Master Class:
NIST Digital Identity Guidelines - SP 800-63 Draft Revision 4

Ryan Galluzzo

Identity Program Lead

NIST

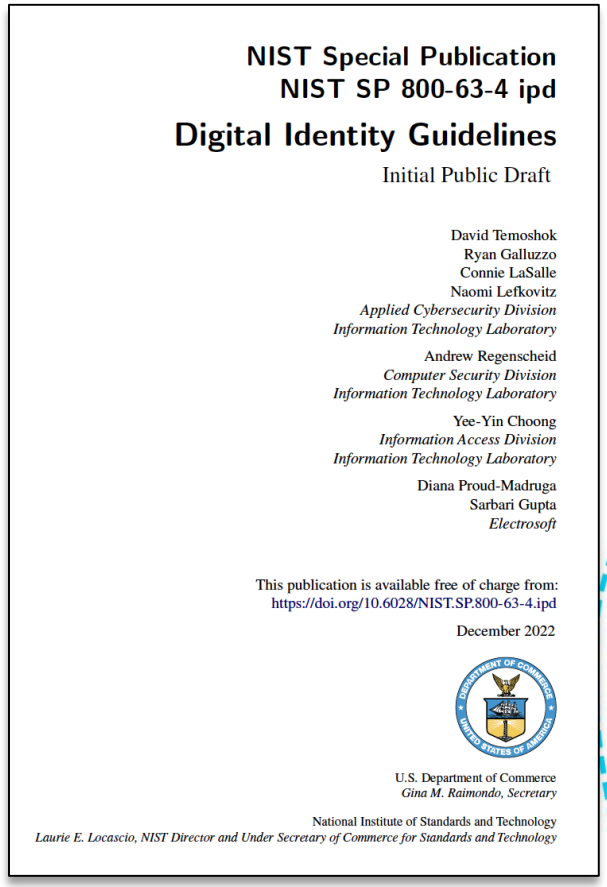
Andrew Regenscheid

PIV Technical Lead

NIST

Digital Identity Guidelines Overview

- Details the process and technical requirements for Digital Identity
- 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 We Made 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.

What Changed? Major Updates

- 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 and introduces Applicant References
- Establishes a new Identity Assurance Level 1 where biometrics are optional
- Provides normative language for vendors and agencies to assess the impact of technology on equity

What Will We Cover Today?

