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/PubsSPs.html#800-63-3

NIST
National Institute of
Standards and Technology
U.S. Department of Commerce

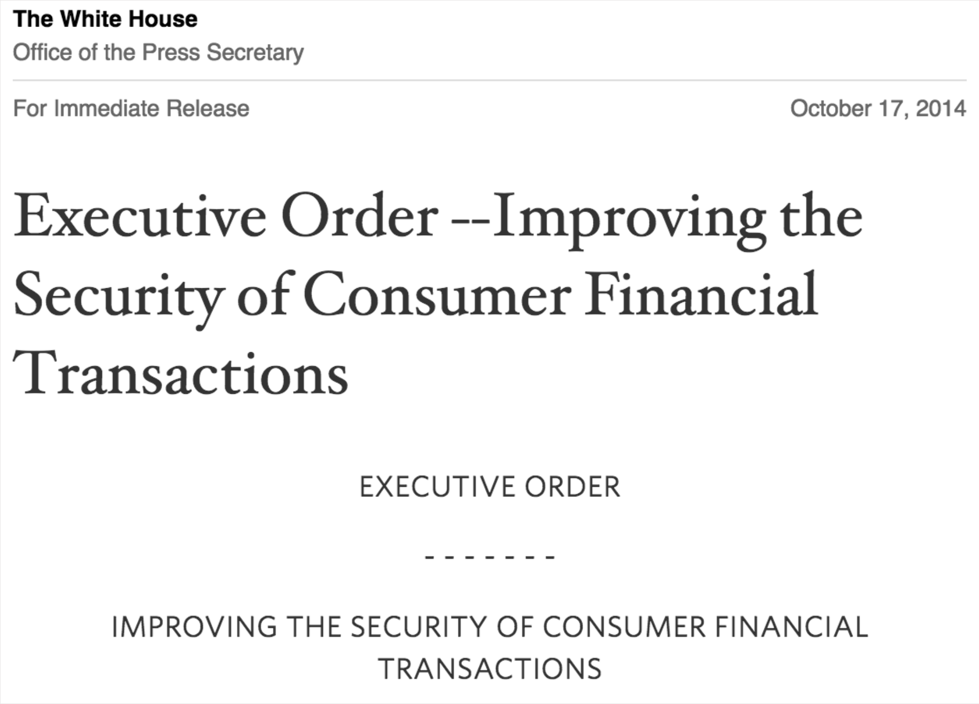
Why the update?

- 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

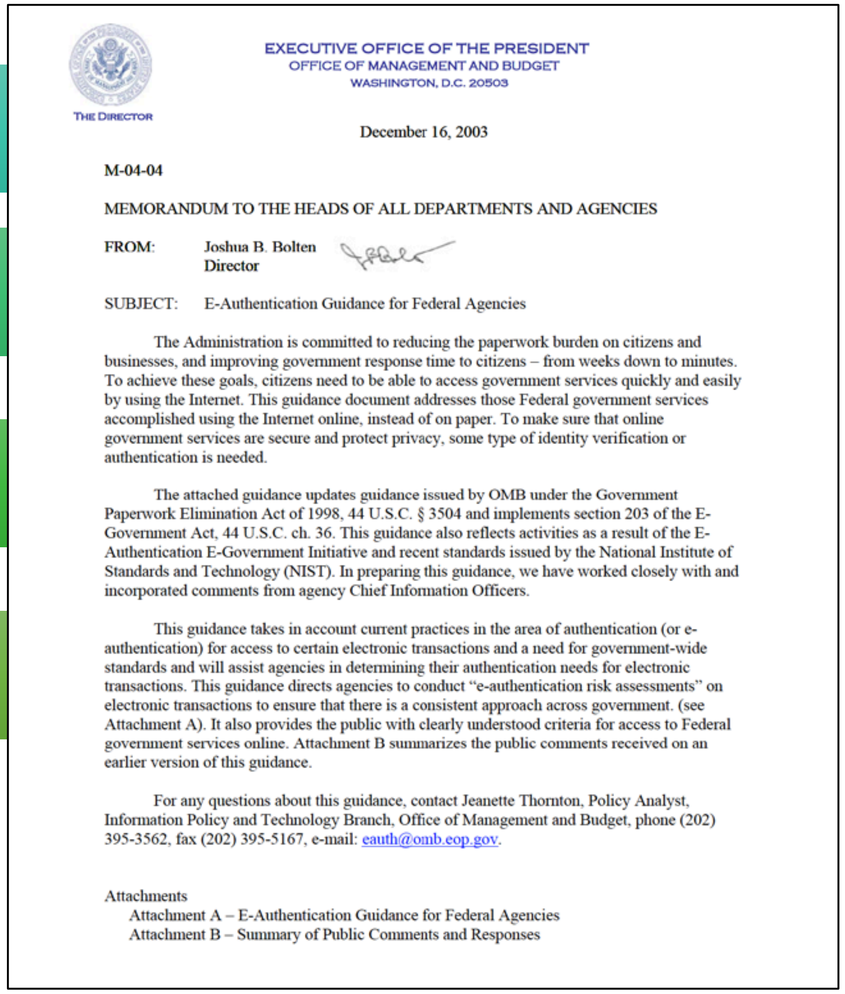
Significant Updates

SP 800-63-3

Digital Identity Guideline

In the beginning…OMB M-04-04

- Issued in 2003
- Established 4 LOAs
- Established Risk Assessment Methodology
- Established Applicability: Externally Facing Systems
- Tasked NIST with 800-63
- FIPS201/PIV Program Uses Same LOA Model



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.

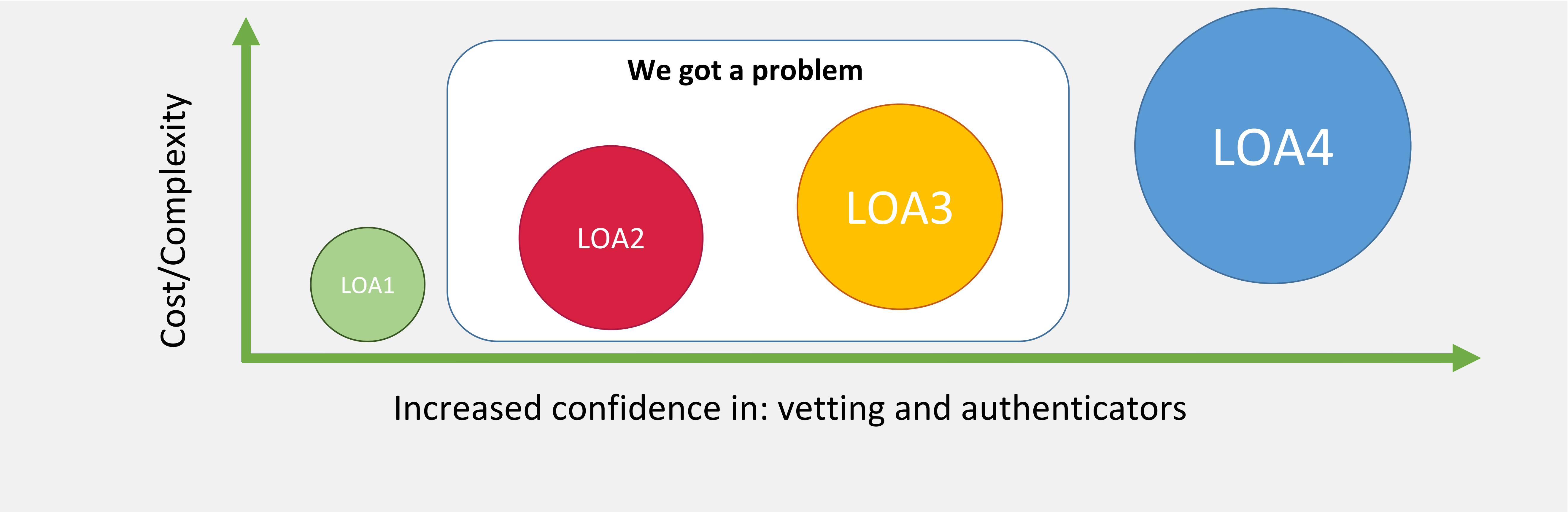
This guidance takes in account current practices in the area of authentication (or e-authentication) for access to certain electronic transactions and a need for government-wide standards and will assist agencies in determining their authentication needs for electronic transactions. This guidance directs 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: eauth@omb.eop.gov.

