

# Draft Special Publication 800-63-3

## Digital Identity Guidelines *(formerly known as Electronic Authentication Guideline)*



**SP 800-63-3**

Digital Identity  
Guidelines



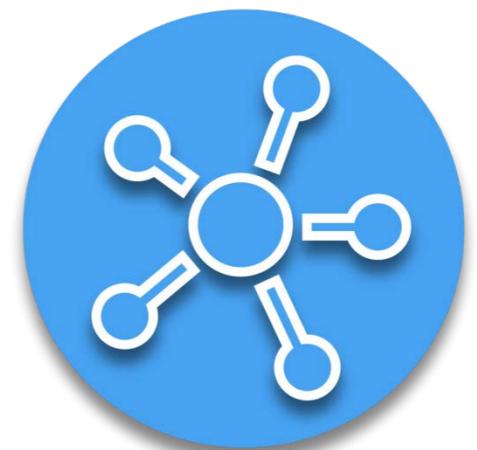
**SP 800-63A**

Identity Proofing &  
Enrollment



**SP 800-63B**

Authentication &  
Lifecycle Management



**SP 800-63C**

Federation &  
Assertions

<https://pages.nist.gov/800-63-3>

<http://csrc.nist.gov/publications/PubsDrafts.html#800-63-3>

# Why the update?

- Implement Executive Order 13681: *Improving the Security of Consumer Financial Transactions*
- Align with market and promote (adapt to) innovation
- Simplify and provide clearer guidance
- International alignment