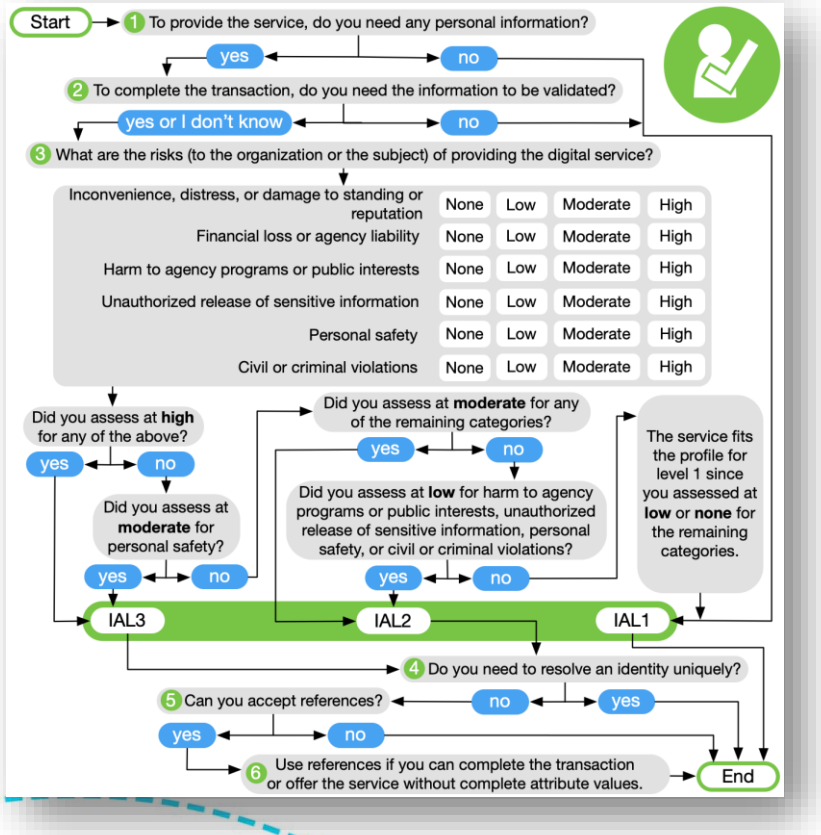
Risk Management and Assurance Selection

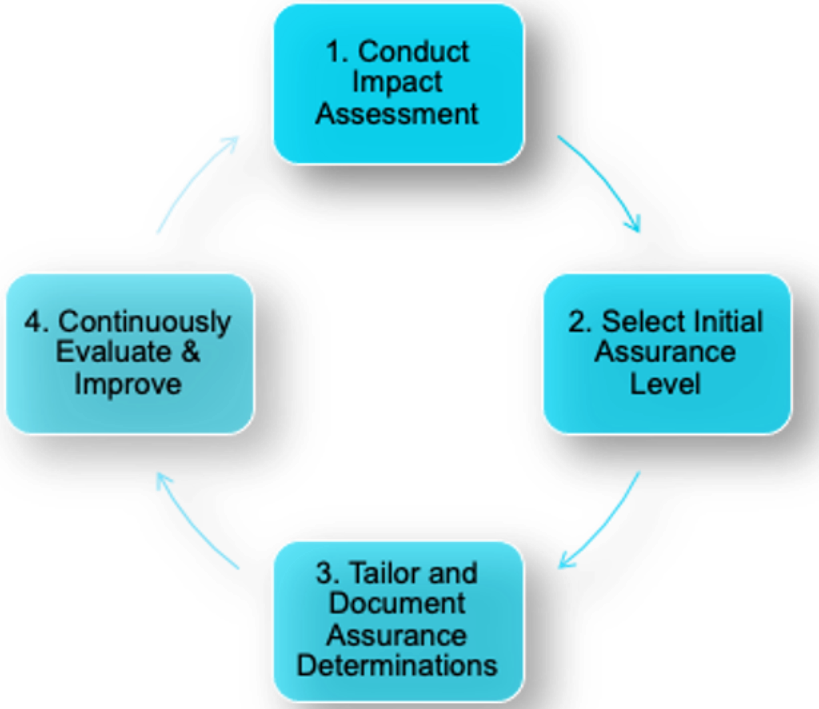
Trusted Referees and Applicant References

Phishing resistance

Public Comments & What's Next

Risk Management & Assurance Level Selection: Re-emphasizing Risk Management





FROM COMPLIANCE TOWARDS RISK MANAGEMENT

Risk Management & Assurance Level Selection: Process Overview

1. Conduct Impact Assessment

Understand your users & application

Assess the impact of potential harms

Document impact level

2. Select Initial Assurance Level

Understand the xALs

Map impact level to xALs

Select your ”baseline” xALs

3. Tailor and Document Assurance Determinations

Evaluate the impact of the xALs

Conduct detailed assessments

Select final xALs and controls

4. Continuously Evaluate & Improve

Define metrics

Establish data collection process

Integrate program

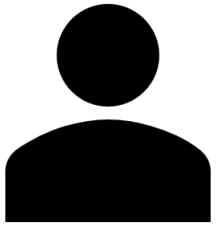
Evaluate & improve

Trusted Referees & Applicant References: What are they?