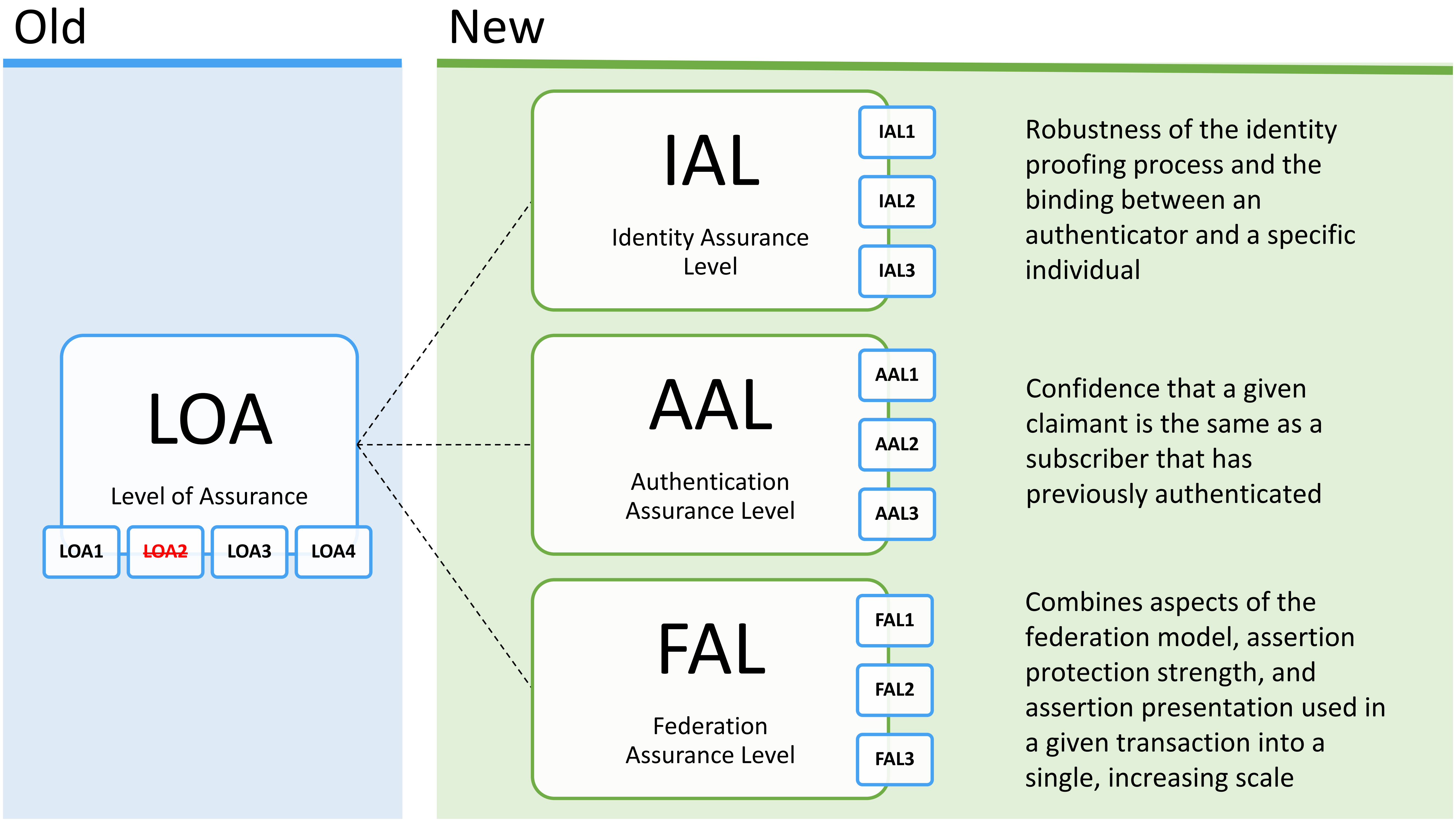
Attachments
Attachment A – E-Authentication Guidance for Federal Agencies
Attachment B – Summary of Public Comments and Responses

What are Levels of Assurance

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



New Model



Old

LOA

Level of Assurance

LOA1

~~LOA2~~

LOA3

LOA4

New

IAL

Identity Assurance Level

IAL1

IAL2

IAL3

Robustness of the identity proofing process and the binding between an authenticator and a specific individual

AAL

Authentication Assurance Level

AAL1

AAL2

AAL3

Confidence that a given claimant is the same as a subscriber that has previously authenticated

FAL

Federation Assurance Level

FAL1

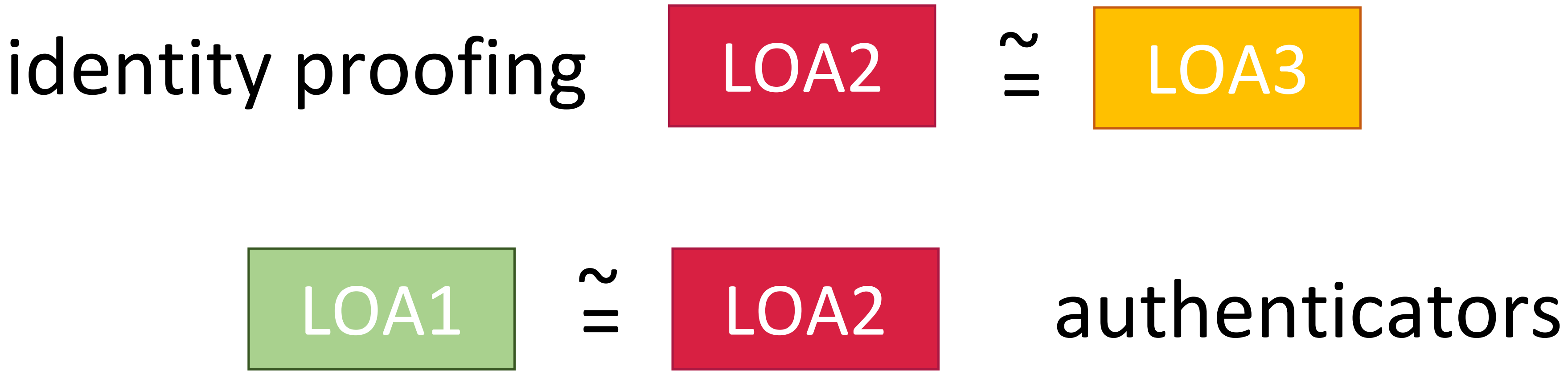
FAL2

FAL3

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

What’s wrong with LOA2?

SP 800-63-2



identity proofing LOA2 $\cong$ LOA3

LOA1 $\cong$ 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

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

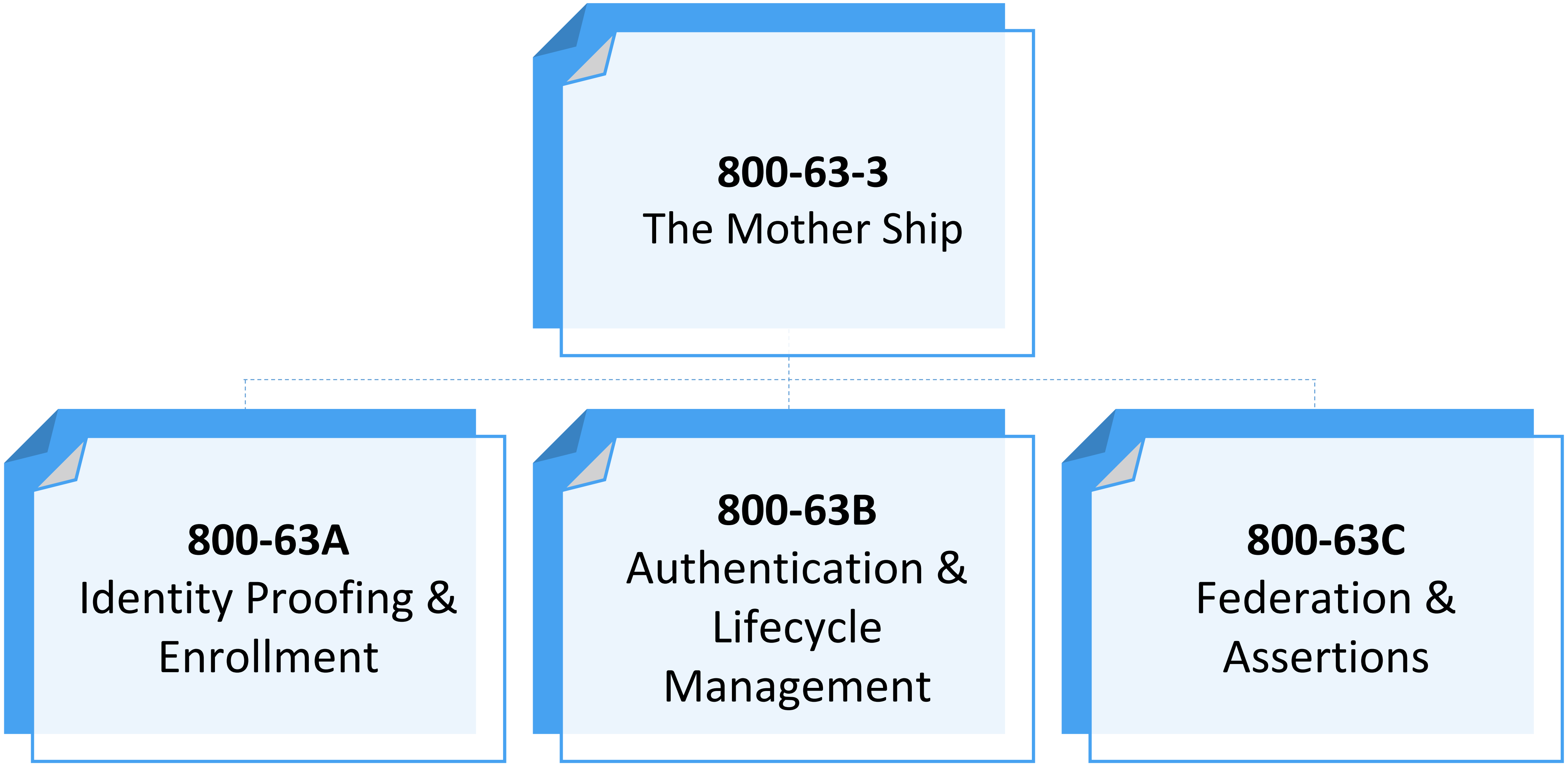
AAL	Description
1	Single-factor authentication
2	Two-factor authentication
3	Two-factor authentication with hardware authenticator

