available at: https://csrc.nist.gov/publications/detail/sp/800-63/4/draft

FROM PRACTICE TO STANDARDS: OUR RECOMMENDATIONS

During its public consultation on the Guidelines, NIST specifically requested public comments on how to improve its guidance on advancing and safeguarding equity in digital identity systems. This is a welcome development, as it is clear from the latest draft of the Guidelines that there is significant room for improvement in the normative and informative guidance around equity. Such improvement will likely only be possible through greater engagement with affected communities, civil society organizations and legal experts outside of the usual technical standards community, as well as integration of the NIST Guidelines with other legislative and policy efforts that are currently underway to safeguard rights in the context of digital identity and the digitalization of public services.

The recommendations outlined below, which summarize more extensive comments delivered to NIST as part of this public consultation, therefore center issues surrounding equity.[3] These recommendations are grounded in research and documentation of lived experiences arising from the roll-out of digital identity systems around the world. If adopted, they would bring the influential technical guidance and decision-making about the technical architecture of digital identity systems as promulgated by NIST closer to the practical realities of systems on the ground.

3 The full comments can be accessed at: https://chrgj.org/wp-content/uploads/2023/05/Digital-Welfare-State-Project-NYU-Law iLIT-Temple-University_NIST-Digital-Identity-Guidelines-Comments.pdf

HOW TO USE THIS PRIMER

To aid in understanding recommendations on how to make digital identity systems more equitable through improvements to NIST's standards, this explainer begins with some tools to help civil society organizations, practitioners, and users to understand the Guidelines and the role of technical standards bodies more generally. This includes providing an overview of the NIST Guidelines (Figure 1) and defining key terms by providing the definition that appears in the Guidelines alongside a plain language description.

We then provide an overview of the risk management framework (Figure 2), and give a brief summary of some of our main recommendations to strengthen the safeguarding of equity within this framework. While these recommendations arose in the context of the public consultation on the Guidelines and are oriented towards NIST specifically, we believe that they are widely applicable to standards setting efforts in many other contexts and may provide a helpful resource to others in engaging with standards in the context of their work.

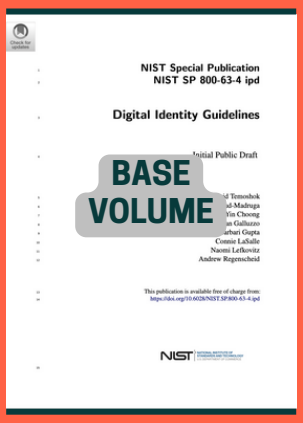
Furthermore, these recommendations all point to a wider need to continue gathering information on how and why digital identity systems lead to unequal and discriminatory treatment for specific communities. Practitioners who work with users of digital identity systems are best-placed to proactively document this information so that standards can better guide how public sector service providers think about digital identity in relation to their role and mission in society. More research and analysis is also needed to understand, inform, and form recommendations on the role of standards bodies and standards in relation to the advice, assistance, and advocacy that practitioners do in their work to promote the rights of people in relation to their governments, as identity and public administration ecosystems become more integrated with digital technologies.

DECODING THE DIGITAL IDENTITY GUIDELINES

What's in the NIST Digital Identity Guidelines?

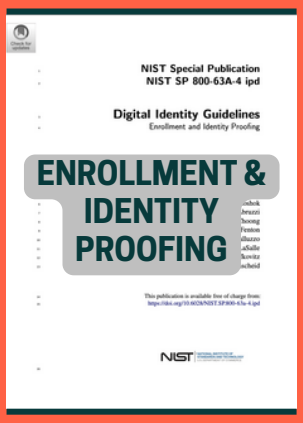
Figure 1: An overview of the four volumes of the NIST Digital Identity Guidelines

NIST SP 800-63-4
initial public draft



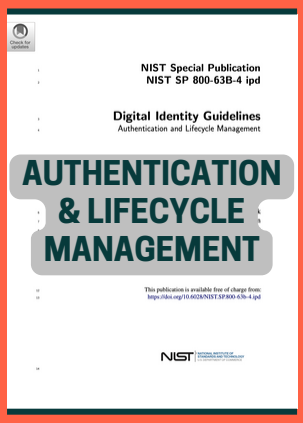
Gives overview of identity frameworks, including the use of **credentials** and the **assurance level selection** process for identification, authentication, and federation. Describes the overall risk assessment and management framework recommended in the Guidelines.

NIST SP 800-63A-4
initial public draft



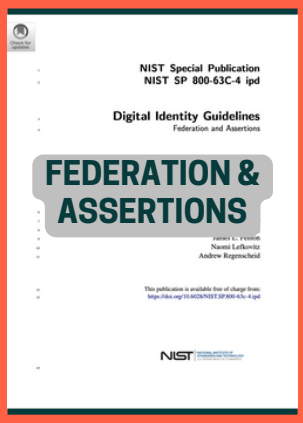
Gives requirements for **enrollment** and **identity proofing**, and each of the three **assurance levels**. Provides normative and informative guidance on risks, including risks to privacy, equity, and usability.

NIST SP 800-63B-4
initial public draft



Gives recommendations for types of authentication processes and choice of **authenticators**, including **biometrics**, for three identity assurance levels. Provides normative and informative guidance on risks, including risks to privacy, equity, and usability.

