REFEDS Assurance Framework Implementation Guidance for the InCommon Federation

Assured Access Working Group, May 2021

community consultation draft, May 12, 2021

Repository ID: TI.157.1
Persistent URL: http://doi.org/10.26869/TI.157.1
Authors: Members of the Assured Access Working Group
Sponsor: InCommon Community Trust and Assurance Board (CTAB)
Superseded documents: N/A
Proposed future review date: N/A
Subject tags: InCommon, federation, assurance, trust, REFEDS

Abstract

The National Institutes of Health (NIH) have announced that they will soon begin checking identity assurance and authentication strength for researchers, grant awardees, and principal investigators (PIs), to log in to their grant management infrastructure and access high-value datasets and services. Specifically, the NIH Researcher Authorization Service (RAS) will begin offering resource providers such as the Electronic Research Administration (eRA), the opportunity to require well-proofed identities, multi-factor authentication (MFA), and other attributes necessary to support Research & Scholarly activities.

Higher education institutions that support research initiatives need to quickly establish or map existing business processes to proof identities, adopt MFA, and implement the technical changes to assert for whom this has been done, through their federated single-sign-on infrastructure.

The risk if US institutions do not do this is that researchers will lose existing access to these services. Until an institution supports NIH's requirements, the only alternative for a researcher to continue access is to obtain credentials through the US government at login.gov, which is not a

desirable user experience for US researchers (yet another login), and is not an option for international collaborators.

InCommon's Community Trust and Assurance Board charged the Assured Access Working Group (AAWG) with publishing these recommendations, intended for local implementation across US higher-ed institutions. A small campus task force composed of research administrators, business/employee operations staff, and IT administrators, should begin examining and implementing the following recommendations. Focus first on getting the means of communicating assurance information working, e.g. local-enterprise or low, then on other assurance values when your processes support them. Task force members should make decisions with risk mitigation and continued access for researchers in mind.

For those interested in a quick guide to implementation, see Appendix A.

Audience

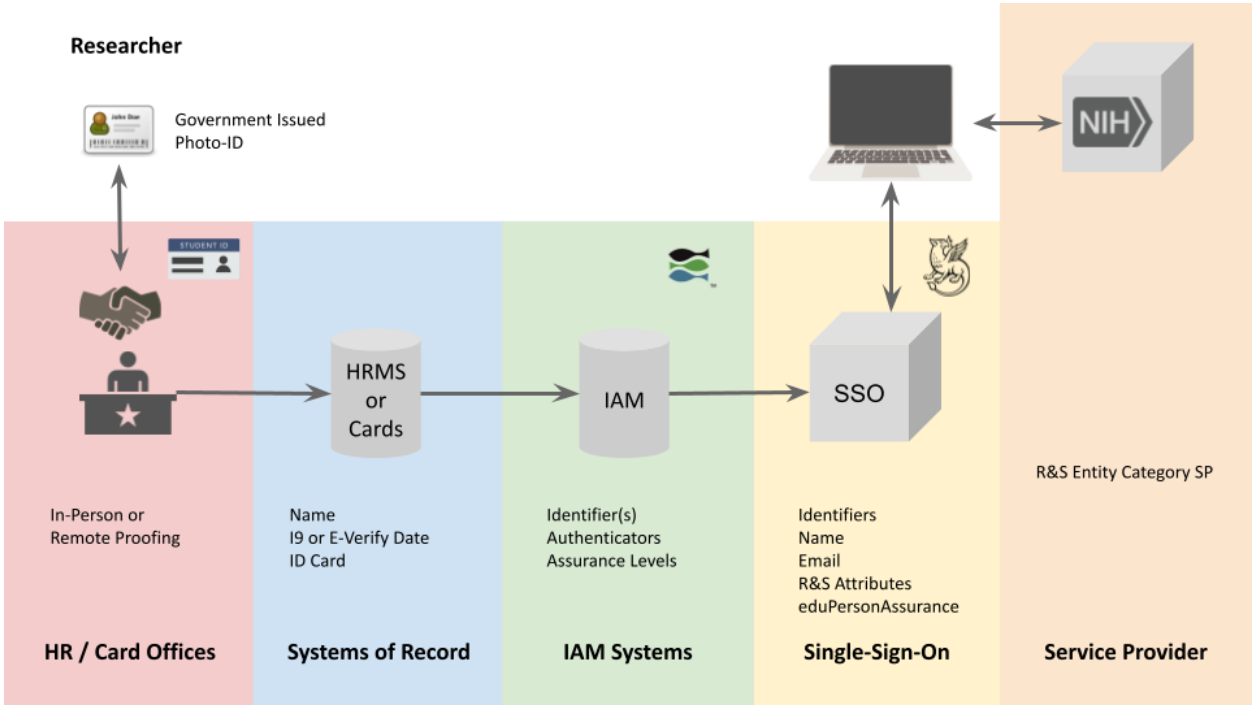
This document is intended for those within higher education institutions responsible for research administration, business/employee operations, and IT administrators that operate Identity Providers (IdPs) used by researchers, and for Service Providers (SPs) in a federation.