Trusted Referee

- Required
- Acts as an agent of the CSP
- Trained to make risk-based decisions based on evidence
- Is known and vetted by the CSP
- Virtual, In-Person, Asynchronous
- ***NOT*** just “attended proofing”

- Recommended
- Acts in support of the individual
- Has knowledge of applicant’s identity and circumstances
- Proofed at least the same xAL.
- Virtual, In-Person, Asynchronous
- ***NOT*** a power of attorney



Applicant Reference

BOTH CONCEPTS HELP ADVANCE INCLUSION AND OPTIONALITY

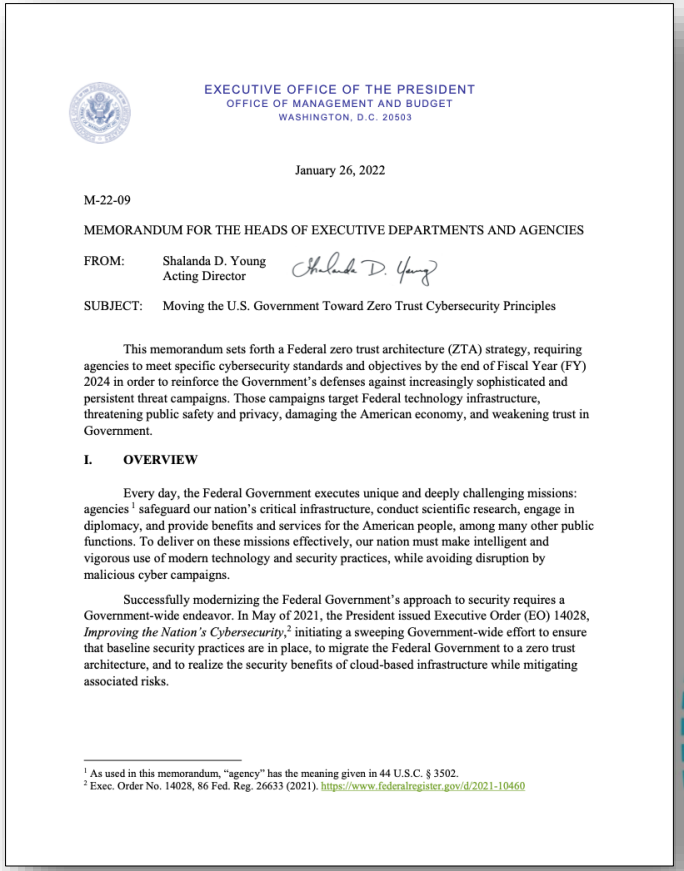
Phishing Resistance

- Increased sophistication in phishing attacks as MFA adoption has grown

Steal static authenticators, e.g., passwords

Relay dynamic authenticators, e.g., OTP

- New forms of strong, phishing-resistant MFA available to enterprises and users
- Phishing resistance in 800-63B-4:
  - ***Required*** at AAL3
  - ***Recommended*** at AAL2
- OMB M-22-09 further requires federal agencies to offer a phishing-resistant authenticator option to public users



EXECUTIVE OFFICE OF THE PRESIDENT
OFFICE OF MANAGEMENT AND BUDGET
WASHINGTON, D.C. 20503

January 26, 2022

M-22-09

MEMORANDUM FOR THE HEADS OF EXECUTIVE DEPARTMENTS AND AGENCIES

FROM: Shalanda D. Young
Acting Director

SUBJECT: Moving the U.S. Government Toward Zero Trust Cybersecurity Principles

This memorandum sets forth a Federal zero trust architecture (ZTA) strategy, requiring agencies to meet specific cybersecurity standards and objectives by the end of Fiscal Year (FY) 2024 in order to reinforce the Government's defenses against increasingly sophisticated and persistent threat campaigns. Those campaigns target Federal technology infrastructure, threatening public safety and privacy, damaging the American economy, and weakening trust in Government.

I. OVERVIEW

Every day, the Federal Government executes unique and deeply challenging missions: agencies [1] safeguard our nation's critical infrastructure, conduct scientific research, engage in diplomacy, and provide benefits and services for the American people, among many other public functions. To deliver on these missions effectively, our nation must make intelligent and vigorous use of modern technology and security practices, while avoiding disruption by malicious cyber campaigns.