NIST SP 800-63C-4
initial public draft



Gives requirements for the use of **federated identity** architectures. Gives recommendations for privacy-enhancing techniques. Provides normative and informative guidance on risks, including risks to privacy, equity, and usability.

A PLAIN LANGUAGE GUIDE TO KEY TERMS AND CONCEPTS

TERM	NIST DEFINITION [FROM DIGITAL IDENTITY GUIDELINES]	PLAIN LANGUAGE EXPLANATION
Enrollment	The process through which an applicant applies to become a subscriber of a Credential Service Provider (CSP) and the CSP validates the applicant's identity.	This is the first stage, when Maria registers into the digital identity system. Maria will need to provide information about herself, like her name, date of birth, and so on, and the organization will check her information and create an identity record or account for her within its system.
Identity Proofing	The process by which a CSP collects, validates, and verifies information about a person.	The organization will check whether the information Maria has provided is true. It will collect information or documents from Maria, for example her driver's license, and will verify that the license is not fake by comparing the information to a reliable and authoritative source, in this case the relevant motor vehicle authority's database of license holders. The organization will then check whether the information on the driver's license Maria has presented matches Maria the real-life user, to make sure she is not claiming someone else's identity. This might, for example, involve comparing Maria's face to the photo on the driver's license.

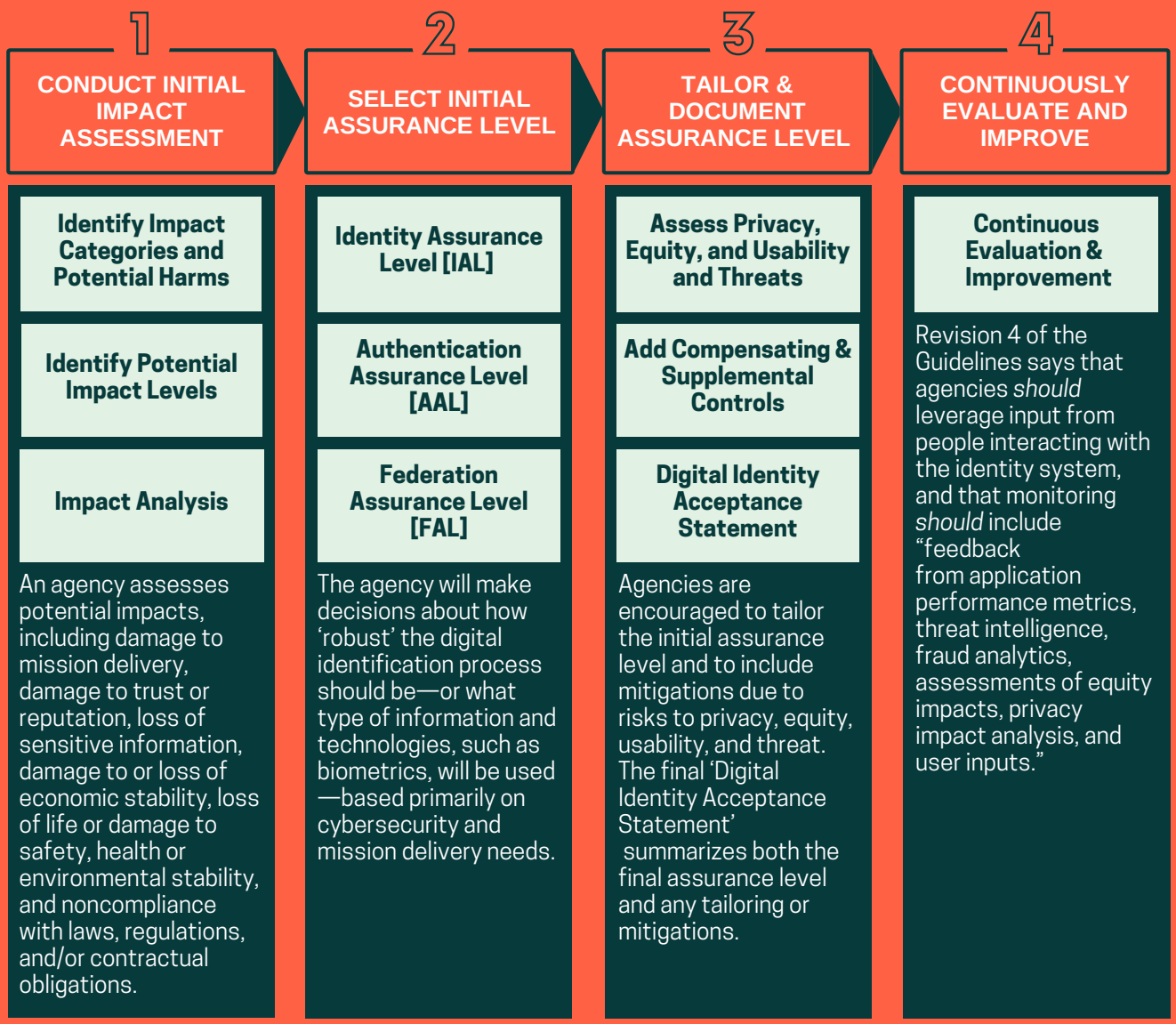
TERM	NIST DEFINITION [FROM DIGITAL IDENTITY GUIDELINES]	PLAIN LANGUAGE EXPLANATION
Authentication	The process of determining the validity of one or more authenticators used to claim a digital identity. Authentication establishes that a subject attempting to access a digital service is in control of the technologies used to authenticate.	This step can happen during many stages of the identity lifecycle. This process answers the question, "are you, the individual seeking to access a service or an account, the same person who has been enrolled and verified?" Maria will need to show some evidence that she is who she is claiming to be. Generally, she will need to show that she is in possession of the credential that has been linked to her identity record, which might be a password, a PIN, a scan of her fingerprint, or a code sent to her mobile phone, for example (see 'credential' below). But she will not necessarily need to show all of the evidence that she presented when she first enrolled – for example, she might have needed to show her driver's license and choose a username and a PIN when she first enrolled, but once she is enrolled, to authenticate each time she accesses the service she only needs to enter the username and PIN. When Maria enters the correct PIN that she had previously chosen when she enrolled, the authentication process will establish that, given that Maria has entered the right PIN, she is indeed the same person who was enrolled. She is thus allowed to access the service.
Credential	An object or data structure that authoritatively binds an identity - via an identifier or identifiers - and (optionally) additional attributes, to at least one authenticator possessed and controlled by a subscriber. A credential is issued, stored, and maintained by the CSP. Copies of information from the credential can be possessed by the subscriber, typically in the form of one or more digital certificates that are often contained, along with their associated private keys, in an authenticator.	This is the 'thing' that is used to vouch that Maria is who she says she is. This might be "something she has" (such as an ID card or passport), or "something she knows" (such as a password or a PIN), or it might be "something she is" (such as a scan of her fingerprint). This 'thing' will be linked to Maria's record in the system, so that when Maria presents it in the future, the organization will trust that she is who she says she is. For example, when Maria scans her fingerprint when she first registers, this will be linked to her record and becomes the 'thing' that vouches for her identity.