The White House

Office of the Press Secretary

For Immediate Release

October 17, 2014

## Executive Order --Improving the Security of Consumer Financial Transactions

EXECUTIVE ORDER

-----

IMPROVING THE SECURITY OF CONSUMER FINANCIAL  
TRANSACTIONS

# Highlights from the Public Comment Period

January – May 2017

4900+

Views on  
Github

540+

Unique  
Visitors

1113

Comments

~800

Accepted

~142

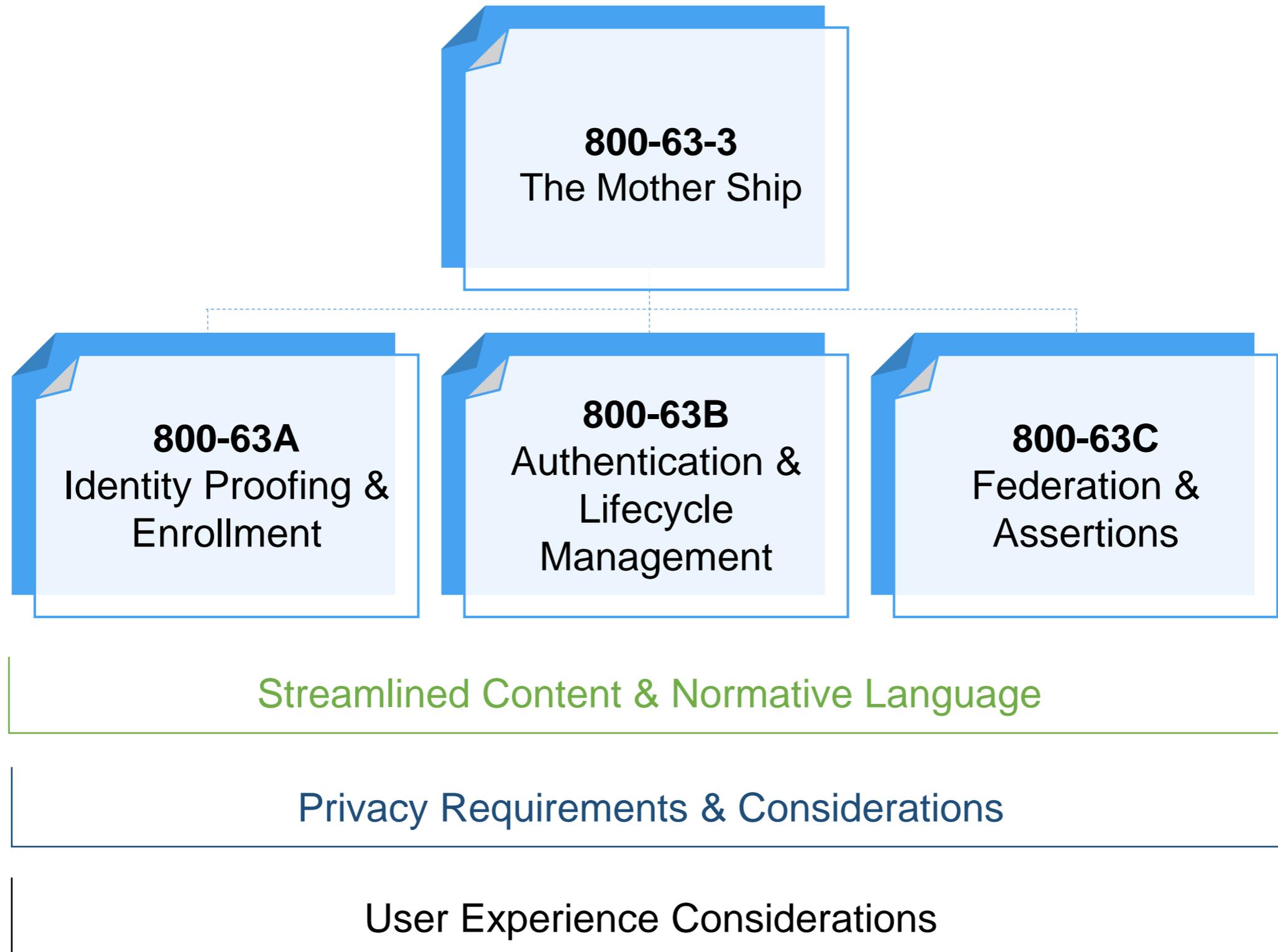
Duplicates

~239

Decline/Noted



# Making 800-63 More Accessible

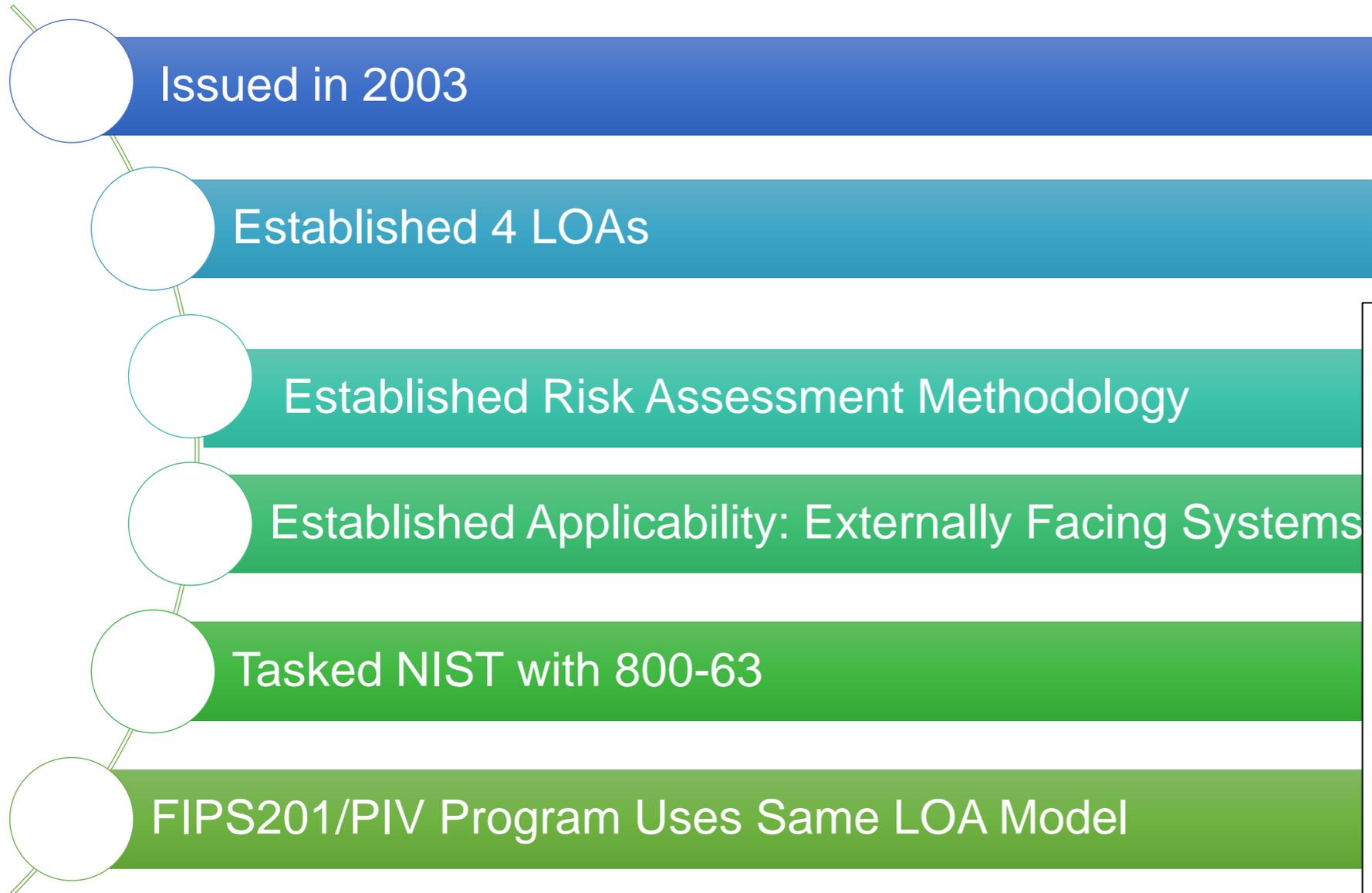


**SP 800-63-3**  
**Digital  
Identity  
Guideline**

---



# In the beginning...OMB M-04-04



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

THE DIRECTOR  
December 16, 2003

M-04-04  
MEMORANDUM TO THE HEADS OF ALL DEPARTMENTS AND AGENCIES

FROM: Joshua B. Bolten   
Director

SUBJECT: E-Authentication Guidance for Federal Agencies

The Administration is committed to reducing the paperwork burden on citizens and businesses, and improving government response time to citizens – from weeks down to minutes. To achieve these goals, citizens need to be able to access government services quickly and easily by using the Internet. This guidance document addresses those Federal government services accomplished using the Internet online, instead of on paper. To make sure that online government services are secure and protect privacy, some type of identity verification or authentication is needed.

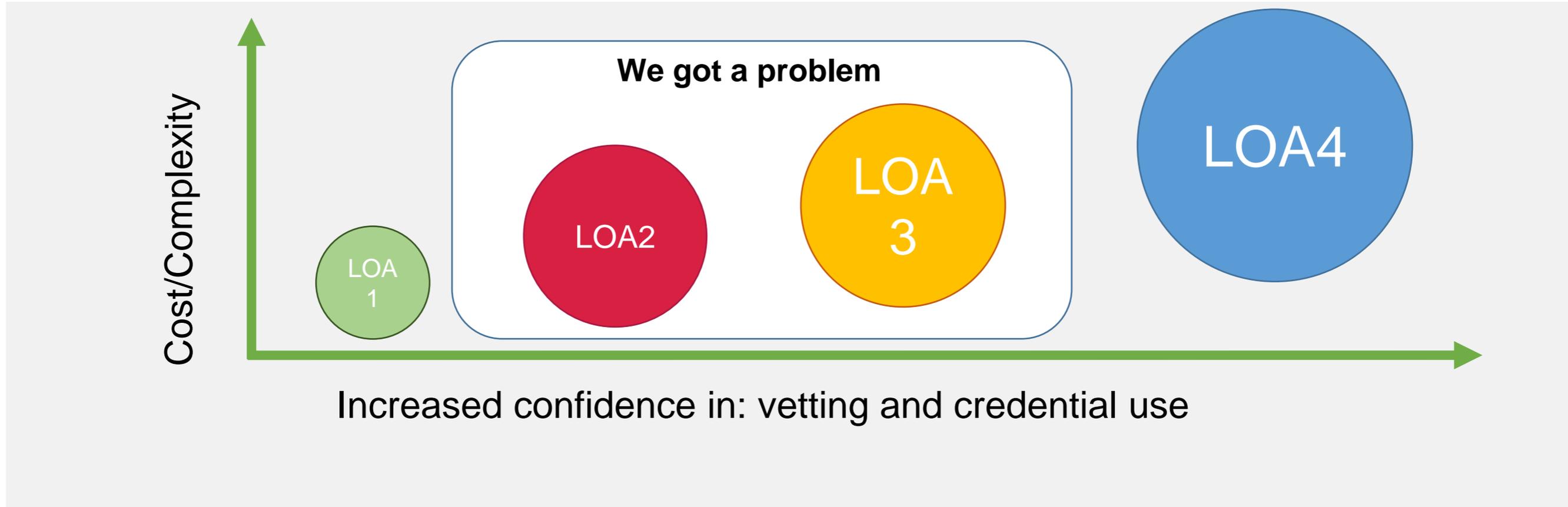
The attached guidance updates guidance issued by OMB under the Government Paperwork Elimination Act of 1998, 44 U.S.C. § 3504 and implements section 203 of the E-Government Act, 44 U.S.C. ch. 36. This guidance also reflects activities as a result of the E-Authentication E-Government Initiative and recent standards issued by the National Institute of Standards and Technology (NIST). In preparing this guidance, we have worked closely with and incorporated comments from agency Chief Information Officers.

This guidance takes in account current practices in the area of authentication (or e-authentication) for access to certain electronic transactions and a need for government-wide standards and will assist agencies in determining their authentication needs for electronic transactions. This guidance directs agencies to conduct “e-authentication risk assessments” on electronic transactions to ensure that there is a consistent approach across government. (see Attachment A). It also provides the public with clearly understood criteria for access to Federal government services online. Attachment B summarizes the public comments received on an earlier version of this guidance.

For any questions about this guidance, contact Jeanette Thornton, Policy Analyst, Information Policy and Technology Branch, Office of Management and Budget, phone (202) 395-3562, fax (202) 395-5167, e-mail: [eaauth@omb.eop.gov](mailto:eaauth@omb.eop.gov).

Attachments  
Attachment A – E-Authentication Guidance for Federal Agencies  
Attachment B – Summary of Public Comments and Responses

# What are Levels of Assurance



**LOA**] mitigates the risk associate of a potential **authentication error**

# What's wrong with LOA2?

SP 800-63-2

identity proofing

LOA2

≈

LOA3

LOA1

≈

LOA2

authenticators

EO 13681

“...consistent with the guidance set forth in the 2011 National Strategy for Trusted Identities in Cyberspace, to ensure that all agencies making personal data accessible to citizens through digital applications require the use of multiple factors of authentication and an effective identity proofing process, as appropriate.”

# Not to mention...

OMB M-04-04:

LOA selected by “determining the potential impact of authentication errors”

However, an authentication error is not a singleton:

- 1: Authentication error = attacker steals authenticator
- 2: Proofing error = attacker proofs as someone else

...and...

Requiring authN and proofing to be the same could be inappropriate

# A real example

Assessed at LOA1:



No proofing



Single factor authN

Should be:



IAL1: No proofing



AL2 (or higher): Multifactor authN

**USAJOBS**

Sign in

Username or email

Enter your username, primary email, or secondary email.

Password

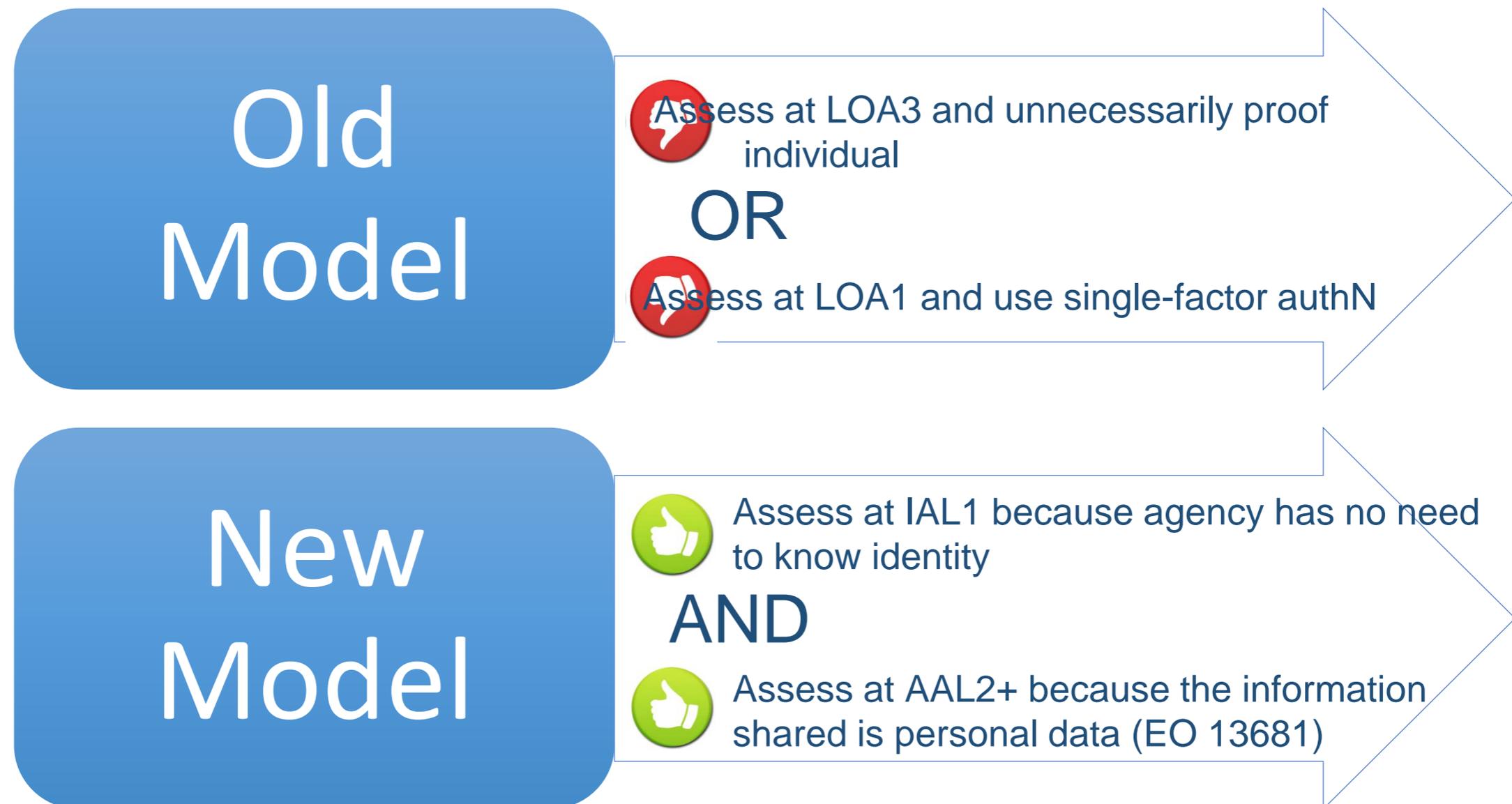
[Forgot your username or password?](#)