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

Making 800-63 More Accessible



800-63-3
The Mother Ship

800-63A
Identity Proofing & Enrollment

800-63B
Authentication & Lifecycle Management

800-63C
Federation & Assertions

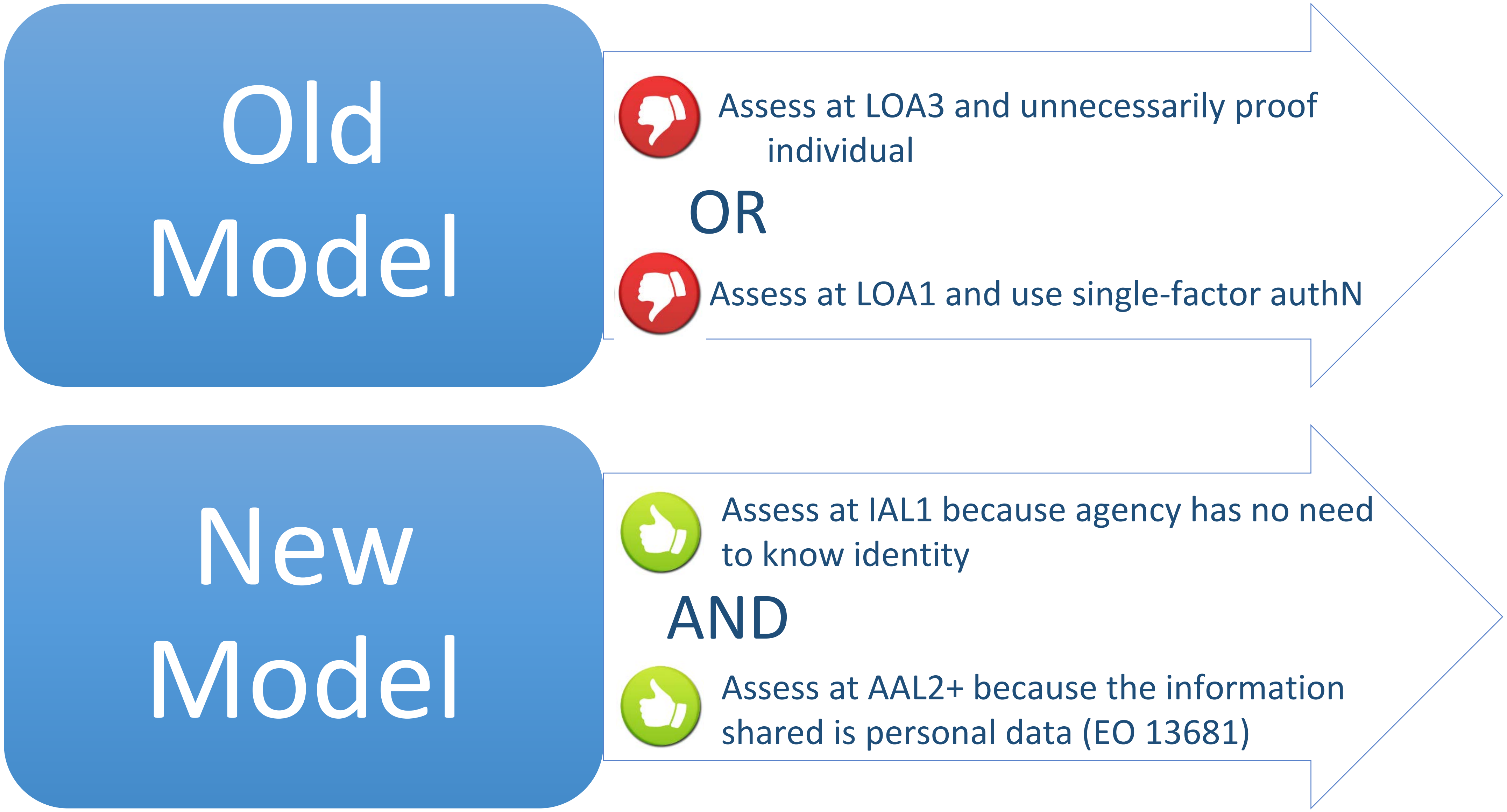
Streamlined Content & Normative Language

Privacy Requirements & Considerations

User Experience Considerations

A future example

Health Tracker Application



Old Model

👎 Assess at LOA3 and unnecessarily proof individual

OR

👎 Assess at LOA1 and use single-factor authN

New Model

👍 Assess at IAL1 because agency has no need to know identity

AND

👍 Assess at AAL2+ because the information shared is personal data (EO 13681)

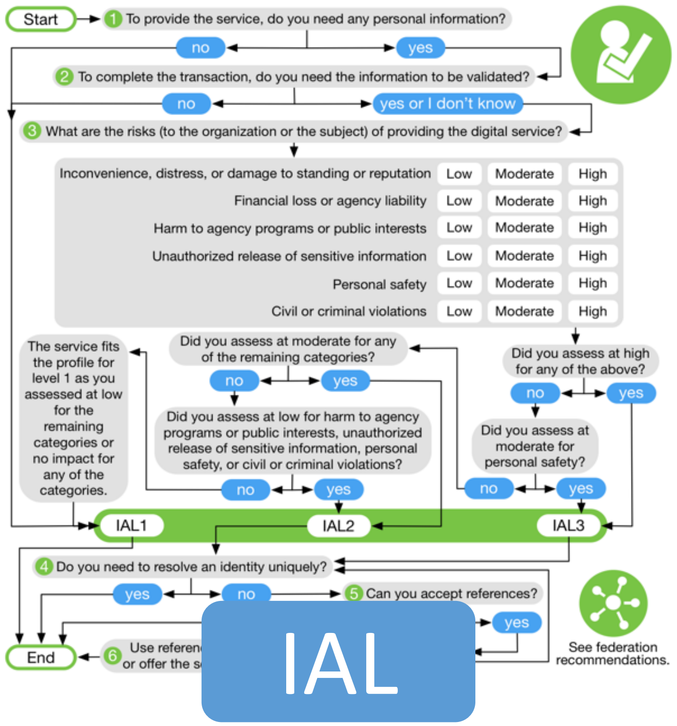
The Plan*

- 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

So go ahead and mix-n-match

	AAL1	AAL2	AAL3
IAL1 without PII	Allowed	Allowed	Allowed
IAL1 with PII	**No**	Allowed	Allowed
IAL2	**No**	Allowed	Allowed
IAL3	**No**	Allowed	Allowed



Start

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

no / yes

2 To complete the transaction, do you need the information to be validated?

no / yes or I don't know

3 What are the risks (to the organization or the subject) of providing the digital service?

Inconvenience, distress, or damage to standing or reputation	Low	Moderate	High
Financial loss or agency liability	Low	Moderate	High
Harm to agency programs or public interests	Low	Moderate	High
Unauthorized release of sensitive information	Low	Moderate	High
Personal safety	Low	Moderate	High
Civil or criminal violations	Low	Moderate	High

The service fits the profile for level 1 as you assessed at low for the remaining categories or no impact for any of the categories.

Did you assess at moderate for any of the remaining categories?

no / yes

Did you assess at low for harm to agency programs or public interests, unauthorized release of sensitive information, personal safety, or civil or criminal violations?

no / yes

Did you assess at high for any of the above?

no / yes

Did you assess at moderate for personal safety?

no / yes

IAL1 IAL2 IAL3

4 Do you need to resolve an identity uniquely?

yes / no

5 Can you accept references?

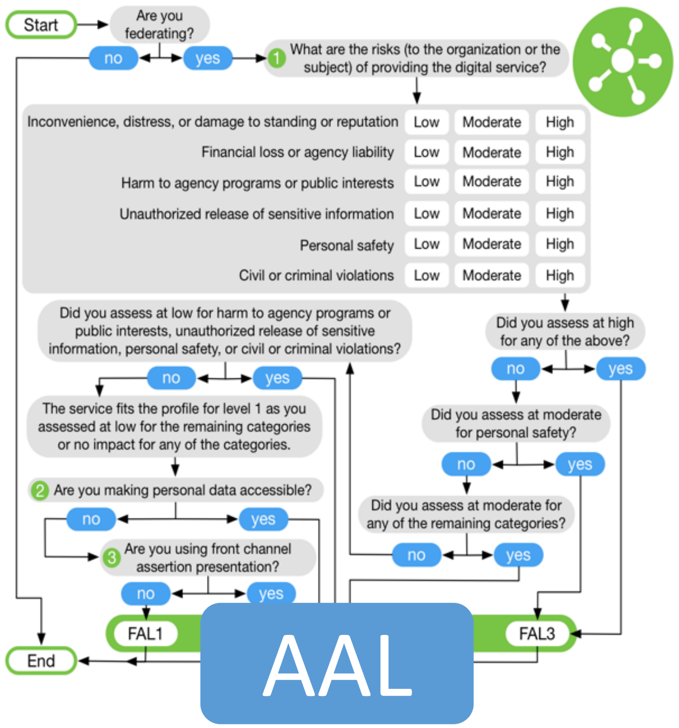
yes

End

6 Use referen
or offer the s

See federation recommendations.

IAL



Start

Are you federating?

no / yes

1 What are the risks (to the organization or the subject) of providing the digital service?

Inconvenience, distress, or damage to standing or reputation	Low	Moderate	High
Financial loss or agency liability	Low	Moderate	High
Harm to agency programs or public interests	Low	Moderate	High
Unauthorized release of sensitive information	Low	Moderate	High
Personal safety	Low	Moderate	High
Civil or criminal violations	Low	Moderate	High

Did you assess at low for harm to agency programs or public interests, unauthorized release of sensitive information, personal safety, or civil or criminal violations?

no / yes

The service fits the profile for level 1 as you assessed at low for the remaining categories or no impact for any of the categories.

2 Are you making personal data accessible?

no / yes

3 Are you using front channel assertion presentation?

no / yes

Did you assess at high for any of the above?

no / yes

Did you assess at moderate for personal safety?

no / yes

Did you assess at moderate for any of the remaining categories?

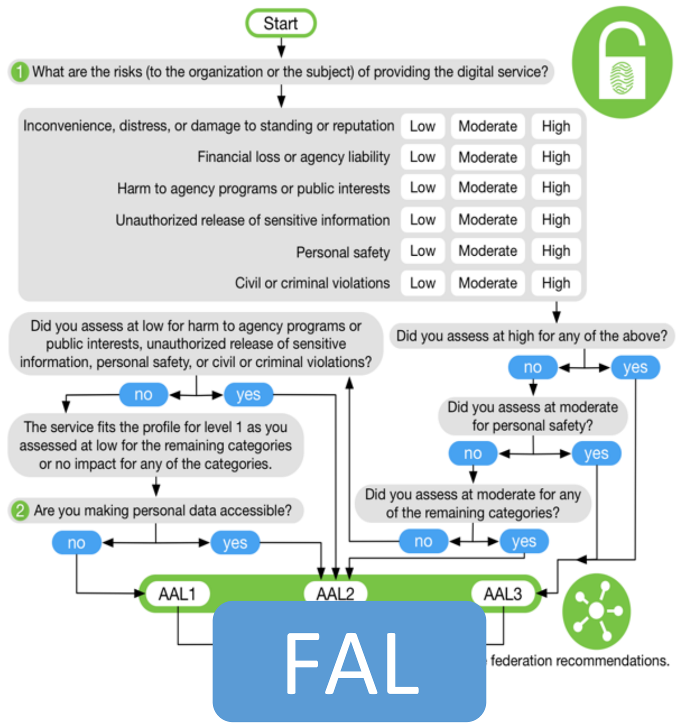
no / yes

FAL1 FAL3

End

AAL

optional



Start

1 What are the risks (to the organization or the subject) of providing the digital service?

Inconvenience, distress, or damage to standing or reputation	Low	Moderate	High
Financial loss or agency liability	Low	Moderate	High
Harm to agency programs or public interests	Low	Moderate	High
Unauthorized release of sensitive information	Low	Moderate	High
Personal safety	Low	Moderate	High
Civil or criminal violations	Low	Moderate	High

Did you assess at low for harm to agency programs or public interests, unauthorized release of sensitive information, personal safety, or civil or criminal violations?

no / yes

The service fits the profile for level 1 as you assessed at low for the remaining categories or no impact for any of the categories.