TERM	NIST DEFINITION [FROM DIGITAL IDENTITY GUIDELINES]	PLAIN LANGUAGE EXPLANATION
Federation	A process that allows the conveyance of identity and authentication information across a set of networked systems.	Federation refers to one of the ways that digital identity systems can be designed. Federation creates an infrastructure that links separate digital identity systems so that information stored on different systems can be shared and accessed by different organizations. Hypothetically, Maria might go through a digital identity verification process for her online banking, while her daughter Rachel might have verified her identity through the Post Office. A federated system for a government service might allow Maria to gain access to the service via her bank and Rachel to gain access via the Post Office, for example. This way, Maria can use her online banking digital identity to access banking as well as government services. Not all systems are federated.
Identity Assurance Level	A category that conveys the degree of confidence that the applicant's claimed identity is their real identity.	This is the level to which the organization can be confident that Maria's claimed identity is her 'true' identity. A government portal which contains sensitive information and delivers critical services, for example, might set a high identity assurance level because it is especially important that people do not gain access using false identities. Setting a high identity assurance level means that the organization needs to be extremely confident that Maria is indeed Maria, and may demand more evidence from Maria to prove this before she is granted access.

TERM	NIST DEFINITION [FROM DIGITAL IDENTITY GUIDELINES]	PLAIN LANGUAGE EXPLANATION
Authentication Assurance Level	A category describing the strength of the authentication process.	The authentication assurance level determines what Maria will need to do each time she accesses the service. If there is a high authentication assurance level, she might need to provide multiple credentials—such as entering a password and receiving a one-time passcode on her phone and scanning her fingerprint—or provide stronger credentials, like longer and more complicated passwords, that are more difficult to fake.
Federation Assurance Level	A category describing the assertion protocol used by the federation to communicate authentication and attribute information (if applicable) to a Relying Party (RP).	Within a federated digital identity system, the federation assurance level describes the level of trust between the service or portal Maria is trying to gain access to, and the digital identity service that Maria is using. So, if Maria is trying to access a government service using her online banking ID, the federation assurance level will determine what the bank needs to communicate to the government portal to assure the government portal that Maria is who she says she is.
Biometrics	Automated recognition of individuals based on their biological and behavioral characteristics.	Biometric information includes biological attributes like a fingerprint, face, or iris, or behavioral characteristics like handwriting or keystrokes. Biological attributes are often scanned or photographed, and then translated into code. If Maria enrolls into a digital identity system that requires biometric information, she might need to have her fingerprint scanned, for example. If biometric authentication is required, she will need to scan her fingerprint each time she wants to access the service, and her fingerprint scan will be automatically compared against the fingerprint data on file within the system.

WHAT IS THE RISK MANAGEMENT APPROACH RECOMMENDED BY THE GUIDELINES?

Figure 2: The Approach to Risk Management Recommended by the NIST Digital Identity Guidelines



RECOMMENDATIONS TO NIST

01 — Technical precision should not be limited to technological terms: Provide robust definitions for key human rights terms and standards

NIST has described the renewed emphasis on privacy, equity, and usability as an effort to place "the risks faced by individuals accessing services alongside risks to the organizations that operate those services." However, while the Guidelines provide precise definitions of many technical terms, some key concepts at the heart of human rights protection are described in vague terms that are disconnected from enforceable legal frameworks and widely accepted human rights norms.

Offering examples and general guidance is helpful, but without precise definitions, many decisions about acceptable risk thresholds will be left to the imagination of implementing agencies. This not only risks fragmentation, it risks significantly weakening rights protections based on agency discretion.