Table of Contents

Introduction

Research Service Providers (SPs) and others face an increasing need to demonstrate that their users have been well identity-proofed and that their authentication credentials are multifactor and well-bound to the user. These needs are incumbent on the users' Identity Providers (IdPs). The Assured Access Working Group developed the following guidance to identify and document processes that may be available at least to US academic organizations to form the basis for asserting corresponding claims of assurance of identity proofing and credential binding.

The following diagram shows typical connections between the researcher, business processes, and technical infrastructure of their host institution:



AAWG RAF Architecture[1]

How well identity-proofed and how well-bound the researcher's credentials will be is determined by reference to the claims of low, moderate, high, and local-enterprise as defined in the REFEDS Assurance Framework[2] (RAF). RAF itself aligns the low, medium, and high values with well-known standards such as those developed by the Kantara Initiative, the Interoperable Global Trust Federation (IGTF), and the electronic IDentification, Authentication and trust Services (eIDAS).

This initial guidance is provided to enable at least some academic institutions to address assurance claims before the NIH begins checking for them and offering a menu of protection to Institutes, Centers, and systems using the Researcher Authorization Service (RAS) in June 2021.

The recommendations below should be considered accurate as of the date of publication, but security and identity assurance should be considered a journey. As security recommendations from service providers evolve, the identity assurance and related processes at identity providers may need to change. The work requires both parties (Service Providers and Identity Providers) to work together to meet these goals, as if tunneling through a mountain from both sides. The content below may seem daunting, so readers are encouraged to approach this as a series of steps along a journey. The overall goal is to advance security collaboratively and in a coordinated fashion, as we each make progress and meet in the middle.

The AAWG may decide to continue work on a more comprehensive or revised set of recommendations after this initial release.

A glossary of many terms used in this document is available in the Internet2 InCommon Glossary[3].

Introduction to REFEDS Assurance Framework

The following guide is intended to assist the InCommon federation use the REFEDS Assurance Framework (RAF) version 1.0. The full specification of the framework can be found here:
https://wiki.refeds.org/display/ASS/REFEDS+Assurance+Framework+ver+1.0

REFEDS Assurance Framework includes four Identity Assurance Profiles (IAPs), three of which can be achieved by fulfilling one of several possible assurance standards' criteria. RAF IAP claims invoke selected identity assurance levels from the Kantara framework based on the deprecated NIST 800-63-2 series[10], the Interoperable Global Trust Federation (IGTF)[11], or the European Union's electronic IDentification, Authentication and trust Services (eIDAS)[12].