2 Are you making personal data accessible?

no / yes

Did you assess at high for any of the above?

no / yes

Did you assess at moderate for personal safety?

no / yes

Did you assess at moderate for any of the remaining categories?

no / yes

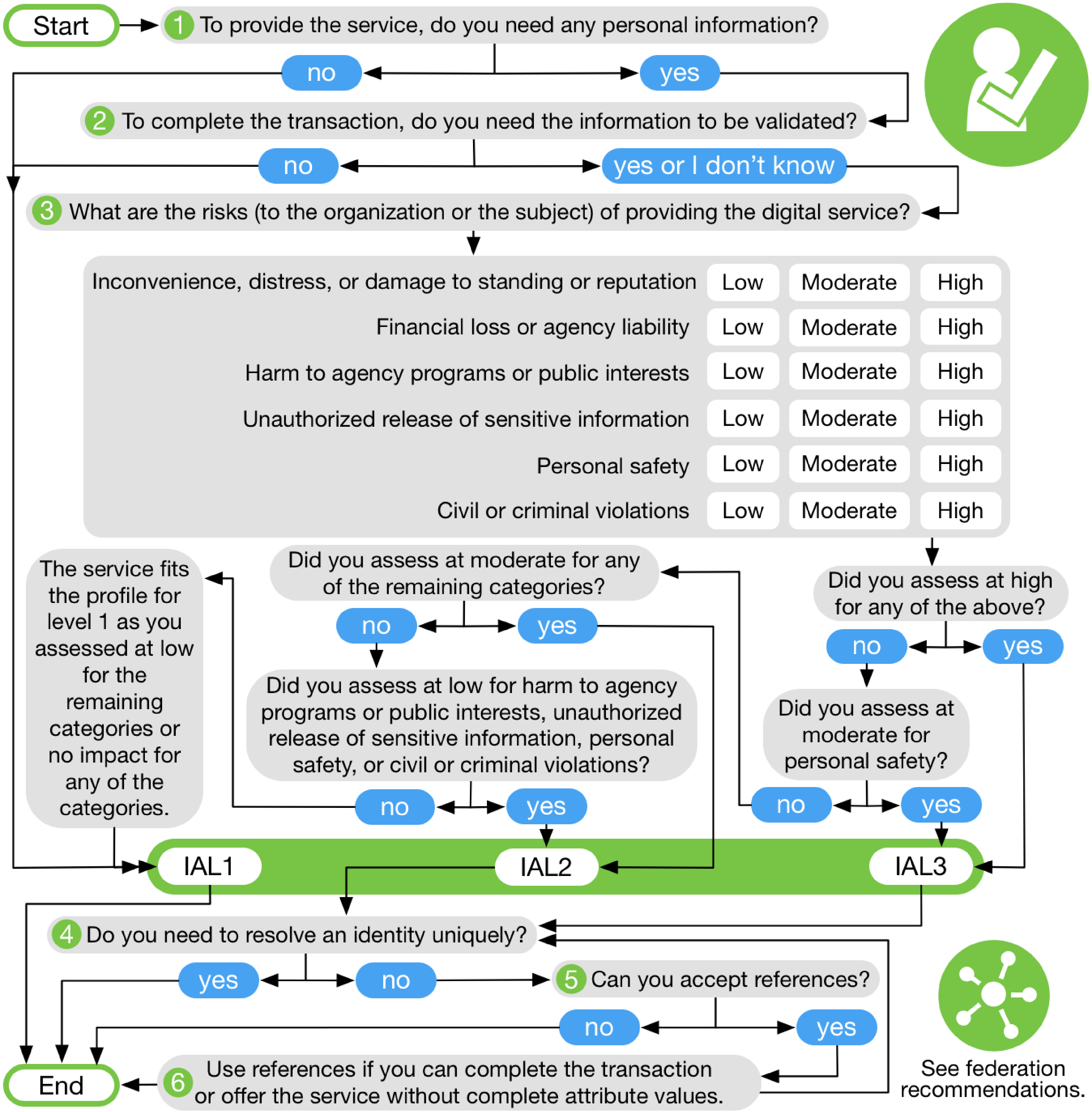
AAL1 AAL2 AAL3

federation recommendations.

FAL

Guidance is risk-based…with some ‘traps’

Choose Your Own IAL



Start

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

no / yes

2 To complete the transaction, do you need the information to be validated?

no / yes or I don't know

3 What are the risks (to the organization or the subject) of providing the digital service?

Inconvenience, distress, or damage to standing or reputation	Low	Moderate	High
Financial loss or agency liability	Low	Moderate	High
Harm to agency programs or public interests	Low	Moderate	High
Unauthorized release of sensitive information	Low	Moderate	High
Personal safety	Low	Moderate	High
Civil or criminal violations	Low	Moderate	High

Did you assess at high for any of the above?

no / yes

Did you assess at moderate for personal safety?

no / yes

Did you assess at moderate for any of the remaining categories?

no / yes

Did you assess at low for harm to agency programs or public interests, unauthorized release of sensitive information, personal safety, or civil or criminal violations?

no / yes

The service fits the profile for level 1 as you assessed at low for the remaining categories or no impact for any of the categories.

IAL1 IAL2 IAL3

4 Do you need to resolve an identity uniquely?

yes / no

5 Can you accept references?

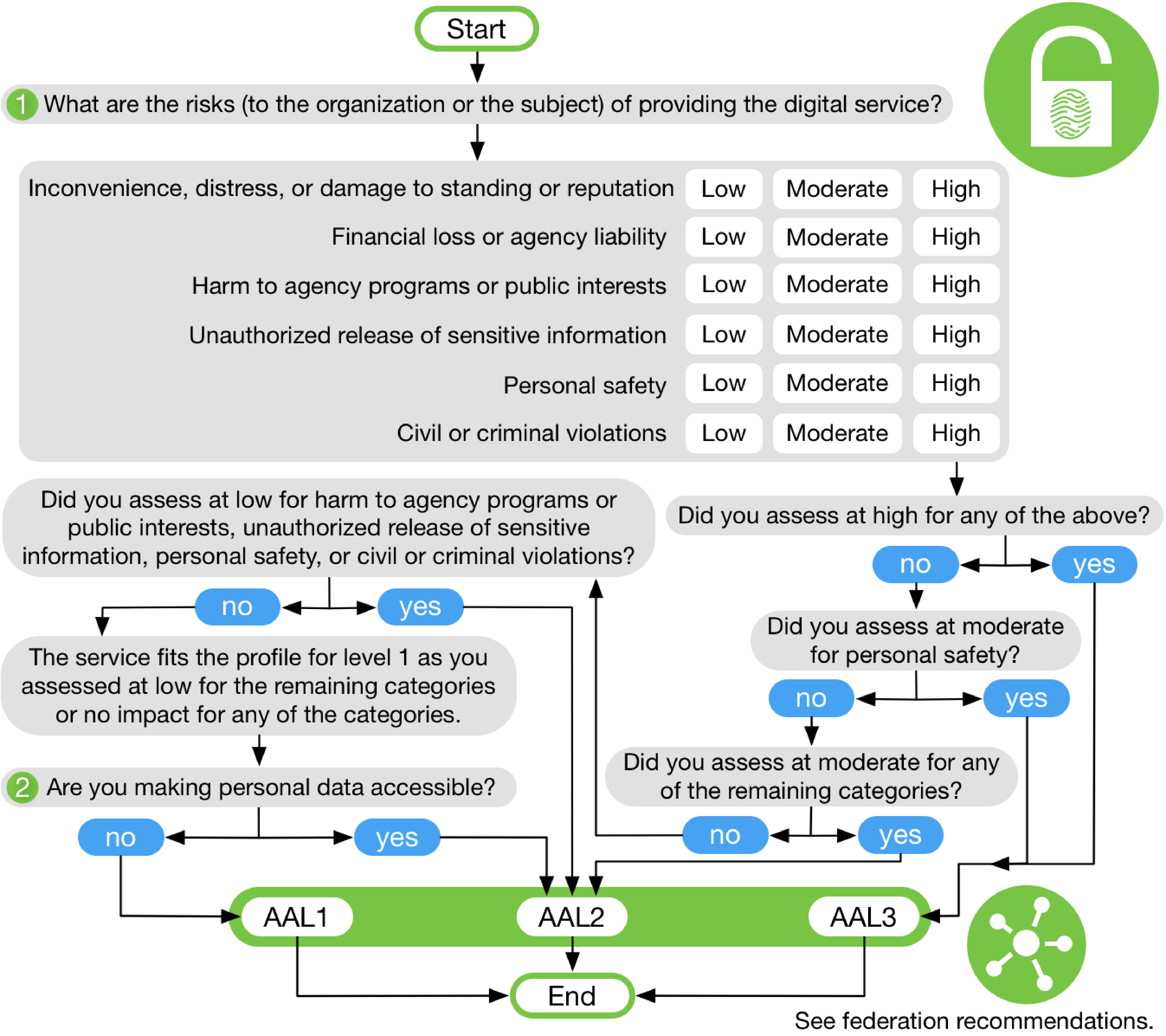
no / yes

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

End

See federation recommendations.

Choose Your Own AAL



Start

1 What are the risks (to the organization or the subject) of providing the digital service?

Inconvenience, distress, or damage to standing or reputation	Low	Moderate	High
Financial loss or agency liability	Low	Moderate	High
Harm to agency programs or public interests	Low	Moderate	High
Unauthorized release of sensitive information	Low	Moderate	High
Personal safety	Low	Moderate	High
Civil or criminal violations	Low	Moderate	High

Did you assess at high for any of the above?

Did you assess at moderate for personal safety?

Did you assess at moderate for any of the remaining categories?