Key terms within the Guidelines should be more clearly defined, in alignment with a rights-based approach to digital identity systems, for instance:

- Equity: The Guidelines refer to a definition of equity from Executive Order 13985 which designates certain underserved communities, and calls for the "consistent, fair, just and impartial treatment of all individuals." This definition has some notable gaps. For instance, it does not include non-citizens, including asylum seekers and refugees, who already face significant barriers accessing government services. Second, it focuses mainly on equity in treatment and not equity in outcome. Given the importance of equity as one of only four risk categories within the Guidelines, and the stand-in for a wide range of civil, political, economic and social rights, a more robust definition, created through consultation, would strengthen the Guidelines.
- User population: The success of any risk assessment process relies on properly identifying potential impacts on the 'overall user population.' However, the Guidelines do not give sufficient guidance on how to identify specific groups who may be especially vulnerable to digital identity related risks, including, for instance, non-citizens and family members of individuals enrolled in the identity system.
- Risk of 'failure': Both the impact assessment and the tailoring process within the Guidelines' risk assessment and management framework emphasize the importance of assessing 'failures' in the digital identity enrollment, proofing, and authentication processes. Often this references technical or operational failures, such as a failure to match biometrics. If the goal of a system, however, is to provide an inclusive, equitable and accessible pathway to public services, then a failure could include burdensome requirements, long delays, and differential treatment.

02 — One size does not fit all: Identify high-risk sectors and tailor risk management recommendations accordingly

Key public services that are essential to the enjoyment of fundamental human rights require a tailored approach in the risk management framework: The Guidelines are designed primarily for federal agencies, many of which are delivering essential social welfare programs covering food and nutrition, health, cash assistance and unemployment insurance. These essential public benefits and entitlements, which are intimately linked to the ability of individuals to enjoy human rights, should not be considered fungible with other forms of government service delivery. High-risk sectors should therefore be identified, and recommendations should be tailored accordingly.

For 'high-risk' sectors, there should be a lower tolerance for risk and more stringent requirements for implementing agencies: The risks of using digital identity systems in certain sectors can lead to a greater risk of injury to health, safety, security, or economic well-being of individuals. This includes not only sectors where timely access is required for the enjoyment of human life, but also sectors where sensitive personal information that is capable of building tracking profiles or leading to other harms is being collected. There may be a need to deviate from the more rigid, cybersecurity focused assurance level selection process to adjust for these risks.

Where a digital identity system is introduced in a high-risk sector, there is a heightened need for continuous monitoring, consultation, and accessible remedies to mitigate sector-specific risks. This should include assessments of sector-specific risks in consultation with those who have sufficient knowledge and qualifications to understand the specific context at hand, such as frontline and grassroots organizations and practitioners. This should also include regular feedback from users on an ongoing basis.

03 — Broaden the scope of mandatory consultation with user communities

Adopt a genuinely user-centered approach: Decision-making surrounding the design and adoption of digital identity systems must be based on the realities experienced by beneficiary populations. 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.4 Yet the Guidelines contain very little discussion of consultation with user communities, and seem to envisage top-down rather than consultative processes for assessing the risks that could arise within digital identity systems. Throughout all stages of designing and implementing a digital identity system, organizations should meaningfully consult all affected groups of users. Design must be genuinely user-centered, taking into account the needs, preferences, and opinions of the individuals who will be using these systems. Consultation should feed into each assurance level separately and independently, leaving open the possibilities of identifying new categories of potential harms through user input.

Organizations should test that the digital identity system works for diverse groups—particularly including marginalized communities—before implementation: In the United Kingdom, a digital identity system deployed within the welfare sector led to significant exclusions among marginalized groups because, in the words of the government projects watchdog, "assumptions based on insight work into customer journey are not at all aligning with reality."5 To avoid making assumptions that lead to inequities and harms when implementing a digital identity system, organizations must approach design based on an understanding of the kinds of technologies that certain communities are unable to use. This understanding is best acquired through inclusive, comprehensive, consultative processes, including user testing. Organizations should therefore consistently test their systems with user communities before deployment, and should create frequent opportunities for users to provide feedback throughout the design process.

4 Julia Simon-Mishel, Maurice Emsellem, Michele Evermore, Ellen Leclere, Andrew Stettner, and Martha Coven, Centering Workers —How to Modernize Unemployment Insurance Technology (Philadelphia Legal Assistance, The Century Foundation, National Employment Law Project, 2020)

5 House of Commons Work and Pensions Committee, Universal Credit Project Assessment Reviews, Fifth Report of Session 2017-19 (8 February 2018), available at https://publications.parliament.uk/pa/cm201719/cmselect/cmworpen/740/740.pdf

04 — Require more safeguards for biometric technologies

The Guidelines should not be permissive of population-wide biometric ID programs: Though the centralization of biometric data through a central identifier is discouraged, large biometric databases for digital identity purposes could be established and remain in compliance with the Guidelines' requirements. The Guidelines therefore do not sufficiently guard against the creation of centralized biometric databases as foundational digital identity infrastructure.