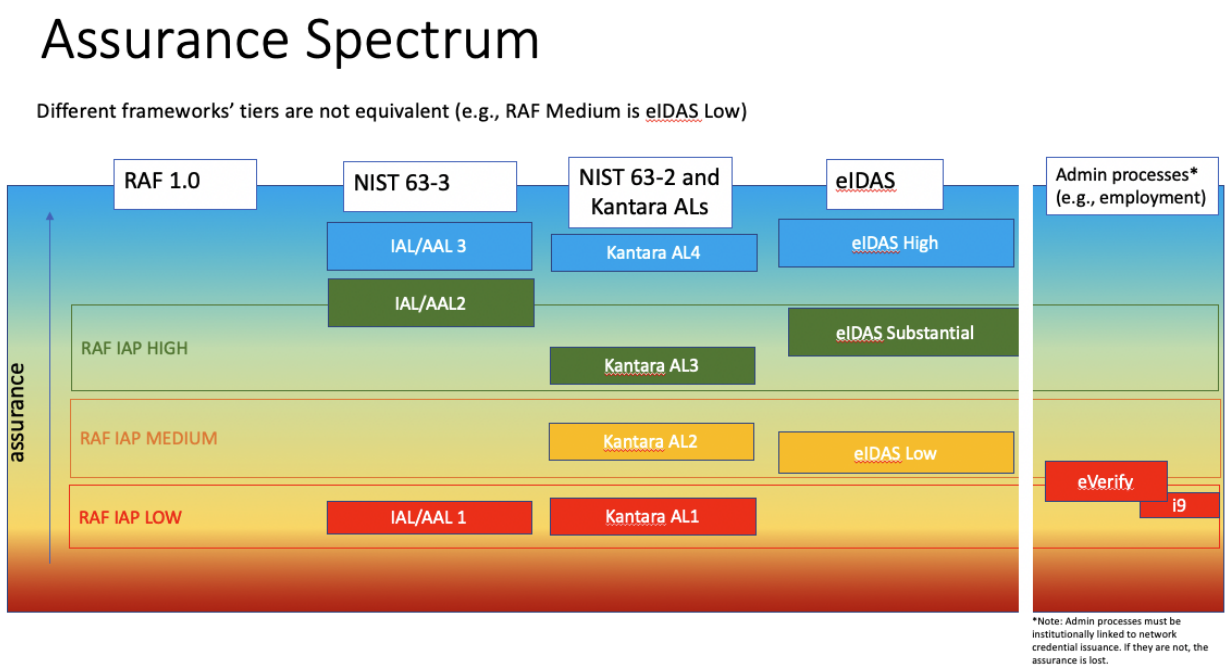
This document attempts to make RAF easier to understand and adopt for both Identity Providers (IdPs) and Service Providers (SPs) in a federation. For an IdP, the assurance framework needs to be easy to understand and practical to implement. To this end, this document describes in plain language what the IAP claim looks like, including leveraging existing business practices if applicable.

For an SP, the assurance framework needs to be easy to understand from a risk assessment perspective. The SP needs to know which IAP claim they should require, and if an IdP asserts an IAP claim it must align with the related identity assurance processes.

It is important for SPs to remember that different assurance standards' measures, e.g. of low, medium, and high, don't always equate to each other. For example, RAF IAP Medium is achievable through eIDAS Low. Also, RAF's highest IAP does not reach above the mid-tier of eIDAS, or achieve the highest Kantara level of AL-4.

The following chart shows rough equivalencies of assurance claims between some sets of assurance standards to aid in SP risk assessment, and as a guide to those familiar with various

identity assurance frameworks. Additional details on RAF Local Enterprise and Low/Medium/High are provided below.



Institutions may already have business processes in place that achieve a certain level of identity assurance. In the context of InCommon, it's important to remember that the identity assurance the federation is interested in refers specifically to an IdP's assurance at the time of issuing the network credential(s). It may be that an institution's employment processes or campus/employee ID card issuing process achieves a certain level of identity assurance, however, if that process is not bound to the issuing of the network credential (e.g., if the IT department issues network access without verifying the campus ID card or that the person claiming to need access is in fact the person who was hired and processed through HR), then the "chain of assurance custody" is broken. Institutions that have existing identity proofing processes could leverage existing practices and bind them to the IT department's credential issuing process, instead of having the IT department construct a separate identity proofing process from the start.

RAF IAP Claim Levels

The following sections highlight the various REFEDS Identity Assurance Profile claim levels, LOCAL ENTERPRISE, LOW, MEDIUM, HIGH. Information in the sections below cover the general practices and assurance procedures in order to assert that claim level for an individual at the organization.

IAP LOCAL-ENTERPRISE

RAF IAP local-enterprise is not included in the assurance spectrum figure above and is not aligned with the traditional framework assurance levels, but this does not mean that it is without substantive value to a relying service provider. All Identity Providers registered with InCommon may assert the IAP/local-enterprise claim for federated logins of credentials assigned to users granted access to any of the organization's *critical internal systems*, and for all credentials managed by the same or better procedures.

Why is this and what systems qualify as critical internal systems?

The definition of IAP/local-enterprise is:

> The identity proofing and credential issuance, renewal and replacement are done in a way that qualifies (or would qualify) the user to access the Home Organisation's internal administrative systems (see appendix A).