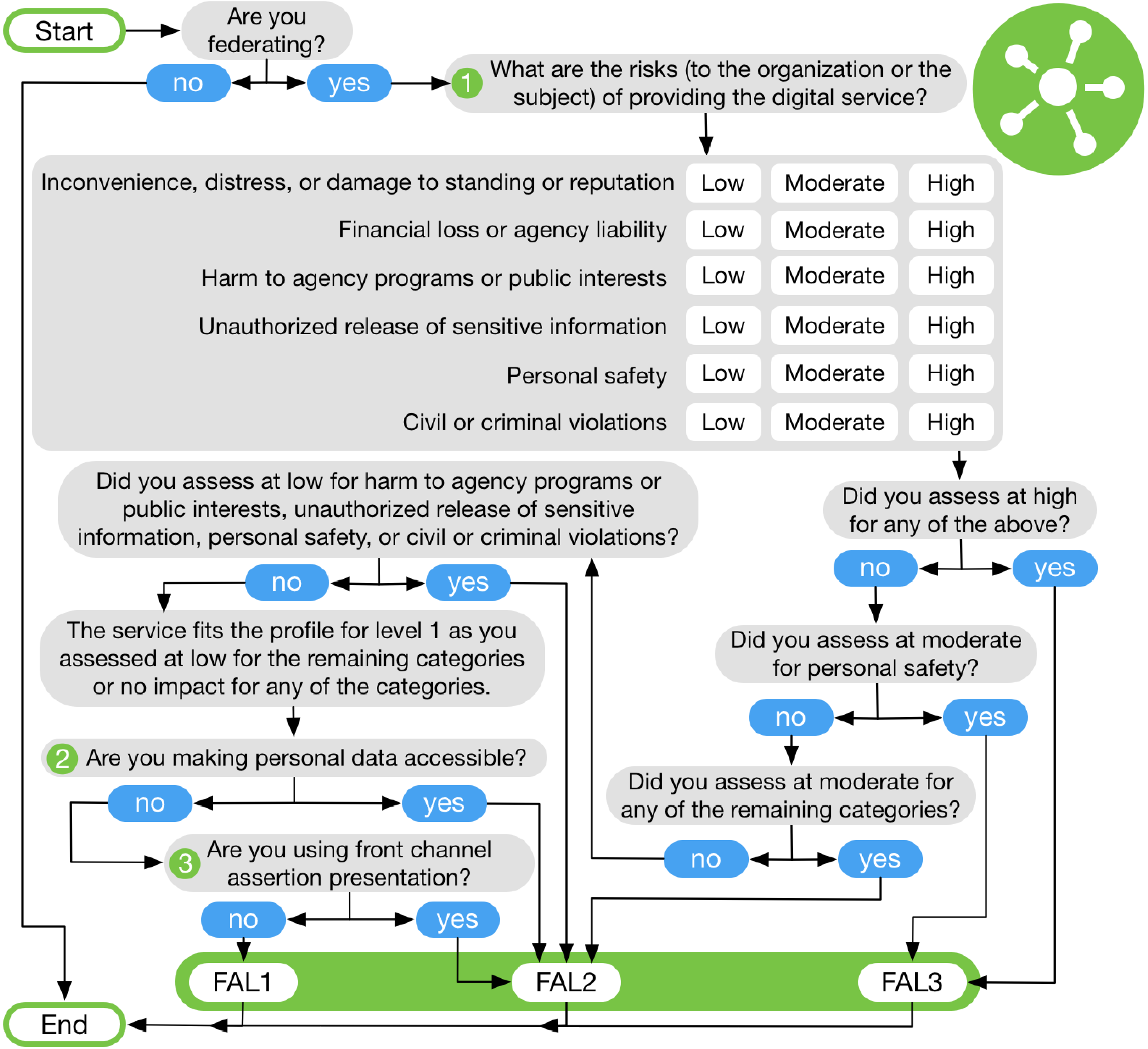
Did you assess at low for harm to agency programs or public interests, unauthorized release of sensitive information, personal safety, or civil or criminal violations?

The service fits the profile for level 1 as you assessed at low for the remaining categories or no impact for any of the categories.

2 Are you making personal data accessible?

See federation recommendations.

Choose Your Own FAL



Start

Are you federating?

no

yes

1 What are the risks (to the organization or the subject) of providing the digital service?

Inconvenience, distress, or damage to standing or reputation	Low	Moderate	High
Financial loss or agency liability	Low	Moderate	High
Harm to agency programs or public interests	Low	Moderate	High
Unauthorized release of sensitive information	Low	Moderate	High
Personal safety	Low	Moderate	High
Civil or criminal violations	Low	Moderate	High

Did you assess at high for any of the above?

no

yes

Did you assess at moderate for personal safety?

no

yes

Did you assess at moderate for any of the remaining categories?

no

yes

Did you assess at low for harm to agency programs or public interests, unauthorized release of sensitive information, personal safety, or civil or criminal violations?

no

yes

The service fits the profile for level 1 as you assessed at low for the remaining categories or no impact for any of the categories.