Strict requirements should be set for the performance levels of biometric technologies: It is well-known that biometric technologies have often demonstrated a higher level of accuracy for some demographic groups over others. Facial image capture technologies, in particular, have been shown to be less reliable for darker skin tones. Though the Guidelines require that any biometric system used for authentication "operate with a false-match rate of 1 in 10000 or better," thereby mandating a certain level of accuracy, this does not address inequalities in the distribution of false matches. Strict, mandatory performance requirements should be established: vendors of biometric technologies should be required to share data on false rejection rates by skin type and gender, and systems should not be deployed unless they are proven to have equally high performance levels across demographic groups.

The use of biometric technologies should never be mandatory: Given their uneven inaccuracies and failures, biometric authentication must never be a mandatory precondition for accessing services. Though the Guidelines mention the need to provide alternative authentication methods wherever biometrics fail, this is insufficient: biometric-based authentication must only ever be optional, and non-biometric alternatives must be consistently and unconditionally available.

Discussion of the risks arising from biometric technologies should not be confined to facial image capture technologies: The Guidelines give several examples of bias in facial comparison algorithms, but significant risks of exclusion can also arise from other biometric technologies. Older persons, people with disabilities affecting their hands, and people whose fingerprints are damaged due to manual labor, for example, face more difficulties using fingerprint authenticators—and reliability also varies based on environmental factors such as heat, moisture, and sweat. If the Guidelines do not discuss these equity-related risks, organizations may interpret them as encouraging fingerprint-based authentication.

05 — Require in-person options for essential steps in identification

In-person options for identity proofing must always remain open, and must be meaningfully accessible: To avoid excluding people who are unable to use digital remote options from the digital identity system, organizations must maintain in-person options for enrollment and proofing processes. Systems relying on smartphone or computer usage and remote scanning of official documents will continue to exclude groups at the margins; this is a key risk which must be avoided in the introduction of remote proofing systems. Organizations should also ensure that those using in-person or physical alternatives are not subject to differential treatment.

Provide accessible in-person channels for authentication: To prevent the exclusion of any individuals who are unable to use digital authentication methods, or who prefer to interact with officials in person when proving their identity for a specific transaction, offline in-person authentication is critical.6 Organizations must therefore 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 authentication alternatives has been a major source of exclusion in the implementation of digital identity systems in many contexts, including India and the United Kingdom. 7

In high-risk sectors especially, the maintenance of in-person options should be mandatory: In sectors such as social security, immigration, health, or education, it is particularly crucial to allow users to enroll and authenticate via in-person, face-to-face channels in brick and mortar offices.

6 See Office of Inspector General, United States Postal Service, RISC Report, The Role of the Postal Service in Identity Verification, May 11, 2022, available at https://www.uspsoig.gov/sites/default/files/reports/2023-01/RISC-WP-22-006.pdf

7 See Reetika Khera (ed.), Dissent on Aadhaar: Big Data Meets Big Brother (Orient Black Swan, 2018); UK House of Commons, Work and Pensions Committee, Universal Credit Project Assessment Reviews, Fifth Report of Session 2017-19 (8 February 2018), available at https://publications.parliament.uk/pa/cm201719/cmselect/cmworpen/740/740.pdf

06 —Poorly designed or under-resourced mitigations can backfire

Offer more guidance on key mitigations and alternatives: The use of Trusteed Referees and Applicant References are two of the only mitigations offered in the Guidelines as an effective means of addressing some of the equity risks, as they provide alternative pathways for in-person or 'human-in-the-loop' identity proofing options, such as a video call. But, to act as a true mitigation for equity-related risks, such systems need to be physically, technically and financially accessible—as well as timely. Specific provisions and guidance should be offered to ensure that these elements are in place. For instance, the United Kingdom Government Digital Service has published detailed guidance on the use of the 'vouch system.'[8]

Trusted Referees and Applicant References should be meaningfully accessible, without delay: Delays in access to Trusted Referees or Applicant References, and thus to public services dependent on the digital identity system, can be a significant source of harm. This was recently experienced by unemployment insurance applicants in the United States who attempted to verify their identity through a virtual Trusted Referee system but were in some cases left waiting weeks to access a Trusted Referee. This led to delays in their receipt of benefits.[9]

Invest in research on these, and alternative forms of mitigations. While such alternatives may be well intended, they may not always function well, have sufficient resources, or be easily accessible for different vulnerable groups. In India, evidence demonstrated that the 'introducer' system implemented to facilitate enrollment into the 'Aadhaar' digital identity system was barely used, and many potential 'introducers' were wary of taking part due to fears about liability.[10] There is much we do not know about what works—and what does not—so further research is needed.

8 UK Government Digital Service, Guidance: How to accept a vouch as evidence of someone's identity, October 22, 2020, available at https://www.gov.uk/government/publications/how-to-accept-a-vouch-as-evidence-of-someones-identity/how-to-accept-a-vouch-as-evidence-of-someones-identity.

9 EPIC, et al., "A Call To Federal and State Agencies To End the Use of ID.me and Other Facial Recognition Identity Verification Services," February 14, 2022, available at https://epic.org/wp-content/uploads/2022/02/Coalition-Letter-ID.me-and-Face-Verification-Feb2022.pdf

10 Ranjit Singh & Steven Jackson, Seeing Like an Infrastructure: Low-resolution Citizens and the Aadhaar Identification Project, Proceedings of the ACM on Human-Computer Interaction 5, no. CSCW2 (October 18, 2021): 315:1-315:26. https://doi.org/10.1145/3476056.