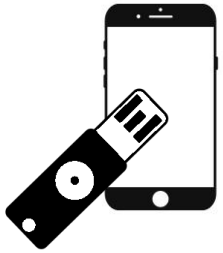
Successfully modernizing the Federal Government's approach to security requires a Government-wide endeavor. In May of 2021, the President issued Executive Order (EO) 14028, *Improving the Nation's Cybersecurity*,[2] initiating a sweeping Government-wide effort to ensure that baseline security practices are in place, to migrate the Federal Government to a zero trust architecture, and to realize the security benefits of cloud-based infrastructure while mitigating associated risks.

[1] As used in this memorandum, "agency" has the meaning given in 44 U.S.C. § 3502.
[2] Exec. Order No. 14028, 86 Fed. Reg. 26633 (2021). https://www.federalregister.gov/d/2021-10460

Phishing Resistance

Channel Binding– *e.g., Client-Authenticated TLS*

- Authentication bound to TLS session between client/server
- Strong security properties mitigating web vulnerabilities/attacks
- Requires PKI and and user certificates



Verifier Name Binding– *e.g., WebAuthn/FIDO2*

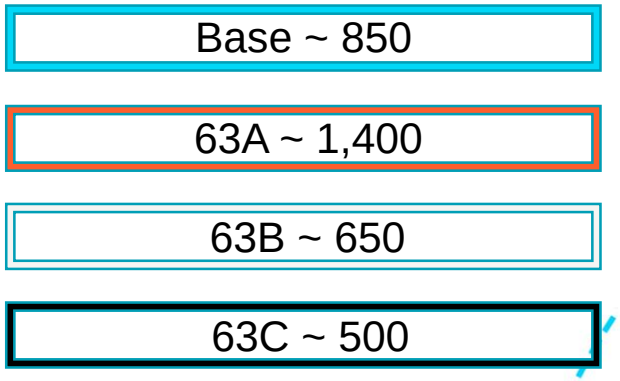
- Authentication bound to web origin/domain
- Prevents relay attacks by lookalike/phishing web sites
- Authenticators embedded in platforms or as standalone tokens

Public Comment Period: Did NIST Get Much Input?