2 Are you making personal data accessible?

no

yes

3 Are you using front channel assertion presentation?

no

yes

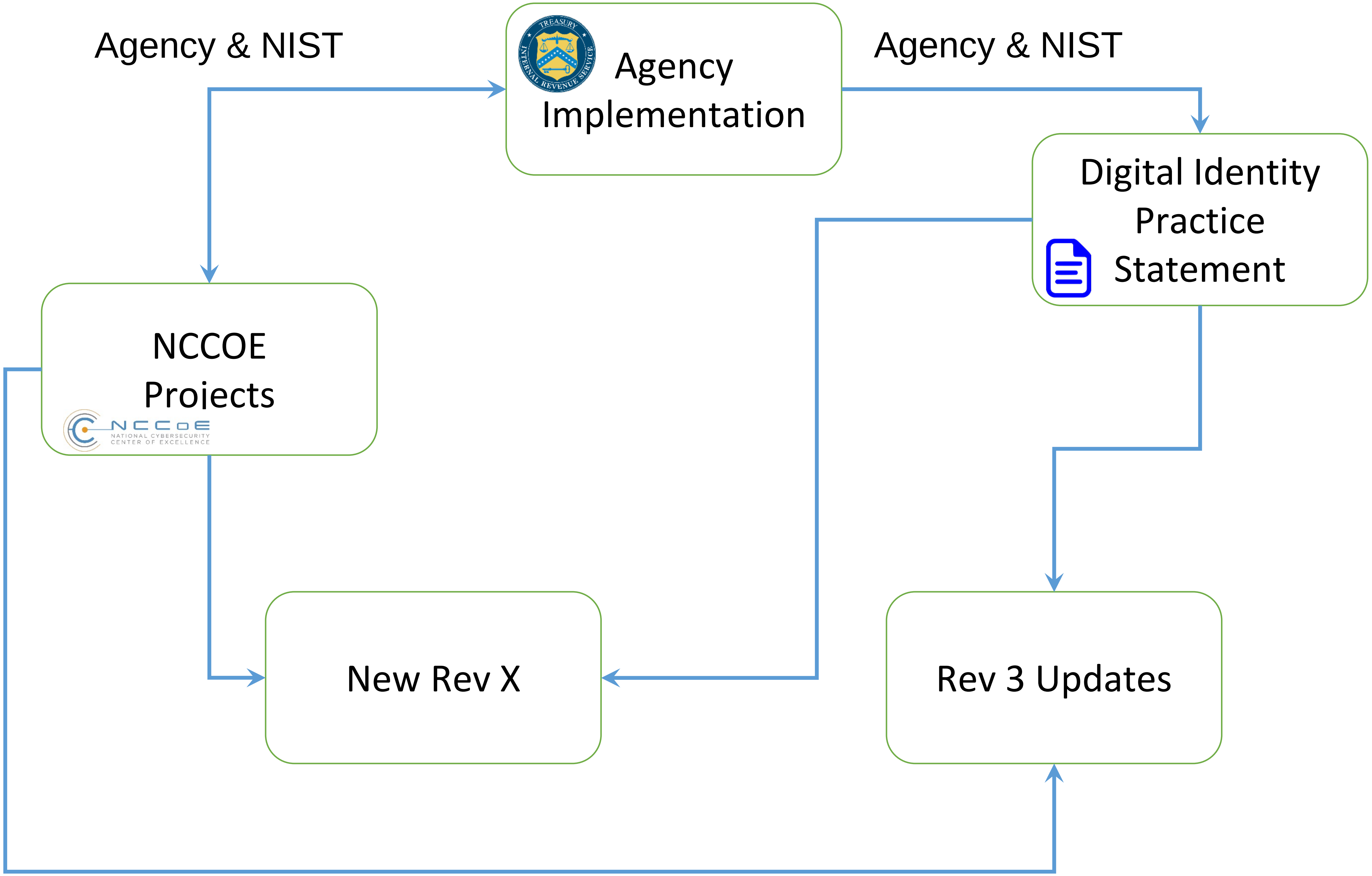
FAL1

FAL2

FAL3

End

Risk Based Feedback Loop



Including step-wise guidance

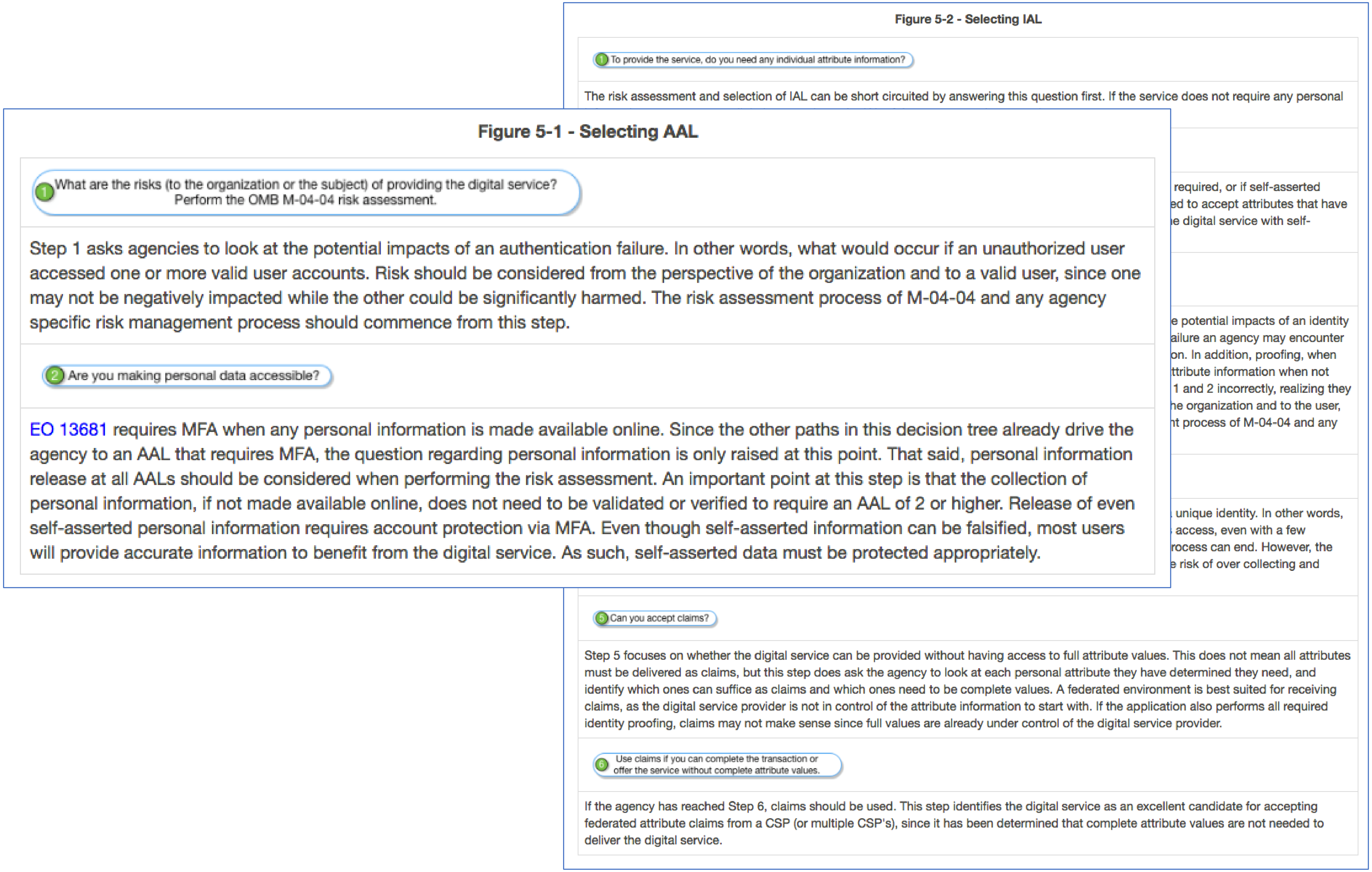


Figure 5-1 - Selecting AAL

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.

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

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

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

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

5 Can you accept claims?

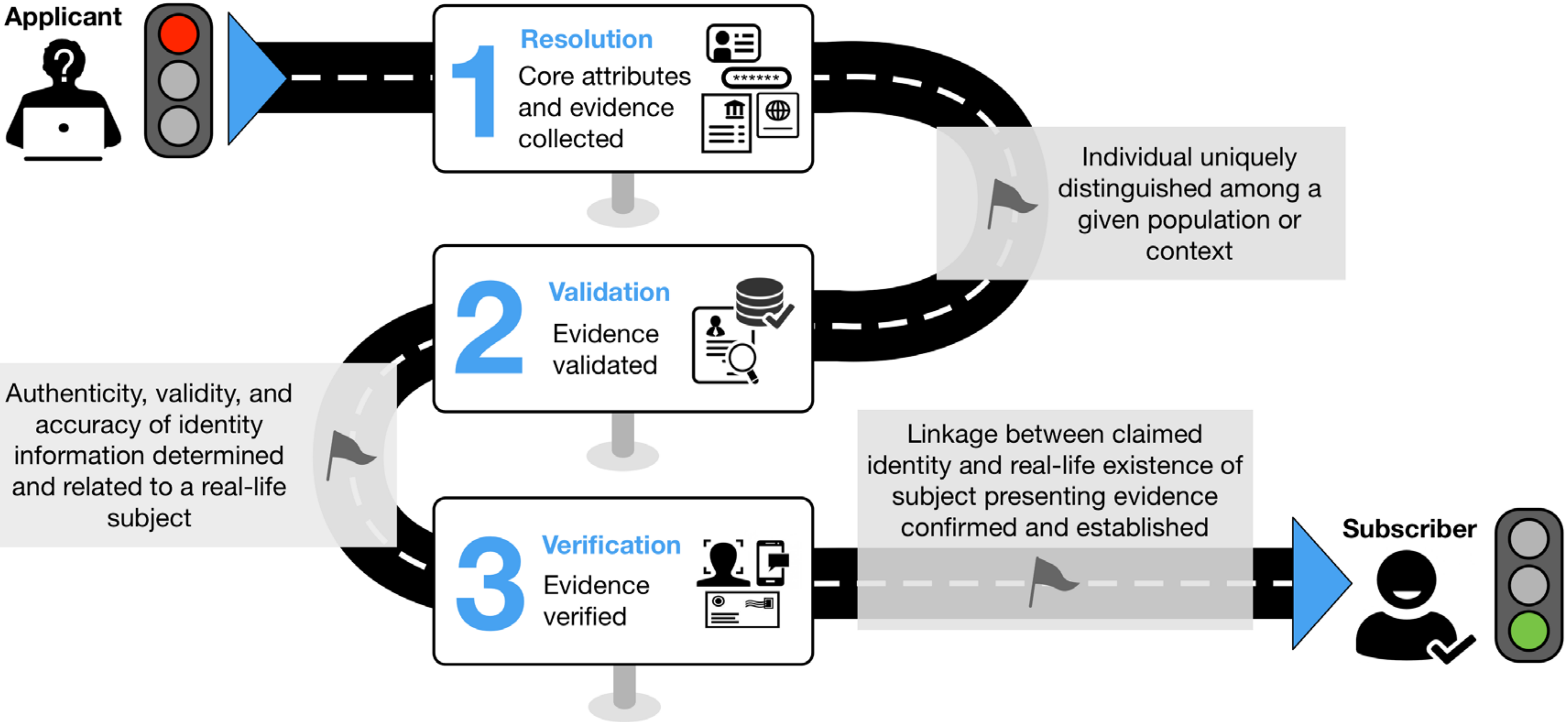
Step 5 focuses on whether the digital service can be provided without having access to full attribute values. This does not mean all attributes must be delivered as claims, but this step does ask the agency to look at each personal attribute they have determined they need, and identify which ones can 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



Applicant
1
Resolution
Core attributes and evidence collected
******
Individual uniquely distinguished among a given population or context
2
Validation
Evidence validated
Authenticity, validity, and accuracy of identity information determined and related to a real-life subject
3
Verification
Evidence verified
Linkage between claimed identity and real-life existence of subject presenting evidence confirmed and established
Subscriber

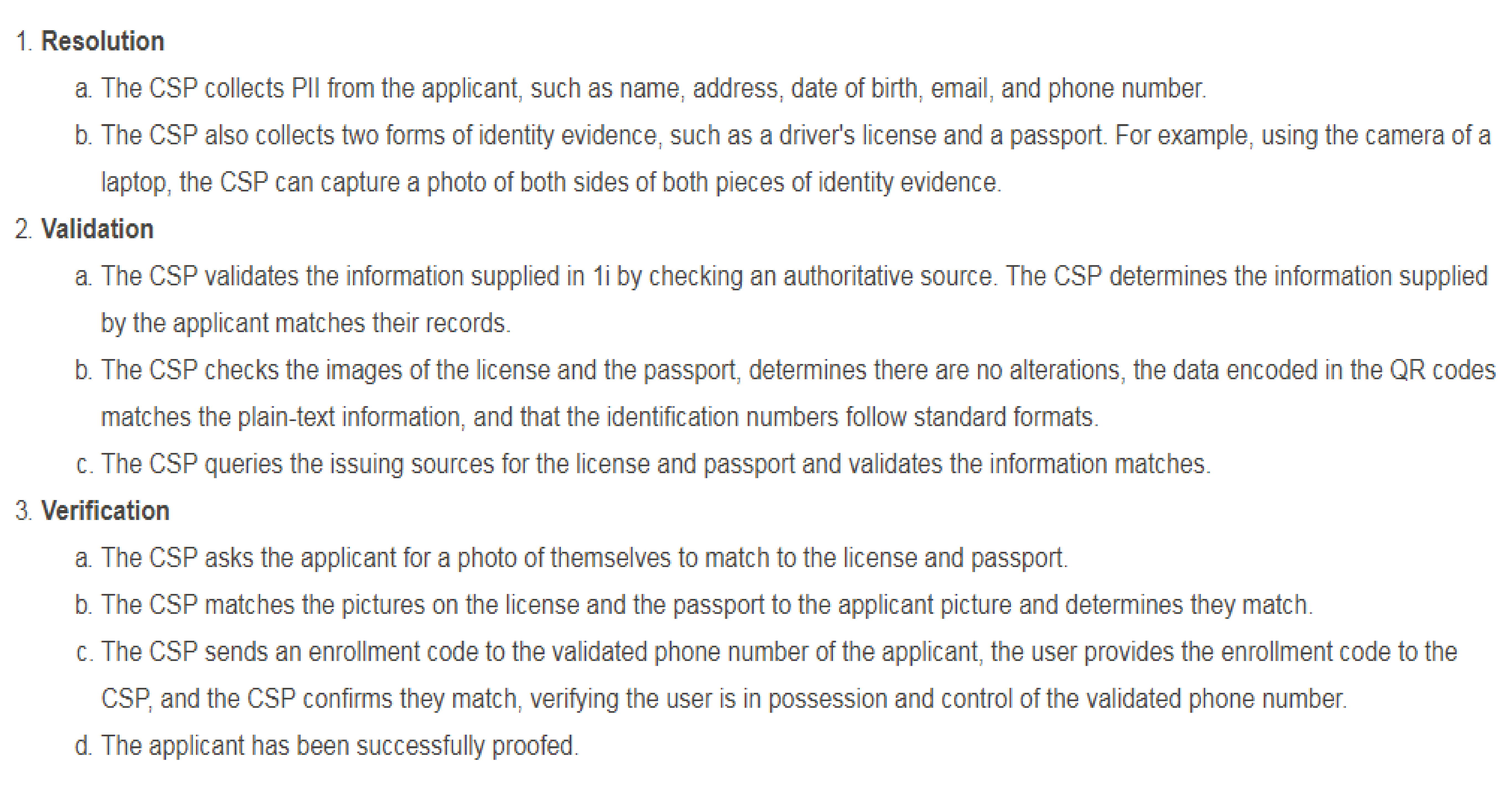
The Identity Proofing Process

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
- Other innovations…



1. **Resolution**
    a. The CSP collects PII from the applicant, such as name, address, date of birth, email, and phone number.
    b. The CSP also collects two forms of identity evidence, such as a driver's license and a passport. For example, using the camera of a laptop, the CSP can capture a photo of both sides of both pieces of identity evidence.
2. **Validation**
    a. The CSP validates the information supplied in 1i by checking an authoritative source. The CSP determines the information supplied by the applicant matches their records.
    b. The CSP checks the images of the license and the passport, determines there are no alterations, the data encoded in the QR codes matches the plain-text information, and that the identification numbers follow standard formats.
    c. The CSP queries the issuing sources for the license and passport and validates the information matches.
3. **Verification**
    a. The CSP asks the applicant for a photo of themselves to match to the license and passport.
    b. The CSP matches the pictures on the license and the passport to the applicant picture and determines they match.
    c. The CSP sends an enrollment code to the validated phone number of the applicant, the user provides the enrollment code to the CSP, and the CSP confirms they match, verifying the user is in possession and control of the validated phone number.
    d. The applicant has been successfully proofed.