Sign In

# A future example



## Health Tracker Application



# The Plan

---

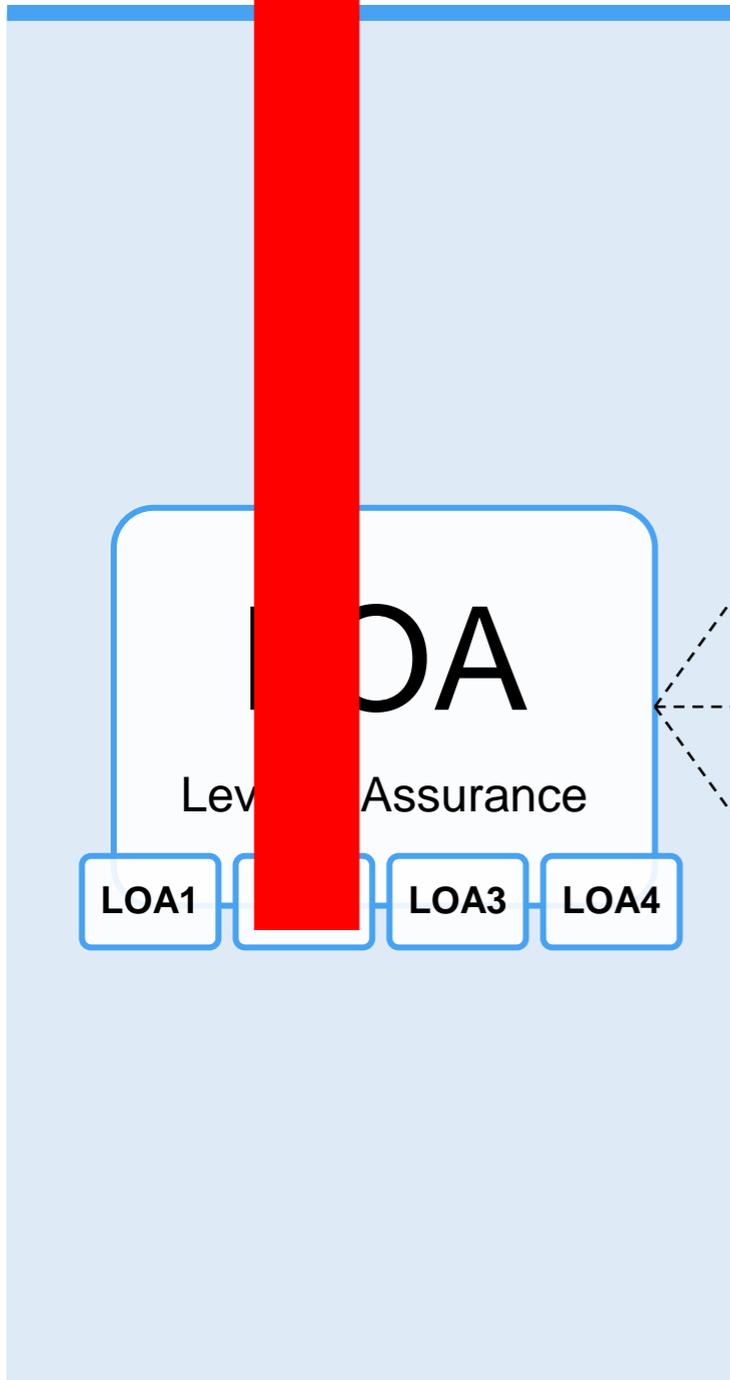


- OMB rescinds M-04-04
- 800-63-3 takes on digital identity risk management and becomes normative
- eAuth risk assessment goes away, Risk Management Framework 'adorned' with identity risks and impacts
- Agencies have risk-based flexibility
- But if they take it, a digital identity acceptance statement is needed

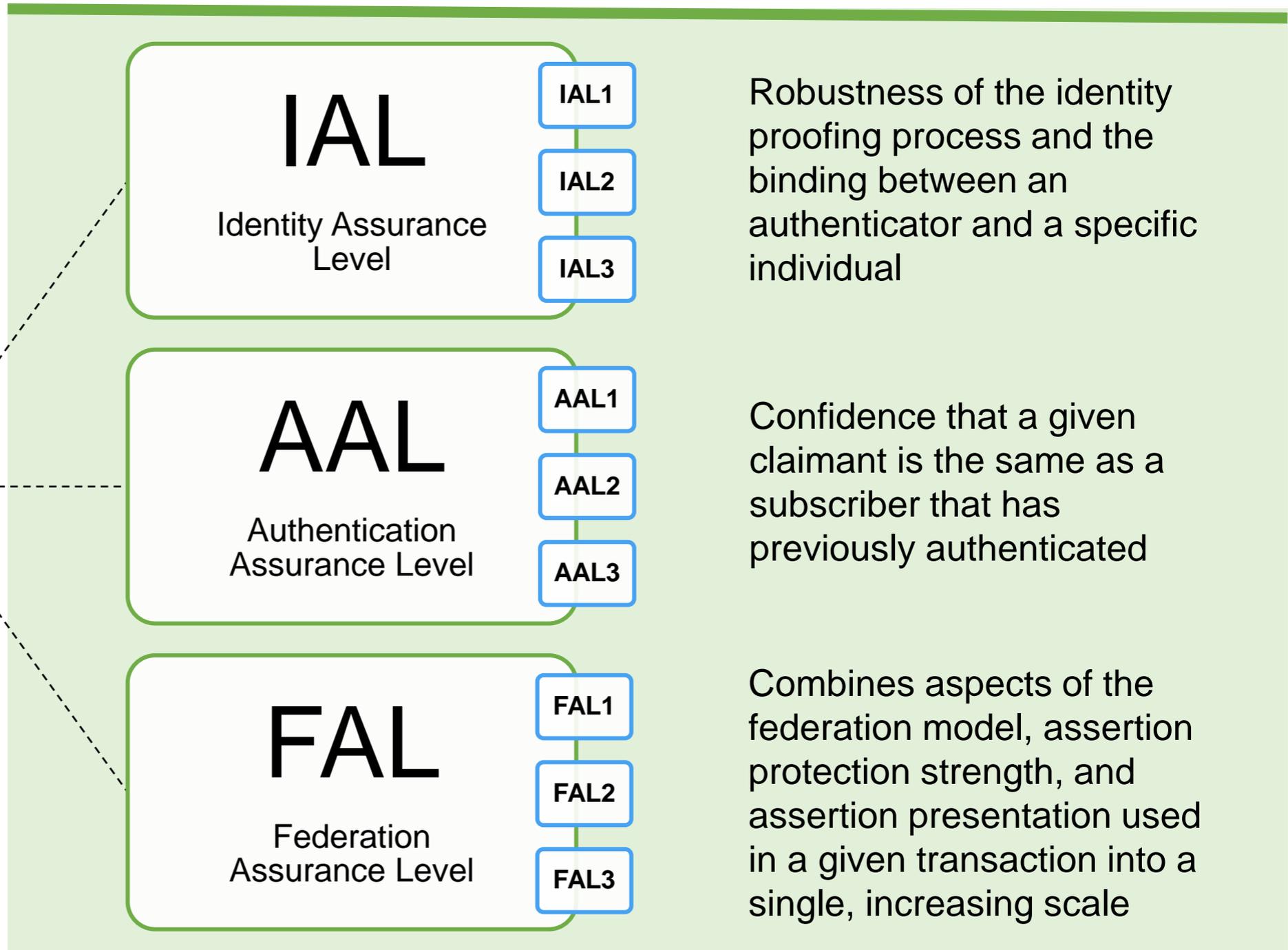
\*OMB reserves the right to change said plan

