ML STRATEGIES

NIST Releases Updated Draft Guidance for Federal Agencies' Use of AI in Identity Verification Systems — AI: The Washington Report

September 12, 2024 | | By **Bruce Sokler**, **Alexander Hecht**, **Christian Tamotsu Fjeld**, Matthew Tikhonovsky

- On August 21, the National Institute of Standards and Technology (NIST) released the **second draft** of its revised Digital Identity Guidance, which NIST first published in 2004 and last revised in 2017.
- The draft guidance provides a framework and requirements for government agencies to securely verify the identity of external individuals, employees, and contractors accessing or interacting with government services and information systems.
- The second draft of the guidance includes a section on AI for the first time, with three requirements for AI that focus on transparency and risk mitigation.
- NIST's public comment period for the draft guidance ends on October 7, 2024.

On August 21, 2024, the National Institute of Standards and Technology (NIST) released its second draft for the fourth revision of the **Digital Identity Guidelines**. The revised draft guidance puts forth a risk-mitigating framework and requirements for "identity proofing and authentication of users (such as employees, contractors or private individuals)" accessing government services or interacting with government information systems online. Building off the **first draft** of the revised guidance, the latest draft now includes an entire section on AI in identity systems, recognizing both the benefits and risks that AI poses in identity systems and proposing three broad requirements to mitigate these risks.

Background on the Digital Identity Guidelines

In December 2022, NIST published an **initial draft** for the fourth revision to NIST's Special Publication 800-63, Digital Identity Guidelines, which NIST first published in 2004 and revised for the third time in 2017. The Digital Identity Guidelines have historically sought to aid federal agencies in verifying the identity of external users, employees, and contractors who access or interface with government systems. Responding to concerns about online impersonation and fraud as well as recent technological advances that have created new and more complex digital identity challenges, the initial draft of the new revised guidance put forth a more robust framework and set of requirements for strengthening identity verification and authentication, while also focusing on mitigating risks in the identity verification process.

The initial draft guidance was followed by a four-month comment period in early 2023, in which over 4,000 comments were submitted. Many comments focused on the need for additional guidance for digital wallets, passkeys, and facial recognition systems, according to a NIST **article**, all of which are digital identity technologies that may rely on AI. Notably, however, the initial draft guidance did not specifically address the use of AI in digital identity systems.

NIST Guidance for AI in Identity Systems

The second draft of the revised guidance builds onto the risk-mitigating framework for identity systems proposed in the first draft but adds a new section on AI. The second draft puts forth various identity proofing models, new requirements for the continuous evaluation of digital identity systems, safeguards for detecting and preventing fraud, and different authentication methods for use cases with different risks. The draft guidance would primarily apply to federal agencies that provide services for "external users, such as residents accessing public benefits or private-sector partners accessing collaboration spaces," but it would also apply to "federal systems accessed by employees and contractors."

"These improved guidelines are intended to help organizations of all kinds manage risk and prevent fraud," **according to** NIST Director Laurie E. Locascio, "while ensuring that digital services are lawfully accessible to all."

On AI, the second draft of the revised guidance recognizes that AI can play multiple, "extensive" roles in digital identity systems, such as "improving the performance of biometric matching systems, documenting authentication, detecting fraud, and even assisting users (e.g., chatbots)." However, the draft guidance notes that the use of AI in digital identity systems also carries numerous risks, "including disparate outcomes, biased outputs, and the exacerbation of existing inequities and access issues."

Balancing the benefits and risks of AI, the new draft guidance proposes three requirements for AI in identity systems, focused on transparency and risk mitigation:

1. Organizations that rely on AI would be required to document and communicate about their AI usage in identity systems. Identity providers and content security policies that leverage AI would be required to document and communicate their AI "usage to all [relying parties] that make access decisions based on information from these systems."
2. Organizations that utilize AI would be required to provide certain information "to any entities that use their technologies," including information about the techniques and datasets used for training their models, the frequency of model updates, and the results of any tests of their algorithms.
3. Lastly, organizations that utilize AI or rely on systems that use AI would be required to adopt the NIST's ***AI Risk Management Framework*** for AI risk evaluation, and also consult the ***Towards a Standard for Managing Bias in Artificial Intelligence***. Both NIST publications lay out practical steps to reduce AI bias, including using datasets with balanced statistical presentation, documenting potential sources of human bias into datasets, updating and testing AI models regularly, creating a fairness metric by which to evaluate AI models, and assembling diverse and inclusive teams to design and deploy AI systems.

The draft guidance also announced that NIST's US AI Safety Institute is "creating a portfolio of safety-focused resources, guidance, and tools that can improve how organizations assess, deploy, and manage their AI systems." In the meantime, NIST is accepting comments on the draft guidance until October 7, 2024.

Authors

Bruce Sokler

Bruce D. Sokler is a Mintz antitrust attorney. His antitrust experience includes litigation, class actions, government merger reviews and investigations, and cartel-related issues. Bruce focuses on the health care, communications, and retail industries, from start-ups to Fortune 100 companies.

Alexander Hecht, Executive Vice President & Director of Operations

Alexander Hecht is Executive Vice President & Director of Operations of ML Strategies, Washington, DC. He's an attorney with over a decade of senior-level experience in Congress and trade associations. Alex helps clients with regulatory and legislative issues, including health care and technology.

Christian Tamotsu Fjeld, Senior Vice President

Christian Tamotsu Fjeld is a Vice President of ML Strategies in the firm's Washington, DC office. He assists a variety of clients in their interactions with the federal government.

Matthew Tikhonovsky

Matthew is a Mintz Senior Project Analyst based in Washington, DC.