An Example

Knowledge Based Verification's Role in Identity Proofing

- 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

SP 800-63B

Authentication & Lifecycle Management

Authenticators

Memorized Secrets

Look-up Secrets

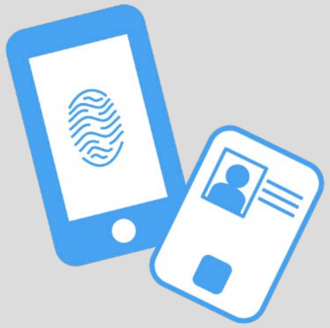
Out-of-Band Devices

Single Factor OTP Device

Multi-Factor OTP Devices

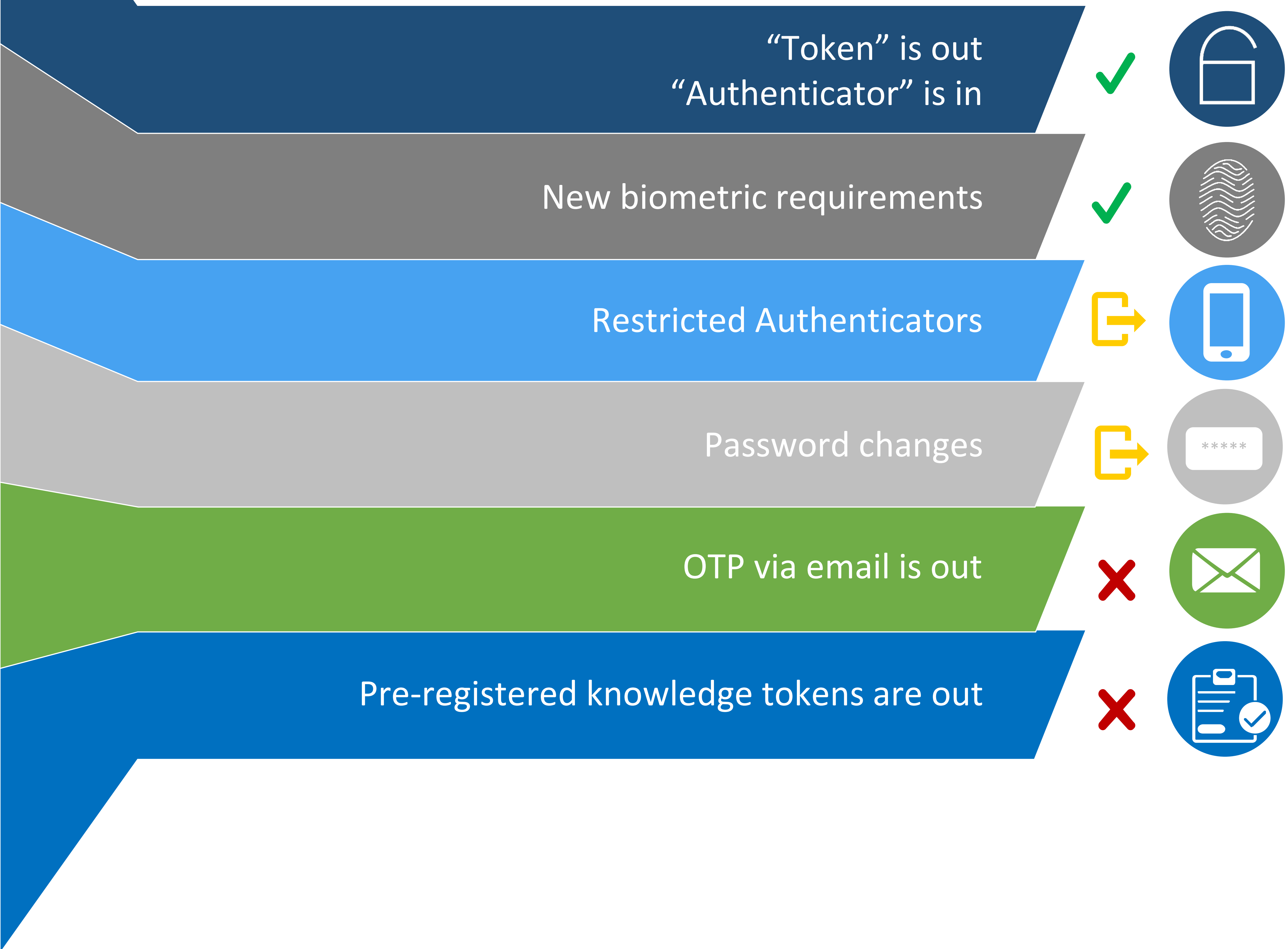
Single Factor Cryptographic Devices

Multi-Factor Cryptographic Software



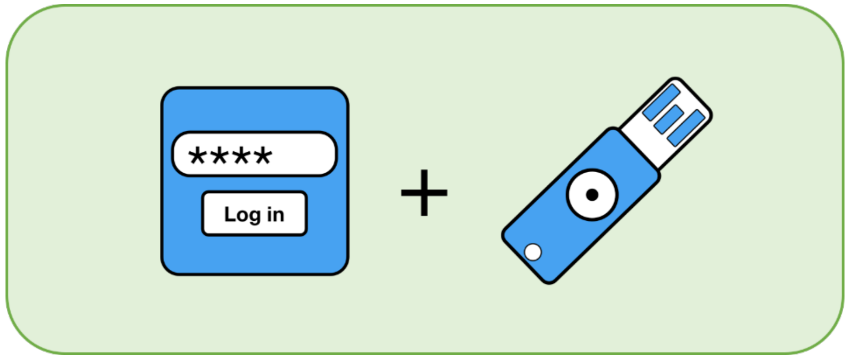
Multi-Factor Cryptographic Devices

Authenticator Guidance Changes



- "Token" is out
  "Authenticator" is in ✓
- New biometric requirements ✓
- Restricted Authenticators ➔
- Password changes ➔
- 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

Restricted Authenticators

- Currently just OTP over PSTN
- Requires:
  - Notification to user
  - Alternative authenticator option

Password Guidance Changes

- Same requirements regardless of AAL
- 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

800-63 ❤️ federation

Anywhere assertions are used

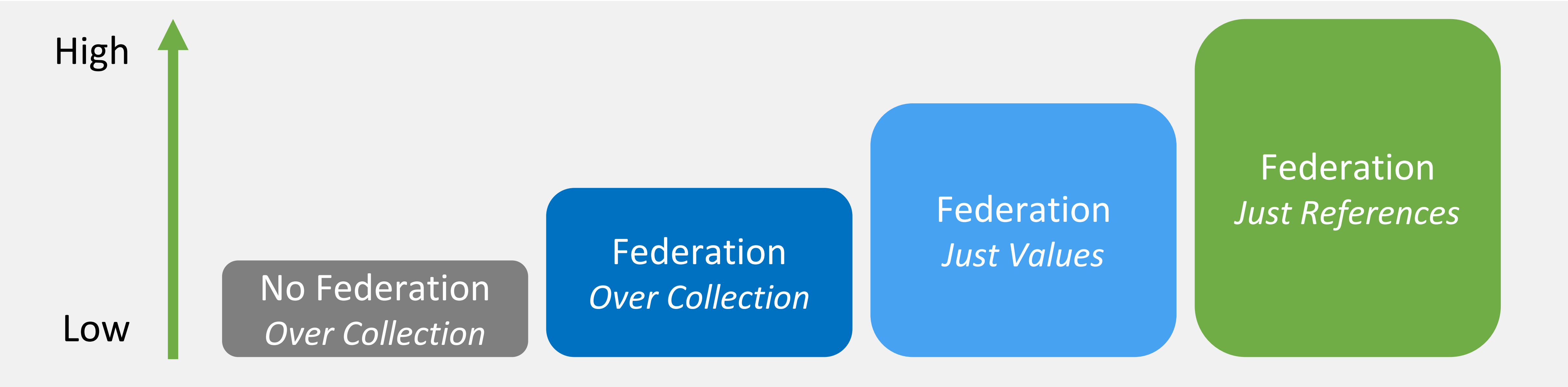
Intra/inter-agency federated credentials

Commercial federated credentials

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

Attribute References vs. Values

Maturity Model



Old		New
Give me date of birth.	→	I just need to know if they are older than 18.
Give me full address.	→	I just need to know if they are in congressional district X.

