NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
U.S. DEPARTMENT OF COMMERCE

# NIST's Digital Identity Guidelines: An Overview of the Draft Update

Ryan Galluzzo, Identity Program Lead
Applied Cybersecurity Division
Information Technology Lab

17 February 2023

# What is NIST's Role in Digital Identity?

NIST's Identity Program is a multi-disciplinary group of IAM Experts, Cryptographers, Mathematicians, Privacy Engineers, Policy Advisors, UX Specialists, and Biometrics Experts who…

**Create Guidance** that is mandatory for federal agencies and voluntary but widely adopted by commercial entities.

**Develop Standards** such as Federal Information Processing Standards and contribute to international standards in ISO, W3C, and FIDO.

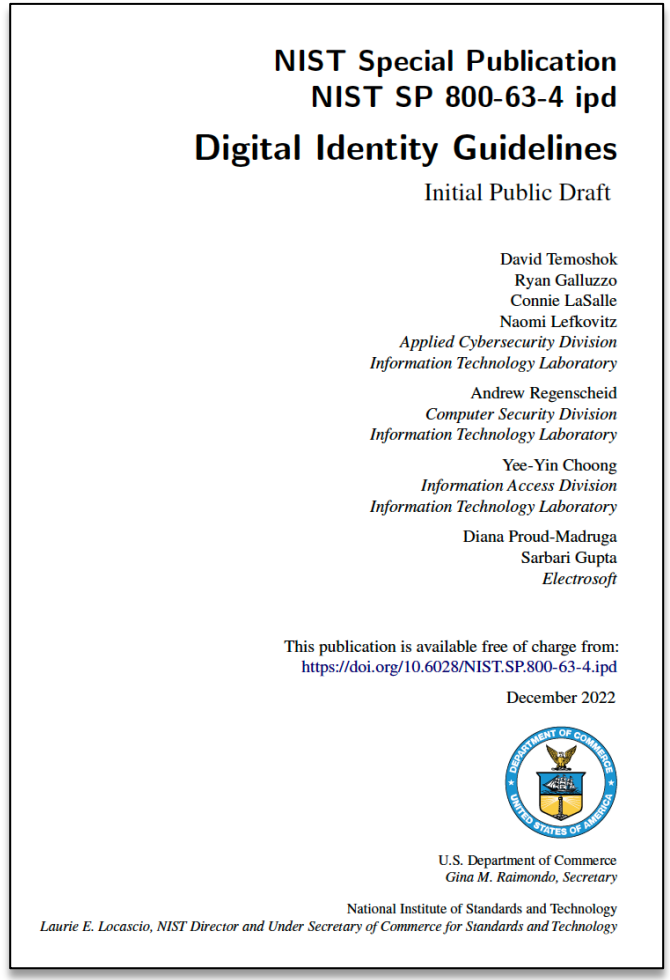
**Conduct foundational and applied research into** Identity Technology and how it impacts standards and implementation.

**Enhance Metrology** of identity systems to better understand performance, security, and equity of digital identity implementation.

**Enable "transition to practice" through** materials that promote adoption, support implementation, and accelerate the impacts of standards and guidance.

# What Are the Digital Identity Guidelines?

- Details the process and technical requirements for digital identity management.
- Describes identity risk management process and assurance level selections (identity proofing, authentication, federation).
- Provides considerations for enhancing privacy and usability of digital identity solutions and technology.
- Inclusive of 4 volumes:
  - Base – Digital Identity Model and Risk Management
  - A – Identity Proofing & Enrollment
  - B – Authentication & Lifecycle Management
  - C – Federation & Assertions
- Last major revision was in June of 2017



NIST Special Publication
NIST SP 800-63-4 ipd

**Digital Identity Guidelines**

Initial Public Draft

David Temoshok
Ryan Galluzzo
Connie LaSalle
Naomi Lefkovitz
*Applied Cybersecurity Division*
*Information Technology Laboratory*