And RAF Appendix A says:

> Some of the components in section 2 define an assurance level implicitly by a statement that the level of assurance is good enough for accessing the Home Organisation's internal systems. This relies on the assumption that if the Home Organisation deems the assurance level good enough for accessing internal systems locally in the Home Organisation, the assurance level may be good enough for accessing some external resources, too. It is assumed that the Home Organisation has made a risk based decision on what exactly are the assurance level requirements for those accounts. Home Organisations may have several internal systems with varying assurance level requirements. It is assumed that the Home Organisation's internal systems referred to here could be:
>
> - The ones that deal with money (for instance, travel expense management systems or invoice circulation systems)
> - The ones that deal with some employment-related personal data (for instance, employee self-service interfaces provided by the Human Resources systems)
> - The ones that deal with student information (for instance, administrative access to the student information system)

The InCommon Participation Agreement legally obligates each Participant to adhere to Baseline Expectations, and the first two Baseline Expectations statements for IdPs require that the credentials used in federated logins are the same as or at least as trustworthy as those used to access the organization's internal systems. Organizations that rely on these credentials for access to its critical internal systems have made a risk based decision, perhaps a series of them over time, to do so, and the organization has likewise demonstrated its satisfaction with the processes used to identify users permitted access to its critical internal systems, bind credentials to them, and manage their credentials on-going. Hence, the organization has

demonstrated that it accepts whatever risk is inherent in potential misuse of any of their critical internal systems by an authorized credential. Consequently, all users whose identity is proofed by the same or better procedures, and who possess credentials that are managed by the same or better procedures, can have an IAP/local-enterprise claim asserted with their federated logins.

Which group of users this applies to for a given organization is a function of which critical internal systems to which the organization permits user access, and other users subject to the same or better identity proofing and credential management practices. Some critical internal systems are identified by RAF Appendix A, and others of a similar nature are listed here:

- Travel expense management
- Financial transaction posting and approval
- Employee self-service applications
- Instructor and administrative access to student information systems
- Grants management
- Contracts management
- Institutional Review Board application system
- Conflict of Interest attestation system
- Environmental Health & Safety compliance systems
- Required privacy and/or security training for which individuals must login to complete so that the organization can track its compliance with these requirements

This list is not exhaustive and other internal systems could be considered critical systems. Here are some criteria by which an internal system might be deemed critical:

- Managing the organization's money; audit trail for how it was allocated and where it was disbursed to
- Managing legal representations the organization makes to external parties
- Managing the organization's regulatory or legal compliance obligations

Note that if, say, student or other broad institutional roles (e.g. eduPersonAffiliation faculty/staff/student) are identity proofed in the same manner as users of any of the above systems, and if their credential is managed in the same way, their federated logins can likewise be accompanied with a claim of IAP/local-enterprise.

IAP LOW

At IAP Low, an IdP can do in-person or remote verification for an applicant. For in-person verification, the IdP accepts the applicant's self-asserted identity, with no evidence required. For remote verification, the IdP might request a self-asserted phone number or email address, and validates the applicant controls the phone number or email address by sending a verification code to that address. This is essentially what Google or Facebook requires for new users.

RAF IAP Low is built on either selected paragraphs from NIST 800-63-2 AL-1 (adapted through Kantara SAC AL-1) or the IGTF levels DOGWOOD and ASPEN.

Abstracting from these, IAP Low can be implemented by an IdP in very few steps, but most SPs, especially SPs from the federal government such as National Institutes of Health, will not find IAP Low to be a sufficient claim of assurance to grant access to federal information systems.

IAP MEDIUM

RAF IAP Medium is built on either selected paragraphs from NIST 800-63-2 AL-2 (adapted through Kantara SAC AL-2) or the IGTF levels BIRCH and CEDAR, or eIDAS assurance level "low".

Abstracting from these, to meet IAP Medium, the applicant must *at least submit a government-issued photo ID* to prove their identity to the IdP Operator. For example, a state driver's license may be used during the I-9[4] or E-Verify[5] employment verification processes.

However, the I-9 process also allows the case where an applicant can submit, for example, a high school ID (a school photo ID not from the IdP's institution) in order to prove the applicant may be employed in the U.S., but such an ID is not sufficient to reach IAP Medium. On the other hand, internal to the IdP's institution, if the local campus ID card contains a photo and is presented to the IT department for the network credential, and the school has a strong identity proofing process in issuing the card that includes requiring a government issued photo ID, then the presentation of a valid campus ID card at the IT department is sufficient. The key here is that the institution establishes a holistically strong binding of identity assurance between the time the person is hired or admitted, gets their campus ID card, and receives an issued network credential.