119
Day
Comment Period

130+
Contributions

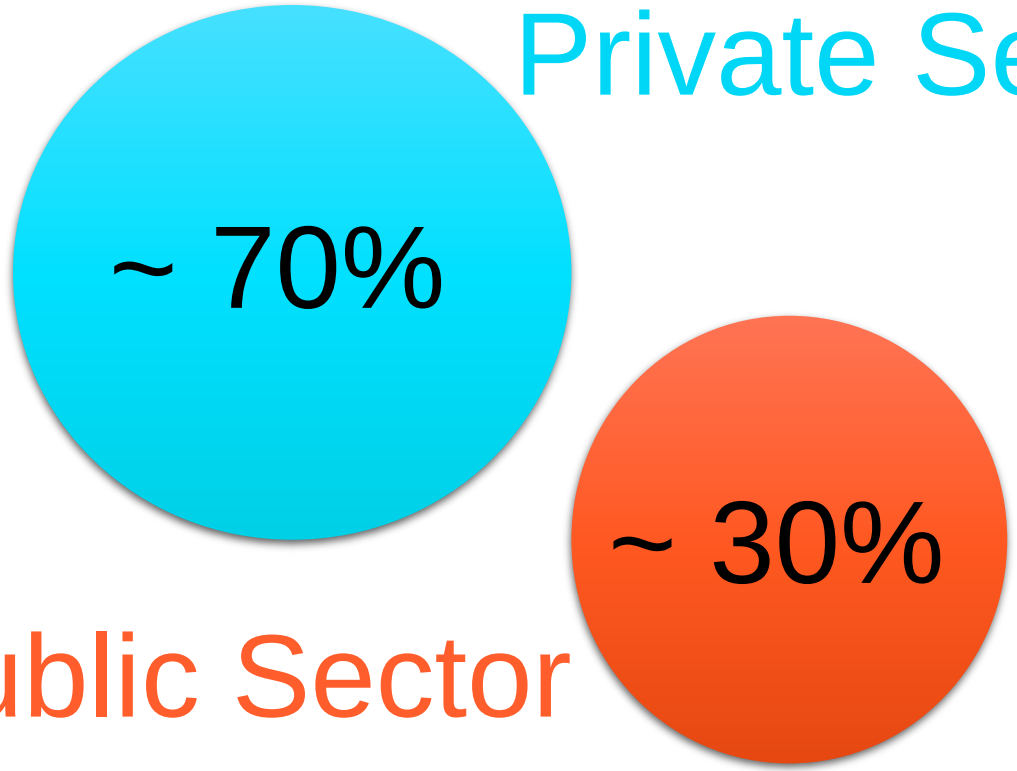
3,400+
Comments/Issues



General Comment Distribution

End of the Comment Period is NOT the end of the conversation!

Public Comment Period: Who Did You Hear From?

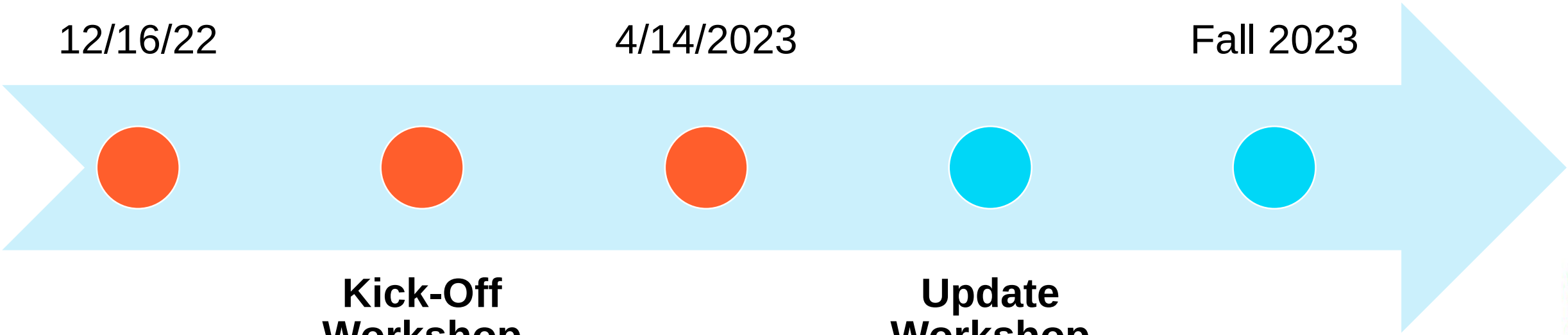


- Government
- Advocacy
- Gaming & Gambling
- Identity Services
- Higher Education
- Manufacturing
- Security

Public Comment Period: What Did They Say?

Trusted Referee and Applicant Reference are generally well received, but more detail is desired	Accounting for synchable authenticators (e.g., passkeys) and their associated requirements
Additional detail is needed on the use of digital evidence in particular how mDL and VC may be used	Clarification on tailoring and how to continue to support interoperability and flexibility together
Additional baseline fraud requirements – specifically for CSPs – and fraud program expectations	Mapping of assurance levels more directly to the mitigated attacks at each level
Additions to the digital identity model to account for ”holder, issuer, verifier” model & attribute services	Treatment of FAIR evidence and the value it brings to the proofing process

What is Next?



Draft Released!
12/16/22

Kick-Off Workshop
1/12/23

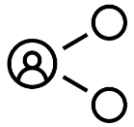
Close of Comment Period
4/14/2023

Update Workshop
Summer 2023

Publication Decision Point
Fall 2023

Get Involved!

Comment on our documents! We have several open comment periods – including our IAM Roadmap comments are due June 16th!