# New Model

Old



New



# Identity Assurance Levels (IALs)

Refers to the robustness of the identity proofing process and the binding between an authenticator and a specific individual

IAL	Description
1	Self-asserted attribute(s) – 0 to n attributes
2	Remotely identity proofed
3	In-person identity proofed (and a provision for attended remote)

# Authenticator Assurance Levels (AALs)

Describes the robustness of confidence that a given claimant is the same as a subscriber that has previously authenticated

AAL	Description
1	Single-factor authentication
2	Two-factor authentication
3	Two-factor authentication with hardware authenticator

# Federation Assurance Levels (FALs)

Combines aspects of the federation model, assertion protection strength, and assertion presentation used in a given transaction into a single, increasing scale

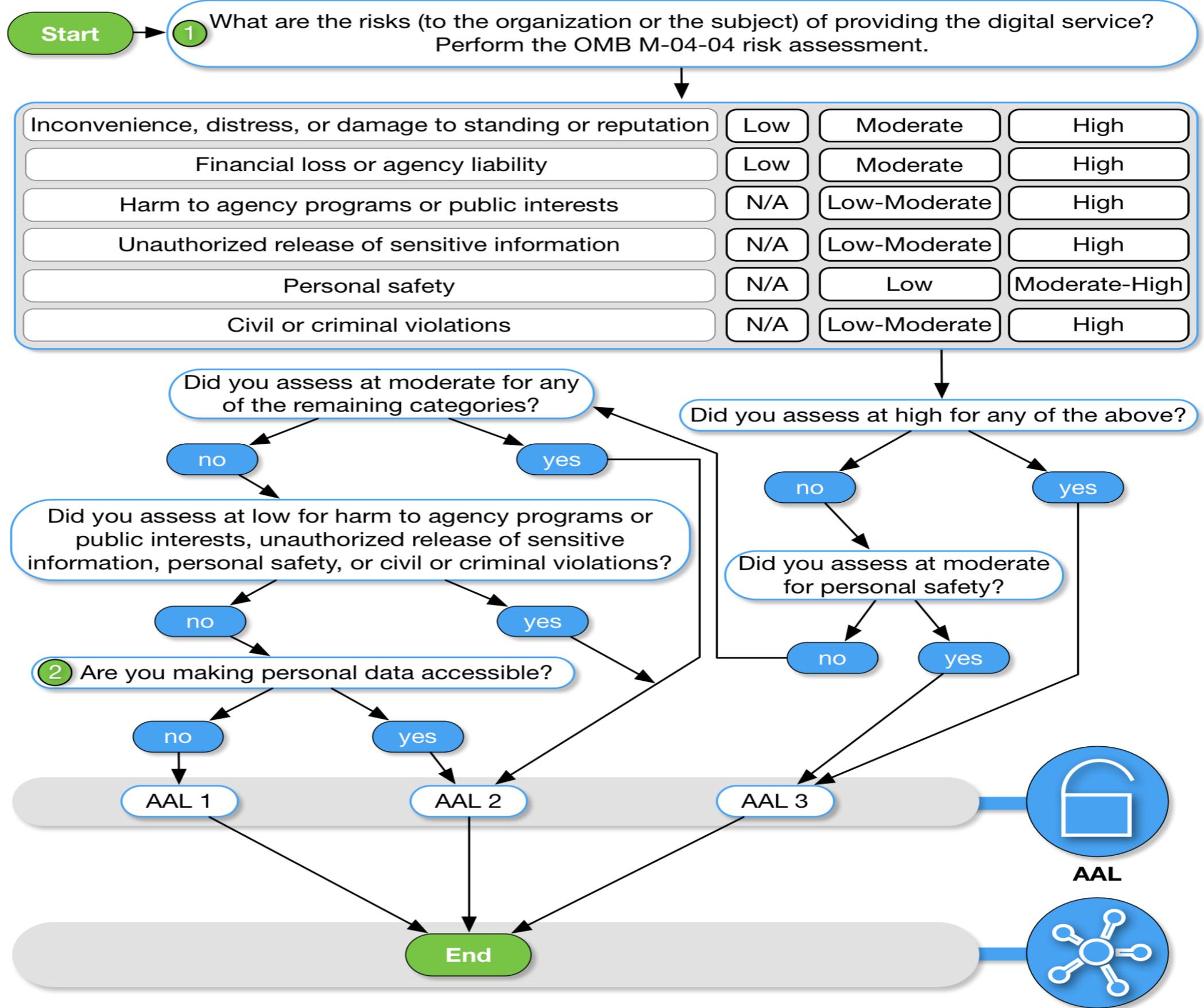
FAL	Presentation Requirement
1	Bearer assertion, signed by IdP
2	Bearer assertion, signed by IdP and encrypted to RP
3	Holder of key assertion, signed by IdP and encrypted to RP

# So go ahead and mix-n-match

	AAL1	AAL2	AAL3
IAL1 without PII	Allowed	Allowed	Allowed
IAL1 with PII	<b>No</b>	Allowed	Allowed
IAL2	<b>No</b>	Allowed	Allowed
IAL3	<b>No</b>	Allowed	Allowed

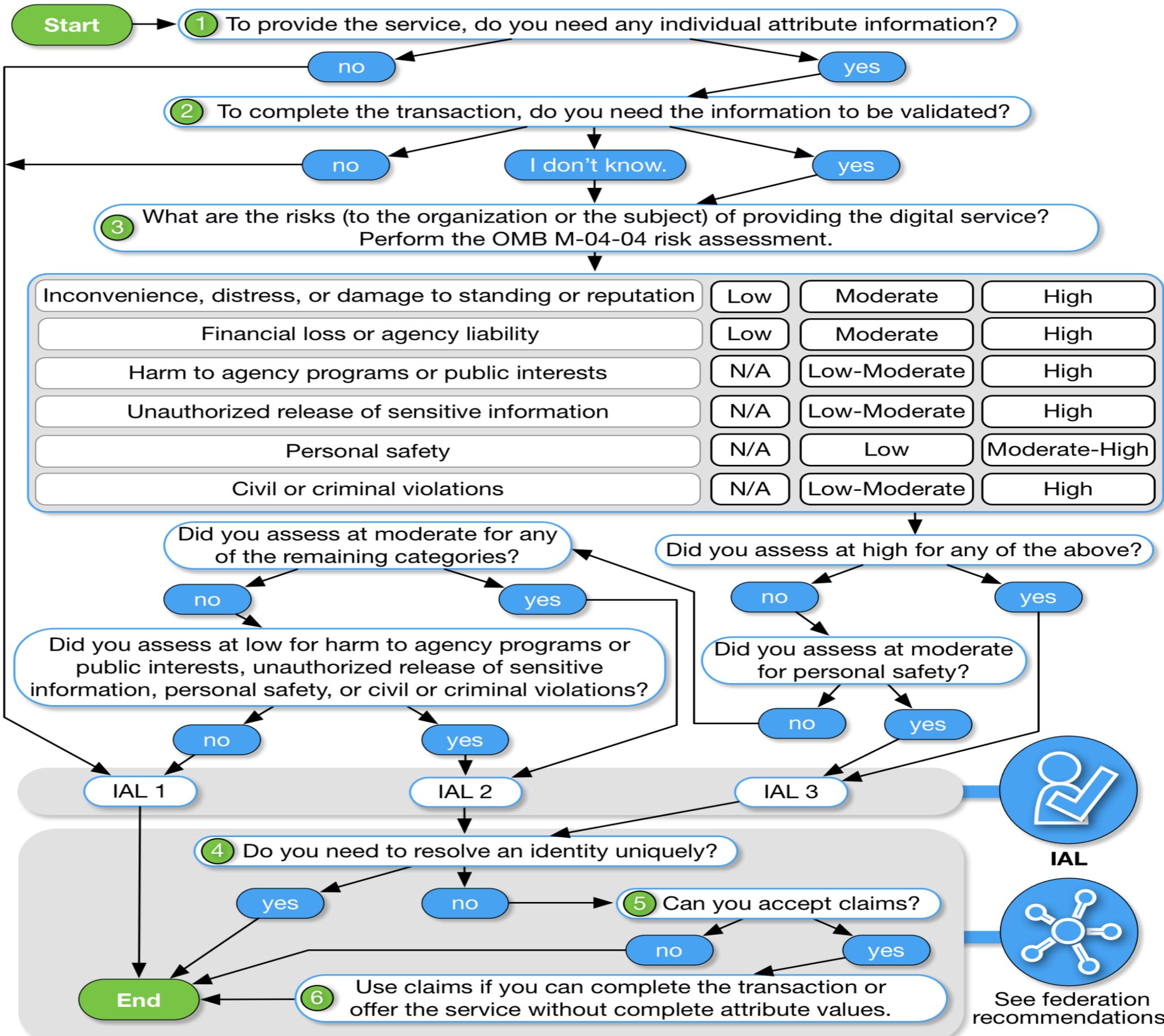
# Choose Your Own AAL

## Discover Your Authenticator Assurance Level (AAL)



# Choose Your Own IAL

## Discover Your Identity Assurance Level (IAL)



# Including step-wise guidance

Figure 5-2 - Selecting IAL

1 To provide the service, do you need any individual attribute information?

The risk assessment and selection of IAL can be short circuited by answering this question first. If the service does not require any personal

Figure 5-1 - Selecting AAL

1 What are the risks (to the organization or the subject) of providing the digital service?  
Perform the OMB M-04-04 risk assessment.