07 —Dirty data: Assume data inaccuracies, don't punish users for them

Take note of known or potential errors and patterns of data inaccuracy within systems of records that lead to exclusion: At the enrollment and identity proofing stage, critical equity questions arise about the root causes of mismatched or erroneous data. The prevailing assumption by governments and standards bodies heavily favors the conclusion that mismatched data indicate identity fraud. Current practice and standards like the NIST Guidelines do not reckon with the political realities and legacies of inequity and discrimination behind data that already exist in identity systems. For example, discrepancies and gaps in attribute provider databases like a national ID registry may contain high levels of errors for specific populations on account of human bias and error. The identity proofing and enrollment process is therefore a key point during which individuals are at risk of being excluded from a service or harmed by a digital identity system. Some groups may not have the necessary identity documents; names may have been entered into systems in ways that lead to unsuccessful matching; facial image capture or fingerprint-scanning technologies do not work well for some groups; databases against which identity data is checked will reflect historic patterns of discrimination and marginalization. These risks fall disproportionately on people of color, immigrants, undocumented persons, low-income persons, people with disabilities, and older persons, among others.

Recognize that compelling reasons may exist for individuals to self-exclude from certain digital identity processes due to trust, safety, and privacy concerns: Some individuals may also have legitimate reasons to self-exclude from identity services for fear of harassment, surveillance and exploitation. Examples include human rights defenders, those accessing sensitive heath programs such as HIV medication, communities experiencing systemic over-policing and surveillance, and non-citizens.

08 —Federation is not decentralization

Federated digital identity systems vary widely, so federation on its own should not be seen as a risk mitigation tool: The NIST Guidelines provide generalized definitions and standards for federated systems and only give minimal information to systems operators about the risks to privacy and equity in federated digital ID systems. But federated systems vary significantly in kind and retain many of the same features and risks as a 'single source' centralized ID system. Some federated digital ID systems are homogenous in terms of the kinds of services provided by the agencies or entities involved in the federation. For example, educational institutions may create a digital ID federation to allow access to digital library databases for researchers from their different institutions.[11] Other federated systems are more administratively complex because different user information is needed for different identity providers and relying parties in the federation. Federated systems will also have their own rules for how much user information is shared in order to authenticate their identity. It is possible for a user to access services anonymously in a federated system, but it is also possible for that user to be identified across the federated system through a unique identifier associated with an extensive record of their personal data and transaction history. It is critical to push for precise, verifiable information on how entities in a federation share data about users and to avoid systems which consolidate tracking or rely on invasive collection, processing and sharing of user's biometric data.

Exclusion from enrollment, invasive data collection, processing and sharing practices, and incorrect or harmful information and decisions about users can propagate across federated systems associated with a wide variety of services, significantly amplifying risks to equity: Because federated digital identity systems operate through trust agreements between a potentially extensive and heterogeneous network of service providers, the impacts on users can be equally extensive and far-reaching. It is important to carefully assess the risk-amplifying effects of federated ID systems.

11 John Palfrey and Urs Gasser, Digital Identity Interoperability and eInnovation (Berkman Center for Internet & Society, 2007)

09—Design effective feedback loops for communities and civil society to report on impacts

Civil society, communities, and user populations should play a central role in the evaluation of system operation, through regularized and formalized feedback mechanisms: In addition to broad consultation in the design and implementation of the system, a key method in preventing and detecting harmful impacts of digital identity systems is to meaningfully and regularly seek feedback from user communities and the civil society organizations who work with them. Formalized mechanisms and channels should be established to gather regular and meaningful feedback about the digital identity system. Formal mechanisms complement direct consultations with users to ascertain inequities and disparate impacts.

Qualitative data and external information should centrally inform evaluation of the system's impacts: In addition to collecting application performance metrics, organizations implementing a digital identity system should collect qualitative data about how the system is functioning, including from external sources. 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. Organizations should meaningfully take into account feedback from civil society groups who work with marginalized individuals who provide input on the impacts felt. Organizations should also integrate information from redress or grievance mechanisms, and set thresholds for when the volume of redress claims should trigger further risk assessments or other exceptional monitoring and evaluation measures.

Support research into the impacts of digital identity systems: More broadly, significant investments are needed to support research into how digital identity systems impact different user populations. Further research is needed into equity in the context of digital identity impact and risk assessment frameworks. This is an emerging field in which more activity by civil society and user populations would add considerable value to the understanding of how digital identity systems are functioning in real-life circumstances, in particular for high-risk populations and in high-risk sectors.

10—Things will go wrong: Build systems around access to redress

Ensure that redress is meaningfully accessible, for all types of harm: Risks relating to digital identity systems are often dynamic and difficult to anticipate. Individuals must be able to access redress when, for instance: identity proofing or authentication fails; errors are made; the digital identity system excludes them from accessing a service; the system has imposed burdens and caused individuals undue delays in accessing services; and for any other issues that may arise. Redress mechanisms must be designed to be accessible and usable by all, which requires the maintenance of multiple alternative channels (in person, telephone, online). Information about options for redress and avenues for technical assistance should be clearly communicated.