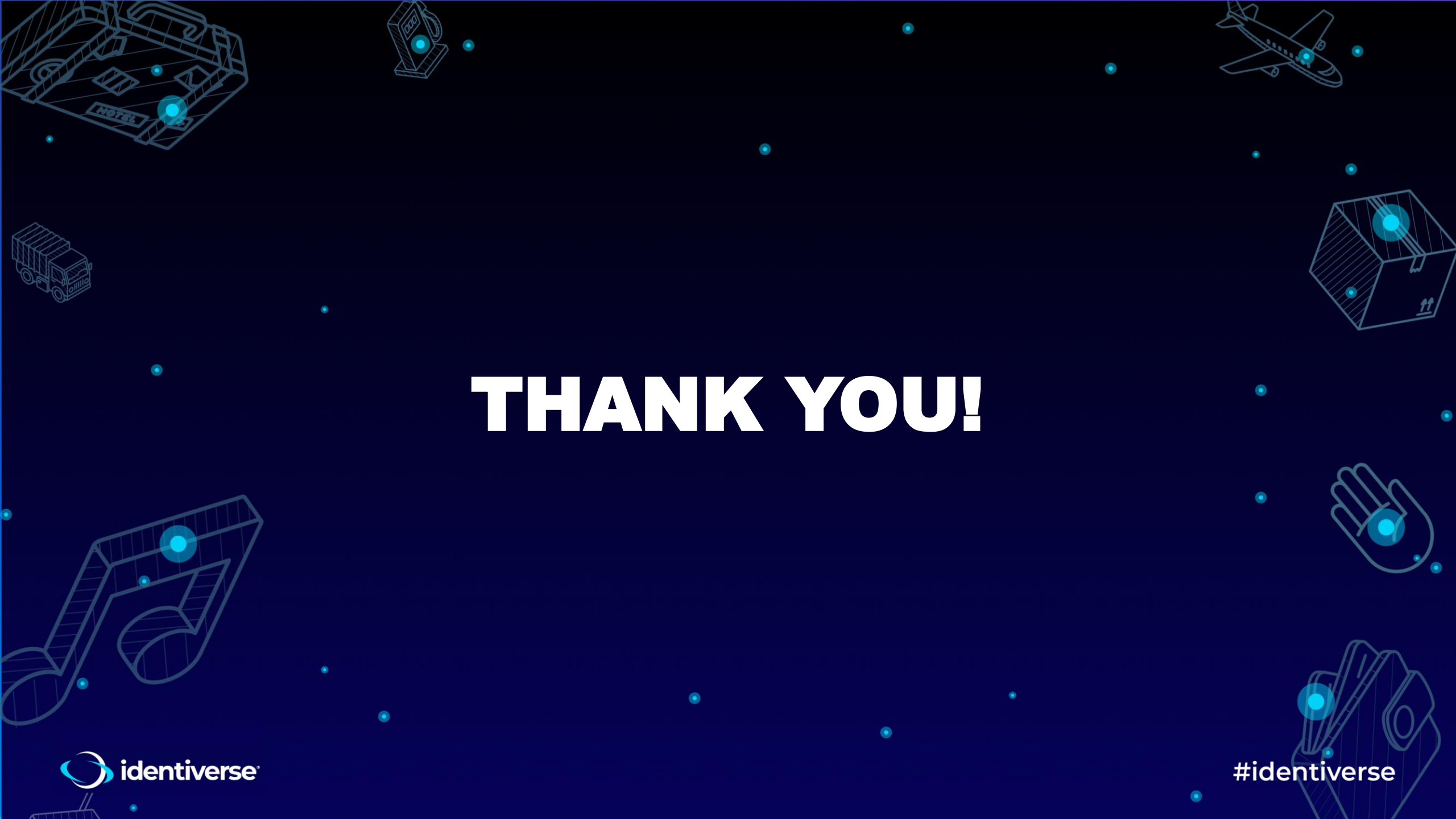


Engage at the NCCoE! From communities of interest to actual project participation there are multiple pathways to participate.

Participate in our Workshops! We have multiple events throughout the year to gain feedback, input, and insights from the community at large!

Email us and just say "hey!" We can be reached at dig-comments@nist.gov or digital_identity@nist.gov

Questions?


THANK YOU!
identiverse
#identiverse