Step 1 asks agencies to look at the potential impacts of an authentication failure. In other words, what would occur if an unauthorized user accessed one or more valid user accounts. Risk should be considered from the perspective of the organization and to a valid user, since one may not be negatively impacted while the other could be significantly harmed. The risk assessment process of M-04-04 and any agency specific risk management process should commence from this step.

2 Are you making personal data accessible?

EO 13681 requires MFA when any personal information is made available online. Since the other paths in this decision tree already drive the agency to an AAL that requires MFA, the question regarding personal information is only raised at this point. That said, personal information release at all AALs should be considered when performing the risk assessment. An important point at this step is that the collection of personal information, if not made available online, does not need to be validated or verified to require an AAL of 2 or higher. Release of even self-asserted personal information requires account protection via MFA. Even though self-asserted information can be falsified, most users will provide accurate information to benefit from the digital service. As such, self-asserted data must be protected appropriately.

required, or if self-asserted to accept attributes that have the digital service with self-

the potential impacts of an identity failure an agency may encounter on. In addition, proofing, when attribute information when not 1 and 2 incorrectly, realizing they the organization and to the user, nt process of M-04-04 and any

unique identity. In other words, access, even with a few process can end. However, the e risk of over collecting and

5 Can you accept claims?

Step 5 focuses on whether the digital service can be provided without having access to full attribute values. This does not mean all attributes must be delivered as claims, but this step does ask the agency to look at each personal attribute they have determined they need, and identify which ones can suffice as claims and which ones need to be complete values. A federated environment is best suited for receiving claims, as the digital service provider is not in control of the attribute information to start with. If the application also performs all required identity proofing, claims may not make sense since full values are already under control of the digital service provider.

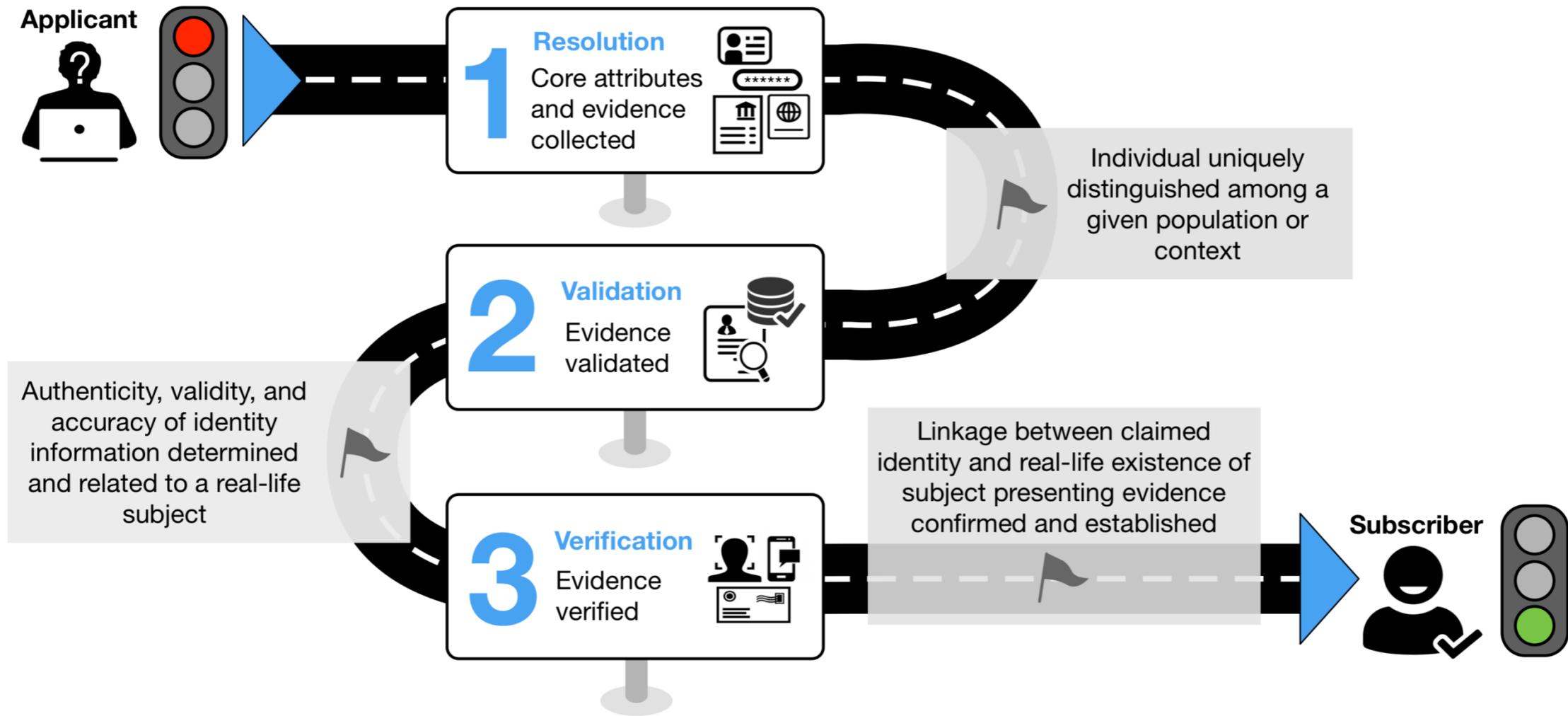
6 Use claims if you can complete the transaction or offer the service without complete attribute values.

If the agency has reached Step 6, claims should be used. This step identifies the digital service as an excellent candidate for accepting federated attribute claims from a CSP (or multiple CSP's), since it has been determined that complete attribute values are not needed to deliver the digital service.

**SP 800-63A**  
Identity  
Proofing &  
Enrollment

---





# The Identity Proofing Process

# What's new with ID Proofing

- Clarifies methods for resolving an ID to a single person
- Establishes strengths for evidence, validation, and verification
  - Unacceptable, Weak, Fair, Strong, Superior
- Moves away from a static list of acceptable documents and increases options for combining evidence to achieve the desired assurance level
- Visual inspection no longer satisfactory at higher IAL
- TFS-related requirements are gone
- Reduced document requirements in some instances
- Clearer rules on address confirmation

## Expanding & Clarifying Identity Proofing Options

- Virtual in-person proofing counts as in-person
- Remote notary proofing
- Remote selfie match
- Trusted referees



- No restrictions in the resolution phase of ID Proofing
- Highly restrictive in verification phase
- Strict and clear rules on the use of KBVs
- Definition of proper/allowable data sources
- Prefers knowledge of recent Tx over static data
- Cannot be standalone