Ensure that responsibilities for redress are effectively allocated and that individuals know how to access redress: The Guidelines impose some redress-related requirements, including requiring credential service providers to provide redress for problems arising from identity proofing, and requiring identity providers and relying parties to provide mechanisms for users to report inequitable authentication requirements. However, a clearer and more systematic approach is needed. For instance, the Guidelines do not set minimum requirements nor provide guidance about how redress should be provided, leaving it to each provider to create its own mechanism. This approach risks creating fragmentation, unclear allocations of responsibilities, and unevenness in access to redress, as some credential service providers' mechanisms may be more unwieldy and difficult to access than others. This could also leave users confused about who they should go to when a problem arises. An alternative approach would be to require the organizations providing services (e.g. government agencies) to establish a holistic complaint mechanism through which users can seek assistance and redress for multiple types of issues. Responsibilities must then be effectively and clearly allocated among various entities within the digital identity ecosystem, but the burden of figuring out where to go when things go wrong would not fall on the individual user. A more centralized avenue for seeking redress would also enable organizations to collect systematic information about problems within their implemented digital identity system.

Provide for independent oversight of redress mechanisms: The Guidelines require that credential service providers assess the functioning of their own redress mechanisms. But self-assessment is inadequate. Centralized oversight of redress mechanisms is necessary to ensure that redress is genuinely accessible, that mechanisms are functioning and adequate, and to ensure continual improvement in the digital identity system. In the European Union, the 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.

11—Train frontline staff on how systems fail and what to do about it

Ensure that staff in frontline agencies are able to help users to access redress: To ensure that redress is meaningfully accessible and easy to use, the Guidelines should address the practicalities of seeking redress. The staff who interface with people using digital identity systems are key points of contact in ensuring users have access to redress. If staff are not provided with a clear understanding of redress mechanisms, alternatives, and avenues for complaints, this raises the risk that they will be ill-equipped to adequately respond when things go wrong within the digital identity system, and they may deny individuals access to 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. This has resulted in exclusions.12 To avoid such situations, staff should be provided with training about redress, and clear processes for helping individuals to remedy problems should be put in place. 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.

Staff who interface with users of the digital identity system should be integrated as a key part of digital identity system evaluations: Organizations should provide their staff with opportunities to share the major barriers that users face and the grievances that users commonly express. There should be a mechanism to feed staff's concerns and insights into the continuous evaluation of the digital identity system, and these inputs should lead to system improvements.

12 Lani Jacobs, Opportunities for Improving Digital Identification in Social Cash Transfer Programmes through Mobile: Insight from Kenya and Malawi (GSMA: April 2020).

12—Be aware of public/private incentive misalignment

Private sector involvement in digital identity systems that are tied to public services carries unique risks—and calls for caution, not blind embrace: Both the Guidelines and the NIST Identity and Access Management Roadmap emphasize the role of federated identity ecosystems and the potential for "greater interoperability among the federal enterprise, other parts of the public sector, and the private sector." However, there has been a poor track record, both nationally and internationally, with private sector involvement in delivering public sector digital identification needs—and in the responsible use of biometrics.[13]

Private sector failures can become public sector nightmares: The risks of integrating private companies into government services is often caused by a fundamental disconnect between the interests of individuals, the interests of public sector providers, and the interests of for-profit enterprises. The United Kingdom's attempt to create a 'marketplace' for identity services through the 'Verify' system was eventually abandoned after five of the seven accredited identity providers dropped out of the program; reliance on the marketplace model and the failed uptake led to disruptions in the provision of online public services, disproportionately affecting marginalized groups and people in poverty.[14] While the incentive structure for private identity providers may have dictated their exit from the program, it was public service users who ultimately paid the highest cost.

Recognize that privacy, security, and usability risks are not the only thing that is at stake—equity is at risk as well: The Guidelines discuss privacy, security, and usability risks in relation to federated systems. But public-private partnerships in digital identity systems and federated identity marketplaces also pose equity risks. Some biometric systems marketed and used by the private sector have raised the potential for bias and discrimination, while others have significant technical requirements that shut out those with poor connectivity or technical literacy. Public-private partnerships in federated identity systems also raise significant equity concerns due to the interoperability of datasets and the use or misuse of personal data, the potential for profiling and differential treatment, and the creation of vulnerabilities to predatory behaviors.

13 United States Federal Trade Commission, 'Press release: FTC Warns About Misuses of Biometric Information and Harm to Consumers,' May 18, 2023, at: https://www.ftc.gov/news-events/news/press-releases/2023/05/ftc-warns-about-misuses-biometric-information-harm-consumers

14 Victoria Adelmant, Marketizing the digital state: the failure of the 'Verify' model in the United Kingdom, March 30, 2021, at: https://chrgj.org/2021/03/30/marketizing-the-digital-state-the-failure-of-the-verify-model-in-the-united-kingdom/

ADDITIONAL RESOURCES ON DIGITAL IDENTITY AND TECHNICAL STANDARDS BODIES

For our full comments, see: Center for Human Rights and Global Justice, New York University School of Law, and Institute for Law, Innovation and Technology, Temple University Beasley School of Law, Comments on Draft of the NIST Digital Identity Guidelines, Special Publication 800-63-4 April 14, 2023 (2023), available at: https://chrgj.org/wp-content/uploads/2023/05/Digital-Welfare-State-Project-NYU-Law_iLIT-Temple-University_NIST-Digital-Identity-Guidelines-Comments.pdf