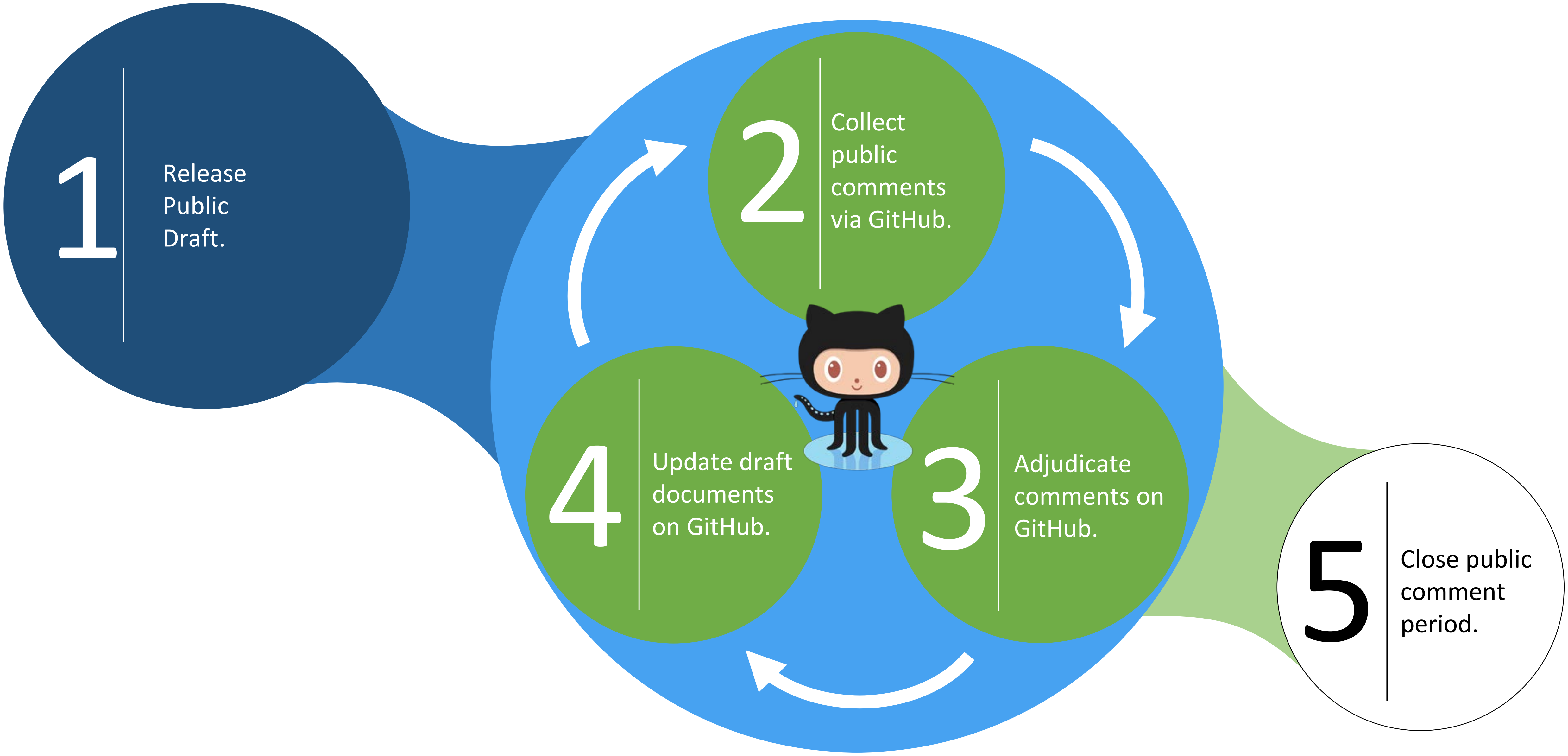
New Requirements

CSP SHALL support references and value API

RP SHOULD request references

Retaining the New Development Approach

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



1 Release Public Draft.

2 Collect public comments via GitHub.

3 Adjudicate comments on GitHub.

4 Update draft documents on GitHub.

5 Close public comment period.

What’s Next

Implementation Guidance

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

New Volume

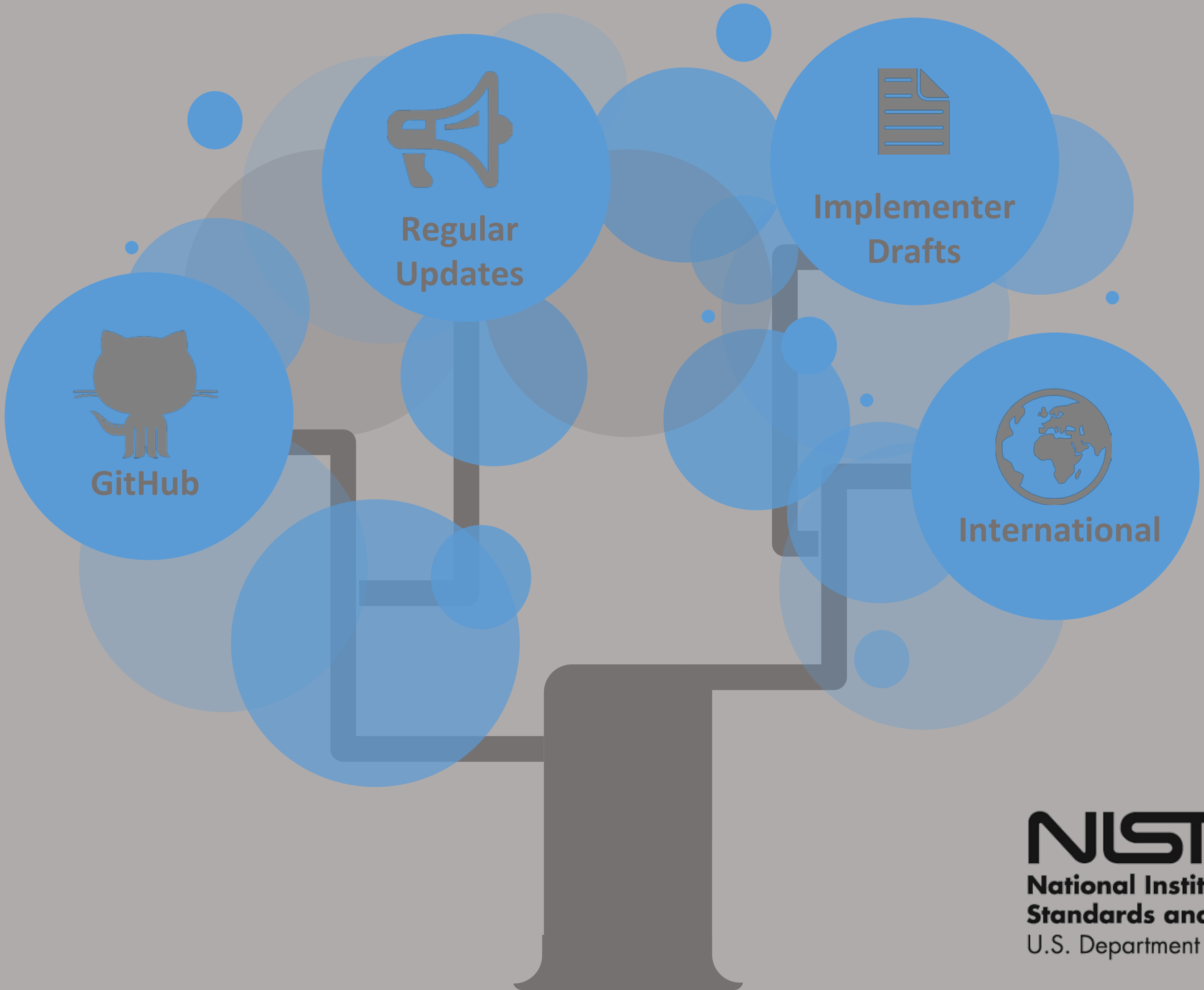
-D: Vectors of Trust
expected **2018**

Errata

Released in September, 2017

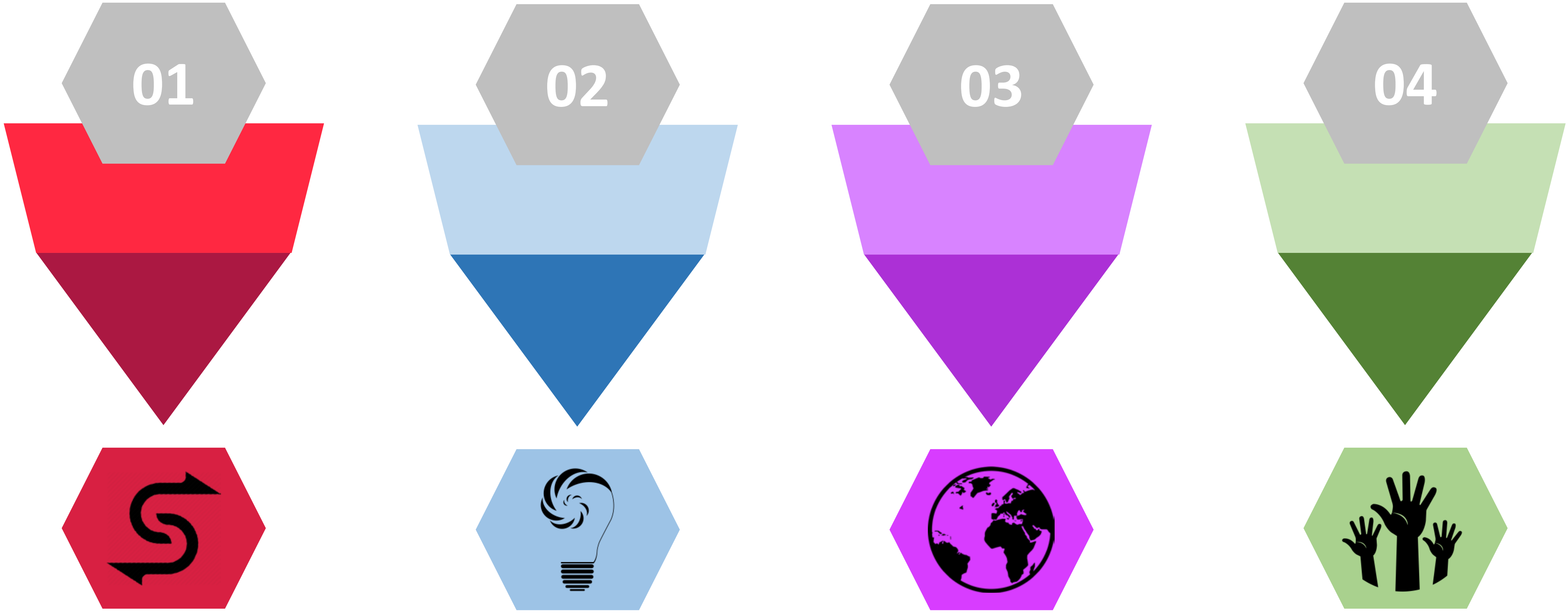
Fostering Growth

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.



National Institute of Standards and Technology
U.S. Department of Commerce

In Closing



01

Major Update

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

02

Innovation

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

03

International

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

04

Participate

Not our document.
It’s yours.
Participate!