## **Knowledge Based Verification's Role in Identity Proofing**

**SP 800-63B**  
**Authenticati**  
**on &**  
**Lifecycle**  
**Managemen**  
**t**

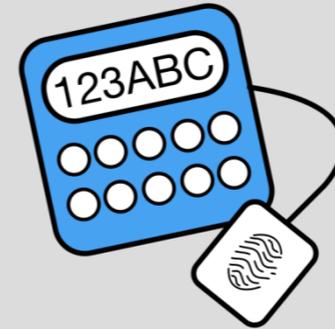
---



# Authenticators



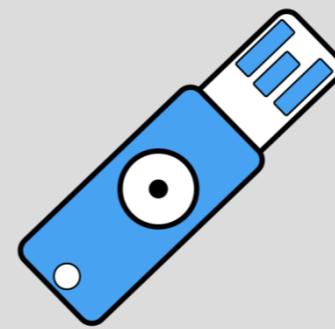
Memorized Secrets



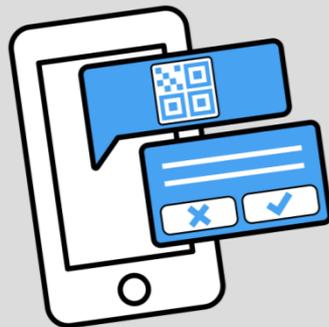
Multi-Factor OTP Devices



Look-up Secrets



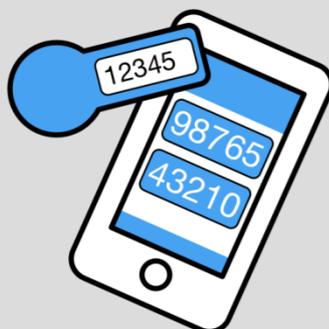
Single Factor Cryptographic Devices



Out-of-Band Devices



Multi-Factor Cryptographic Software



Single Factor OTP Device



Multi-Factor Cryptographic Devices

# Authenticator Guidance Changes

“Token” is out  
“Authenticator” is in



Greater allowance for biometrics, but with rules



SMS OTP Requirements



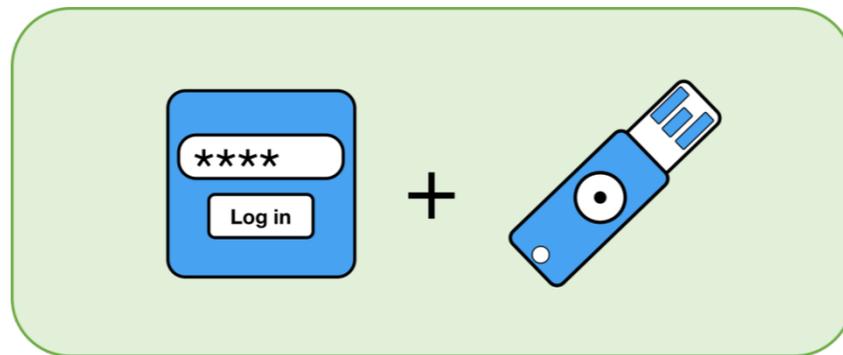
OTP via email is out



Pre-registered knowledge tokens are out



# New authenticators at AAL3 (aka LOA4)



FIPS 140-2

Level 1/Physical Level 3

Level 2/Physical 3

## Why it matters

- M-05-24 Applicability (**Action Item 1.3.2\***)
- Derived PIV Credentials (**Action Item 1.3.2\***)
- Consumers already have these (**Action Item 1.3.1**)
- PIV Interoperability should expand beyond PKI (**Action Item 1.3.2\***)

**\* Action Item 1.3.2: The next Administration should direct that all federal agencies require the use of strong authentication by their employees, contractors, and others using federal systems.**

“The next Administration should provide agencies with updated policies and guidance that continue to focus on increased adoption of strong authentication solutions, including but, importantly, not limited to personal identity verification (PIV) credentials.”

- *Commission on Enhancing National Cybersecurity, Report on Securing and Growing the Digital Economy, December 1, 2016*

# Password Guidance Changes

- Same requirements regardless of AAL
- SHALL be minimum of 8 characters.
- SHOULD (with heavy leaning to SHALL) be:
  - Any allowable unicode character
  - Up to 64 characters or more
  - No composition rules
  - Won't expire
  - Dictionary rules
- SHALL - Storage guidance to deter offline attack (salt, hash, HMAC)

# Reauthentication

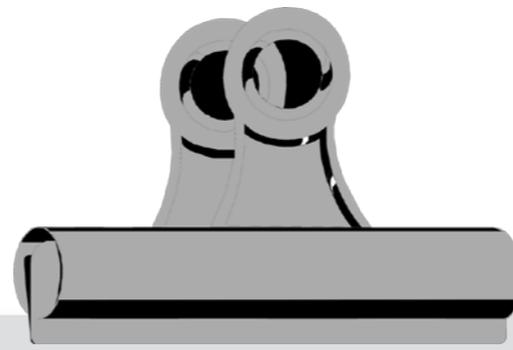
AAL	Description	Timeout
1	Presentation of any one factor	30 days
2	Presentation of any one factor	12 hours or 30 minutes of activity
3	Presentation of all factors	12 hours or 15 minutes of activity



**SP 800-63C**  
**Federation &**  
**Assertions**

---





# 800-63-C

## Federation & Assertions

- 1 Discusses multiple models & privacy impacts & requirements
- 2 Modernized to include OpenID Connect
- 3 Clarifies Holder of Key (HOK) for the new AAL 3
- 4 Attribute requirements

# 800-6 ❤️ federation



Anywhere assertions are used



Intra/inter-agency federated credentials



Commercial federated credentials

(but 800-63-3 remains agnostic to any architecture)

# Attribute Claims vs. Values

## Maturity Model



## Old

Give me date of birth.

Give me full address.

## New

I just need to know if they are older than 18.

I just need to know if they are in congressional district X.