Alyssa Levitz, Unemployment Insurance Modernization: Identity Proofing (US Digital Response, 2021), available at https://usdr.gitbook.io/unemployment-insurance-modernization/identity-proofing-vendor-comparison/identity-proofing-vendor-comparison

Amber Sinha, Towards a Framework for Evaluation of Digital Identity (2019), available at: https://digitalid.design/evaluation-framework-01.html

Ariel Kennan, Elizabeth Bynum Sorrell, and Milda Aksamitauskas, Logging In and Providing Proof: A Guide to U.S. Government Actions on Digital Identity (Beeck Center for Social Impact + Innovation, Georgetown University, March 2023), available at: https://www.digitalbenefitshub.org/guide-to-us-federal-government-digital-identity#dig-id-standards

Berkman Klein Center, Enhancing Inclusion in Digital Identity Policies and Systems: An Assessment Framework, Final Policy Output, Research Sprint on Digital Identity in Times of Crisis (2022), available at: https://drive.google.com/file/d/1UTuFjOjcbrMWFTsuUz9Ve5XX8ea9_ufl/view?usp=share_link

Carolina Caeiro, Kate Jones and Emily Taylor, 'Technical Standards and Human Rights: The case of New IP' in Christopher Sabatini (ed.), Reclaiming Human Rights in a Changing World Order (Chatham House, 2022), available at: https://oxil.uk/publications/2021-08-27-technical-standards-human-rights/Human_rights_and_technical_standards.pdf

CDT response to the Office of the High Commissioner for Human Rights call for inputs on the relationship between human rights and technical standard-setting processes for new and emerging digital technologies, March 2023, available at: https://cdt.org/wp-content/uploads/2023/03/CDT-response-to-OHCHR-technical-standards-2023.pdf

Christine Galvagna, Octavia Reeve, Imogen Parker, and Andrew Strait, Discussion Paper: Inclusive AI Governance: Civil society participation in standards development (Ada Lovelace Institute, March 2023), available at: https://www.adalovelaceinstitute.org/wp-content/uploads/2023/03/Ada-Lovelace-Institute-Inclusive-AI-governance-Discussion-paper-March-2023.pdf

Digital Benefits Network, What Is Digital Identity? (Beeck Center for Social Impact + Innovation, Georgetown University, December 2022), available at: https://uploads-ssl.webflow.com/63345e33f3c909d27d0e558b/6387c6e49047907d41cc2dc6_FE_dcr9MSh-e8TeuUhjqV_VWco8rFN2RuAHNJTQCahE.pdf

Digital Benefits Network, Digital Identity Glossary (Beeck Center for Social Impact + Innovation, Georgetown University, December 2022), available at: https://uploads-ssl.webflow.com/63345e33f3c909d27d0e558b/6387c769b57d870c4dc3f7d9_fLpkGAcbr0kjGuDqgwnD_pgSx1Q-FqJCLkxgK8KGWoA.pdf

Financial Action Task Force, 'Appendix A' in Guidance on Digital Identity, (FATF, Paris, 2020), available at: https://www.fatf-gafi.org/content/dam/fatf-gafi/guidance/Guidance-on-Digital-Identity-Appendice%20A.pdf

Mallory Knodel, Joey Salazar, and Mehwish Ansari, A Guide to the Internet Engineering Task Force (IETF) For Public Interest Advocates (Article 19 and the Center for Democracy & Technology, January 2023), available at: https://cdt.org/wp-content/uploads/2023/02/Art19-Guide-to-the-IETF-2023-03-21.pdf

Michele Gilman, Poverty Lawgorithms: A Poverty Lawyer's Guide to Fighting Automated Decision-Making Harms on Low-Income Communities (Data & Society, 2020), available at: https://datasociety.net/wp-content/uploads/2020/09/Poverty-Lawgorithms-20200915.pdf

Nick Doty, Alissa Cooper and Wendy Seltzer, Human rights and technical standard-setting for the Web, Unofficial Draft 10 March 2023, available at: https://cdt.org/wp-content/uploads/2023/03/human-rights-web-standards.html

World Bank, 'Glossary' in ID4D Practitioner' Guide: Version 1.0 (October 2019), available at: https://id4d.worldbank.org/guide/glossary

World Bank, Catalog of Technical Standards for Digital Identification Systems, (August 2022), available at https://id4d.worldbank.org/technical-standards

United Kingdom, Government Office for Science, Biometrics: A Guide (2019), available at https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/715925/biometrics_final.pdf

United Nations Office for the High Commissioner for Human Rights, Call for inputs: "The relationship between human rights and technical standard-setting processes for new and emerging digital technologies (2023)", Report of the High Commissioner for Human Rights, available at: https://www.ohchr.org/en/calls-for-input/2023/call-inputs-relationship-between-human-rights-and-technical-standard-setting

CENTER FOR HUMAN RIGHTS & GLOBAL JUSTICE
NYU SCHOOL OF LAW

This explainer is the result of a joint project between the Center for Human Rights and Global Justice at New York University School of Law and the Institute for Law, Innovation and Technology at Temple University Beasley School of Law. It was written by Victoria Adelmant, Katelyn Cioffi, and Laura Bingham. Graphic design by Uma Natarajan.

This is a living document that will improve with input from affected communities and interested parties. We welcome your participation and feedback.

Publication date: June 2023

https://chrgj.org/

https://law.temple.edu/ilit/