Andrew Regenscheid
*Computer Security Division*
*Information Technology Laboratory*

Yee-Yin Choong
*Information Access Division*
*Information Technology Laboratory*

Diana Proud-Madruga
Sarbari Gupta
*Electrosoft*

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-63-4.ipd

December 2022

U.S. Department of Commerce
*Gina M. Raimondo, Secretary*

National Institute of Standards and Technology
*Laurie E. Locascio, NIST Director and Under Secretary of Commerce for Standards and Technology*

# Why Are We Making Changes?

- Advance equity.
- Emphasize optionality and choice for individuals.
- Deter phishing, fraud, and advanced threats.
- Address lessons learned through real-world implementations.
- Emphasize multi-disciplinary risk management processes.
- Clarify and consolidate requirements where needed.

***OUR WORLD HAS CHANGED IN PROFOUND WAYS SINCE 2017; IT IS TIME FOR OUR GUIDANCE TO CHANGE TOO…***

# What Are Some Our Key Changes?

The draft introduces substantive changes to all four volumes and specifically…

Revamps Risk Management and Assurance Selection Process

Updates biometric performance requirements for proofing and authentication

Introduces digital evidence concept (e.g., mDL and Verifiable Credentials)

Defines phishing resistance and updates password requirements (e.g., composition & rotation)

Mandates Trusted Referees as an option and introduces Applicant References

Establishes a new Identity Assurance Level 1 where biometrics are optional

Provides normative language for the vendors and agencies to assess the impact of technology on equity

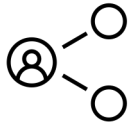
# What Are We Researching and Assessing?

Even as our comment period continues there are still areas we continue to research, assess, and build including:

- Syncable and shareable credentials (i.e., Passkeys)
- Identity proofing methods, for example risk analytics, risk scoring, behavioral analysis, and methods that do not rely up on biometrics
- Mobile Driving License, Verifiable Credentials, EU Wallets, and their emerging ecosystems
- Application of privacy enhancing technology for fraud detection models
- Biometric algorithm testing for Presentation Attack Detection, Morph Detection, and Demographic Performance

# How Can You Get Involved?

**Comment on our guidance!** We need your feedback! Comments on the Digital Identity Guidelines are due March 24th (send to dig-comments@nist.gov)



**Engage at the NCCoE!** From communities of interest to actual project participation there are multiple pathways to participate. https://www.nccoe.nist.gov/

**Participate in our events!** We have three upcoming webinars in March you can register here: https://www.nccoe.nist.gov/digital-identity-guidelines-webinar-series

**Email us and just say "hey!"** We can be reached at dig-comments@nist.gov or email me directly at ryan.galluzzo@nist.gov

***Digital Identity Guidelines Comments Are Due March 24th***

# Questions?

# Bonus Slide!

# How Does the Comment Period Work?

- Where can I find the documents?
  - 800-63-4: Base Volume
  - 800-63A-4: Identity Proofing and Enrollment
  - 800-63B-4: Authentication and Lifecycle Management
  - 800-63C-4: Federation and Assertions
- How do I submit comments?
  - Email them to: dig-comments@nist.gov
- What format should my comments be in?
  - The preferred format is the comment sheet available here: Comment template (xls)
- What kind of comments are most helpful?
  - All of them!
  - Reference our Note to Reviewers for specific questions
  - Please do not send marketing material
- What if I have questions before I submit comments?
  - Email any questions or requests for clarifications you may have to: dig-comments@nist.gov
  - We will do our best to respond to as many questions as possible
- Will my comments be made public?
  - Yes! Our process is open and transparent and we will post all comments as issues on our GitHub repository
- How can I keep up to speed on any changes?
  - There will not be changes to the text between now and the close of the comment period
  - But, if we get frequent comments or areas where clarification is regularly requested, we will post them to our "Ongoing Updates" page
  - Follow along at: https://pages.nist.gov/800-63-4/

***COMMENTS ARE DUE MARCH 24th***