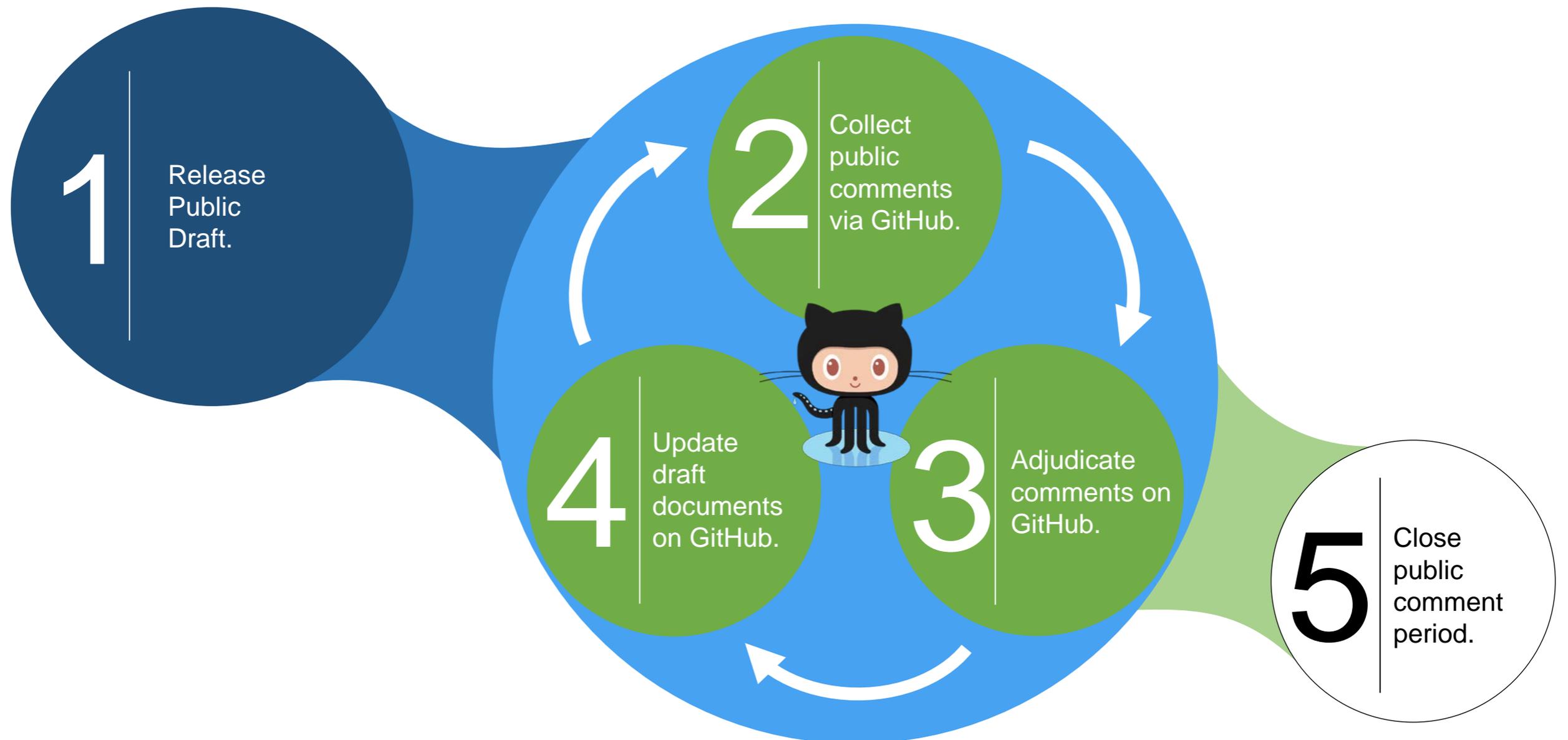
## New Requirements

**CSP** SHALL support claims and value API

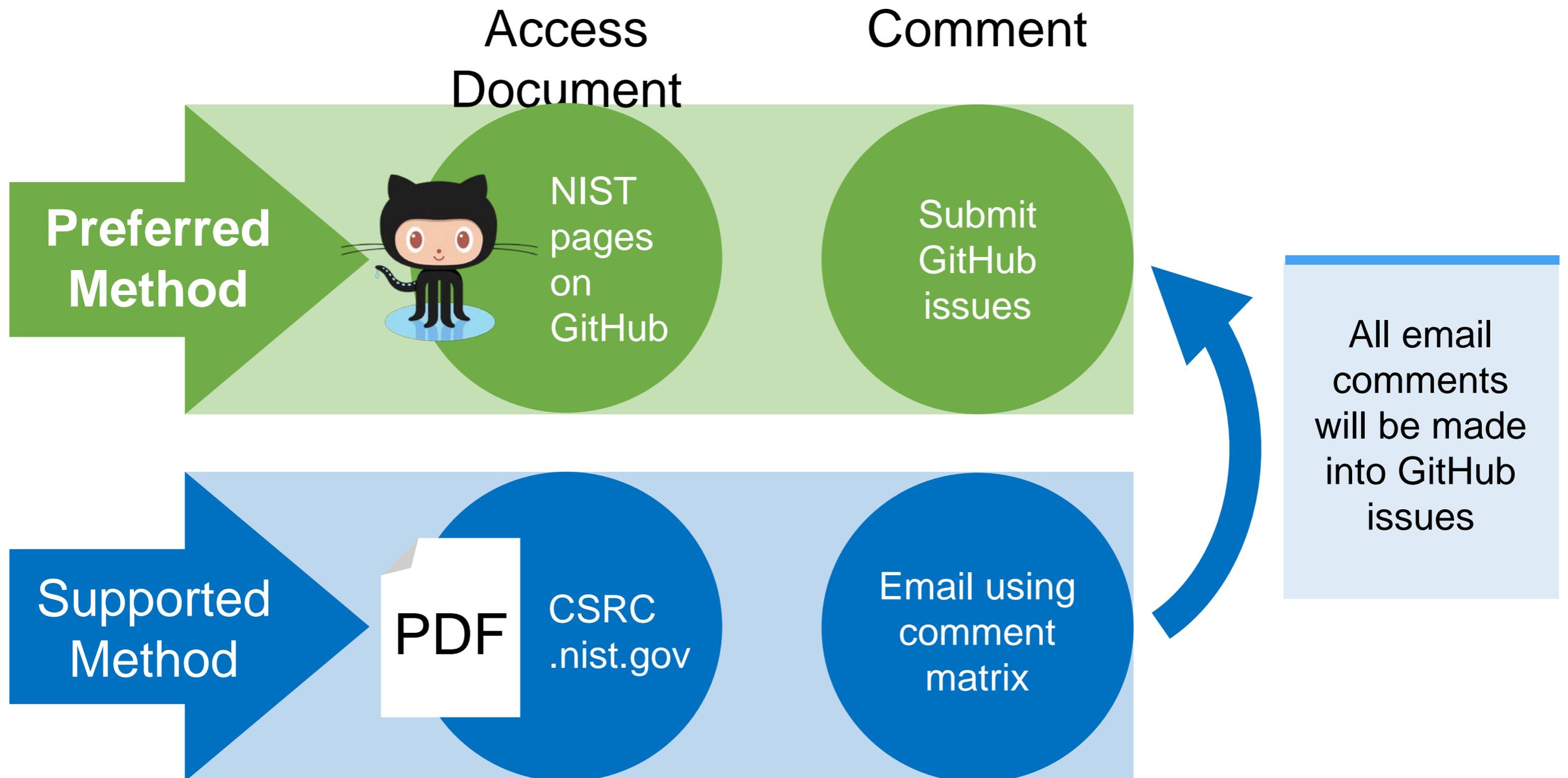
**RP** SHOULD request claims

# Retaining the New Development Approach

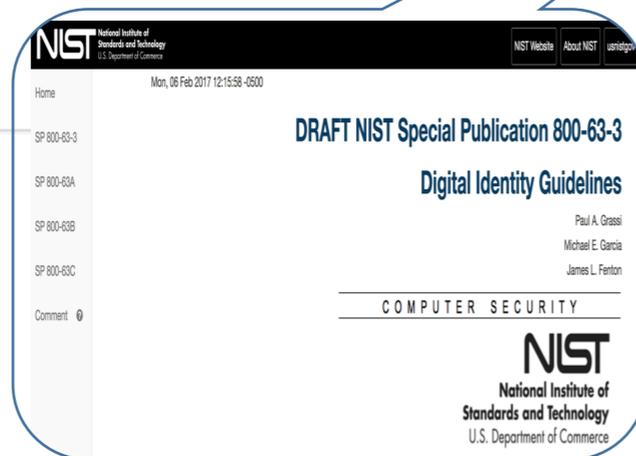
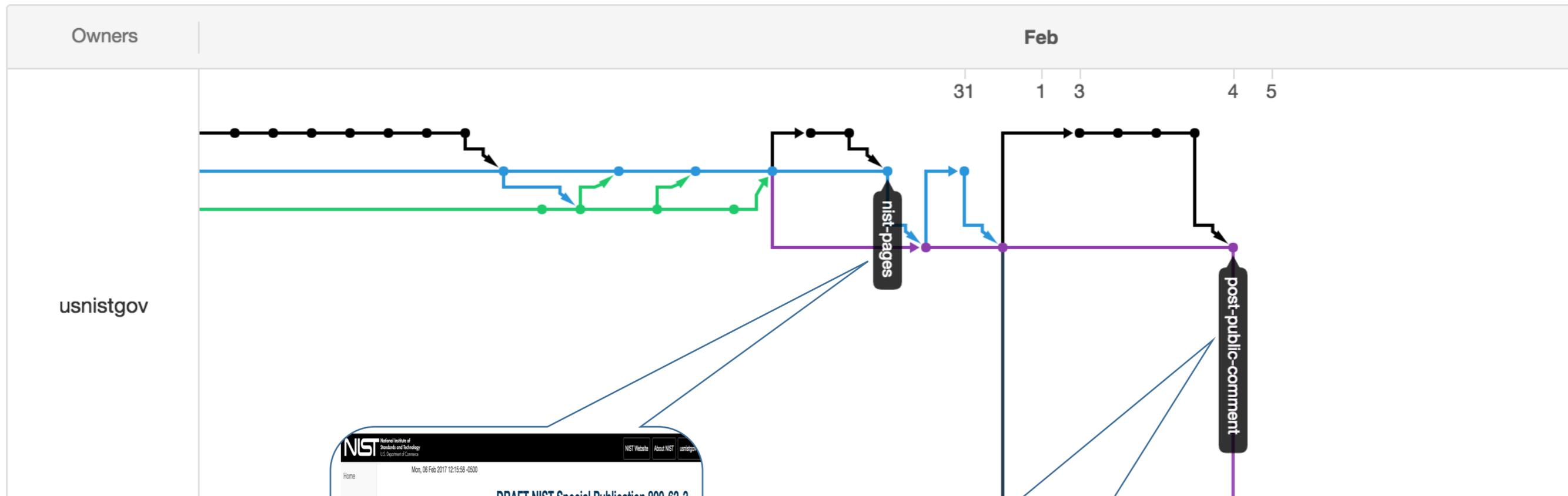
*Iterative – publish, comment, and update in a series of drafting sprints*



