These guidelines retire the concept of a level of assurance (LOA) as a single ordinal that drives implementation-specific requirements. Rather, by combining appropriate business and privacy risk management side-by-side with mission need, agencies will select IAL, AAL, and FAL as distinct options. While many systems will have the same numerical level for each of IAL, AAL, and FAL, this is not a requirement and agencies should not assume they will be the same in any given system.

For non-federated systems, agencies will select two components, referred to as *Identity Assurance Level(IAL)* and *Authenticator Assurance Level (AAL)*. For federated systems, agencies will select a third component, *Federation Assurance Level (FAL)*.

- **IAL** refers to the identity proofing process.
- **AAL** refers to the authentication process.
- **FAL** refers to the strength of an assertion in a federated environment, used to communicate authentication and attribute information (if applicable) to a relying party (RP).

The separation of these categories provides agencies flexibility in choosing identity solutions and increases the ability to include privacy-enhancing techniques as fundamental elements of identity systems at any assurance level. For example, these guidelines support scenarios that will allow pseudonymous interactions even when strong, multi-factor authenticators are used. In addition, these guidelines encourage minimizing the dissemination of identifying information by requiring federated identity providers (IdPs) to support a range of options for querying data, such as asserting whether an individual is older than a certain age rather than querying the entire date of birth. While many agency use cases will require individuals to be fully identified, these guidelines encourage pseudonymous access to government digital services wherever possible and, even where full identification is necessary, limiting the amount of personal information collected as much as possible.

SP 800-63A Enrollment and Identity Proofing

NIST SP 800-63-A addresses how applicants can prove their identities and become enrolled as valid subscribers within an identity system. It provides requirements by which applicants can both identity proof and enroll at one of three different levels of risk mitigation in both remote and physically-present scenarios. *SP 800-63A contains both normative and informative material.*

SP 800-63A sets requirements to achieve a given IAL. The three IALs reflect the options agencies may select from based on their risk profile and the potential harm caused by an attacker making a successful false claim of an identity. The IALs are as follows:

IAL1: There is no requirement to link the applicant to a specific real-life identity. Any attributes provided in conjunction with the authentication process are self-asserted or should be treated as such (including attributes a Credential Service Provider, or CSP, asserts to an RP).

IAL2: Evidence supports the real-world existence of the claimed identity and verifies that the applicant is appropriately associated with this real-world identity. IAL2 introduces the need for either remote or physically-present identity proofing. Attributes can be asserted by CSPs to RPs in support of pseudonymous identity with verified attributes.

IAL3: Physical presence is required for identity proofing. Identifying attributes must be verified by an authorized and trained representative of the CSP. As with IAL2, attributes can be asserted by CSPs to RPs in support of pseudonymous identity with verified attributes.

SP 800-63B Authentication and Lifecycle Management

For services in which return visits are applicable, a successful authentication provides reasonable risk-based assurances that the subscriber accessing the service today is the same as that which accessed the service previously. The robustness of this confidence is described by an AAL categorization. NIST SP 800-63B addresses how an individual can securely authenticate to a CSP to access a digital service or set of digital services. *SP 800-63B contains both normative and informative material.*

The three AALs define the subsets of options agencies can select based on their risk profile and the potential harm caused by an attacker taking control of an authenticator and accessing agencies' systems. The AALs are as follows:

AAL1: AAL1 provides some assurance that the claimant controls an authenticator bound to the subscriber's account. AAL1 requires either single-factor or multi-factor authentication using a wide range of available authentication technologies. Successful authentication requires that the claimant prove possession and control of the authenticator through a secure authentication protocol.

AAL2: AAL2 provides high confidence that the claimant controls authenticator(s) bound to the subscriber's account. Proof of possession and control of two distinct authentication factors is required through secure authentication protocol(s). Approved cryptographic techniques are required at AAL2 and above.

AAL3: AAL3 provides very high confidence that the claimant controls authenticator(s) bound to the subscriber's account. Authentication at AAL3 is based on proof of possession of a key through a cryptographic protocol. AAL3 authentication SHALL use a hardware-based authenticator and an authenticator that provides verifier impersonation resistance; the same device MAY fulfill both these requirements. In order to authenticate at AAL3, claimants SHALL prove possession and control of two distinct authentication factors through secure authentication protocol(s). Approved cryptographic techniques are required.

SP 800-63C Federation and Assertions

NIST SP 800-63C provides requirements when using federated identity architectures and assertions to convey the results of authentication processes and relevant identity information to an agency application. In addition, this volume offers privacy-enhancing techniques to share information about a valid, authenticated subject and describes methods that allow for strong multi-factor authentication (MFA) while the subject remains pseudonymous to the digital service. *SP 800-63C contains both normative and informative material.*

The three FALs reflect the options agencies can select based on their risk profile and the potential harm caused by an attacker taking control of federated transactions. The FALs are as follows:

FAL1: Allows for the subscriber to enable the RP to receive a bearer assertion. The assertion is signed by the IdP using approved cryptography.

FAL2: Adds the requirement that the assertion be encrypted using approved cryptography such that the RP is the only party that can decrypt it.

FAL3: Requires the subscriber to present proof of possession of a cryptographic key referenced in the assertion in addition to the assertion artifact itself. The assertion is signed by the IdP and encrypted to the RP using approved cryptography.

These guidelines are agnostic to the vast array of identity service architectures that agencies can develop or acquire, and are meant to be applicable regardless of the approach an agency selects. However, agencies are encouraged to use federation where possible, and the ability to mix and match IAL, AAL, and FAL is simplified when federated architectures are used. Furthermore, federation is a keystone in the ability to enhance the privacy of the federal government's constituents as they access valuable government digital services.