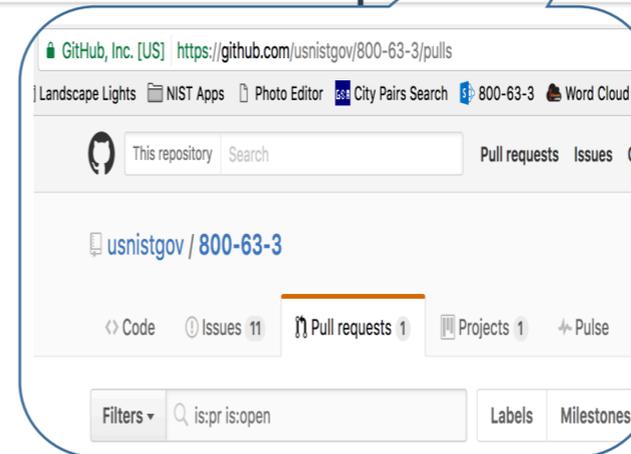
# Contributing During Public Comment



# Advanced Contribution Option



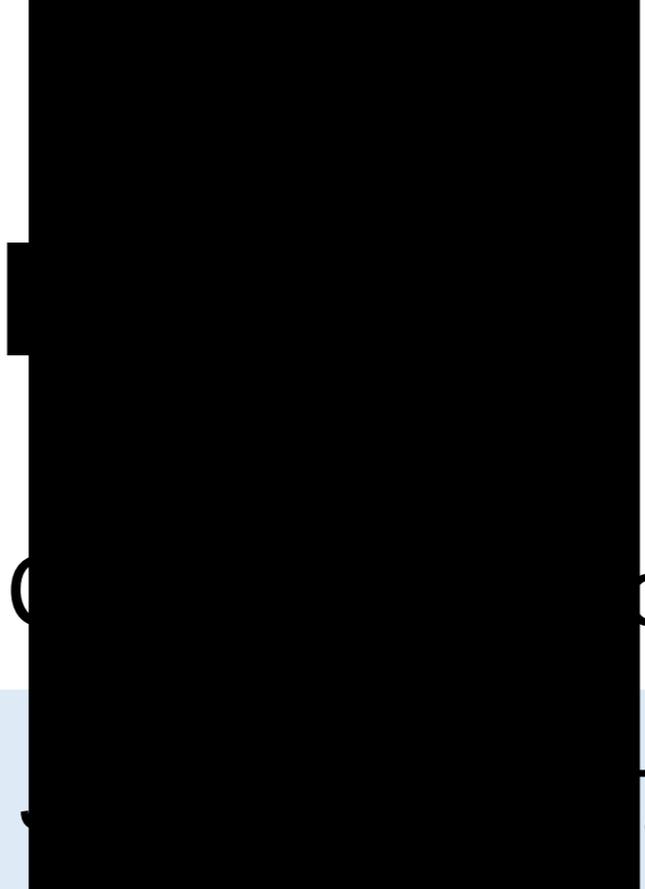
Stable Version



Where to send pull requests

# What's

## Public Draft od

opens  7  
closes **March 31, 2017** **May 1, 2017 (-3 only)**

## Final Document

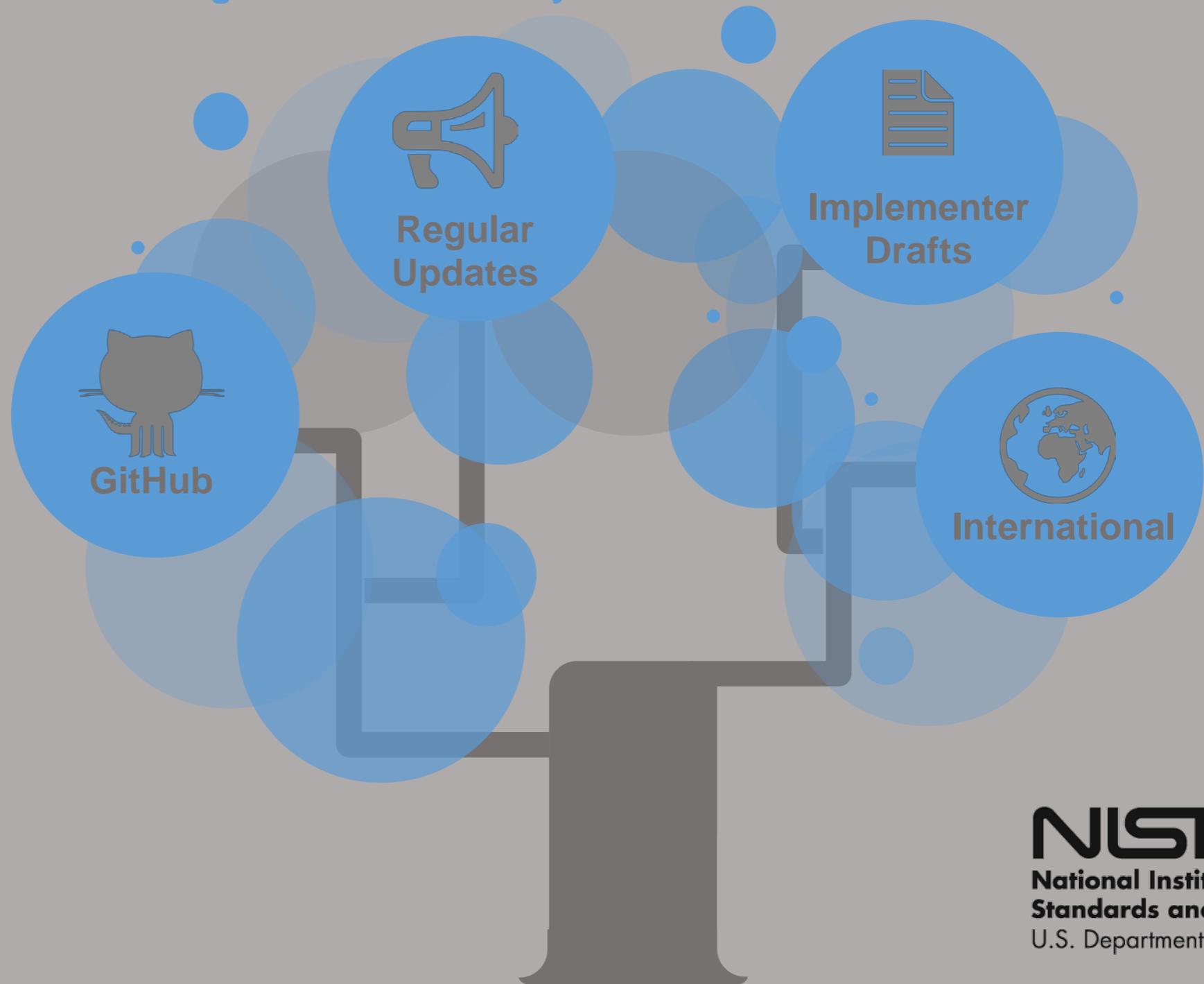
expected **Summer 2017**

## Implementation Guidance

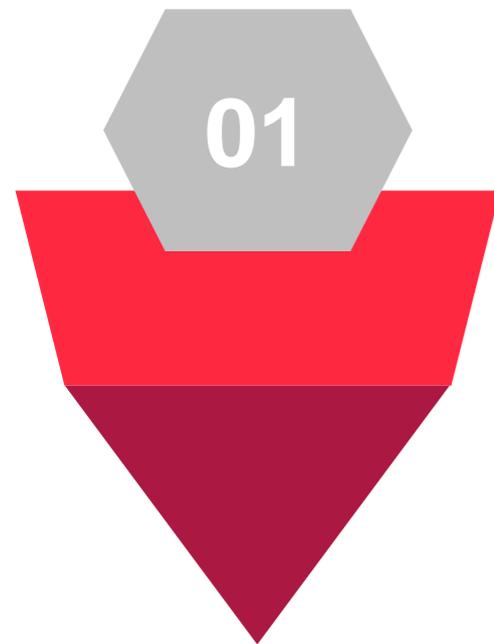
~= Operations Manual/Implementation Guide  
v0.1 focused on proofing

# Fostering Growth

Seeking new ways to engage our stakeholders in order to promote innovation and best practices, while reducing risk and avoiding an ever-constantly moving target.

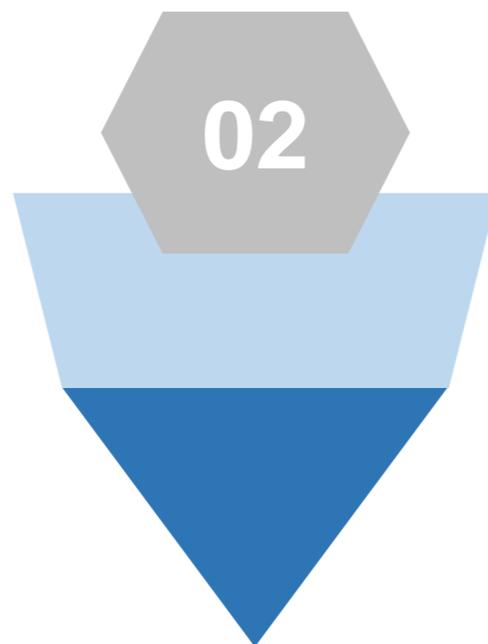


# In Closing



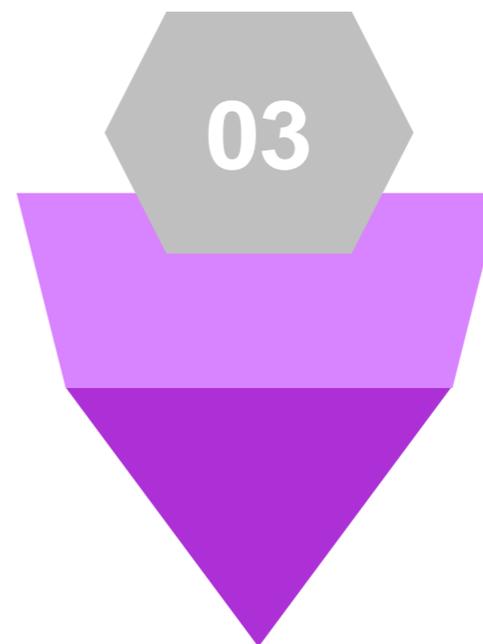
## Major Update

Biggest update since original version.  
Did we get it right?



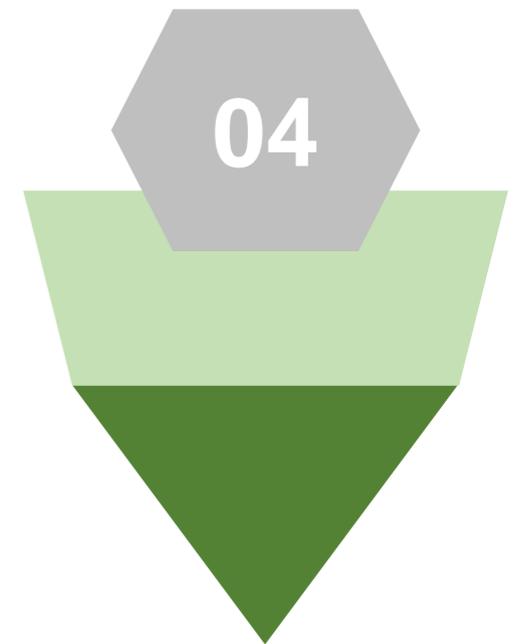
## Innovation

Focused on private sector capabilities.  
Did we future-proof it?



## International

Need 1 less of these than # of countries.  
OK? Use cases?



## Participate

Not our document.  
It's yours.  
Participate!

Backup

---



# Highlights from the Public Preview

May – September 2016

**12,000+**

Views on  
Github

**3,600+**

Unique  
Visitors

**250+**

Comments

**200**

Pull  
Requests

**30**

Contributors

**503**

Commits