For in-person verification, the photo ID must reasonably appear to be valid to the person checking it, and the person holding the photo ID must reasonably appear to be the person to whom the ID was issued (i.e., the person checking the credential in person must look at the photo and it must reasonably match the person presenting the card), and the card must be current (e.g., not expired).

For remote verification, the applicant can send their government issued photo ID to the IdP, and the IdP has had a remote live video conversation with the applicant. See more information on Remote Proofing below.

IAP HIGH

RAF IAP High is built on either selected paragraphs from NIST 800-63-2 AL-3 (adapted through Kantara SAC AL-3) or eIDAS assurance level "substantial".

Abstracting from these, IAP High builds on the IAP Medium claim, but enhances it through a more rigorous validation that the identity document is a legitimate piece of evidence and

validation that the person presenting it is the person to whom the document was issued. To meet IAP High, the IdP Operator must confirm an unexpired government photo ID, validated as legitimate, and verified with an authoritative source to minimize risk of a lost, stolen, suspended, revoked or expired document. Validation can be in-person as long as the evidence (such as a govt-issued ID card) has verification means built into the card that can be visually inspected (e.g., to include but not limited to holographic images, laser etching, etc.). Any electronic verification of an evidence's data must be cryptographically protected.

As discussed for IAP Medium, the IdP Operator must meet this requirement, but this proofing does not have to happen in the IT department itself, as long as there is an unbroken chain of custody between the institution's process (for example, a school's ID card issuing office's process) and the office issuing the network credential.

Form I-9 and E-Verify at High: The I-9 and E-Verify processes are intended to verify eligibility to work in the U.S, and as such, the identity assurance bar to pass this process is not sufficient to meet IAP High by itself. Most importantly: to determine eligibility to work, the institution **may not** require which specific identity evidences from the I-9 "LISTS OF ACCEPTABLE DOCUMENTS" must be presented, but must accept all valid evidences provided. Furthermore, even if the institution requires government photo IDs as part of the employment process for other reasons than verifying eligibility to work in the U.S. (e.g. identity verification for access to an institution's sensitive or administrative information), the verification process with E-Verify is still not sufficient. E-Verify checks the data entered into the I-9 form, but does not validate the identity documents themselves.

Assigning RAF Claims to Subjects

The various REFEDS Assurance Claim Levels should be applied to individuals or subsets of the network credential holders from the IdP Operator organization. An institution likely has existing business processes which can be leveraged to align with the relevant RAF IAP Levels. Readers should examine the Existing Processes to Leverage section for more information.

Business processes, such as employment/hiring practices, campus ID card operations, as well as risk mitigating strategies should be incorporated into determining the appropriate levels. Consequently, business processes or policies may need to be adjusted to increase the assurance in the identities and their bound credentials.

An institution may decide to identify just those researchers impacted by the NIH changes, or take a broader approach to establish RAF IAP claim levels to cover the majority of campus users, including an elevation process whereby an individual subject may elevate their network credential and identity assurance in order to obtain services which require a higher claim level. The assessed scope of effort will inform the different approaches a campus may wish to undertake.

Identifying Researchers and Access Needs

Representatives from the National Institutes of Health (NIH) and InCommon examined the data on grant recipients to identify members of the InCommon federation that may be in scope for this effort. Over 260 organizations were identified. In order to identify individuals at a specific institution, the NIH provides a reporting website where principal investigators can be identified by organization. Institutions can use the RePORT[6] tool to identify researchers to communicate with.

This method of identifying researchers does not include other collaborators that are not the principal investigator, including those applying for grants. It is recommended that local grant management systems also be leveraged to augment the results provided by NIH.

Recommendations

The working group recommends that institutions with researchers accessing the NIH services*, or with an interest in elevating their identity proofing and security posture, establish a campus task force or working group to begin examining and implementing the following recommendations.

The task force should include research administrators, business/employee operations staff, and IT administrators to map existing processes and apply the recommended practices within their own university context.

A high-level project outline is provided as a guide:

1. Assess and document existing business practices that support the system(s) of record where identity proofing events are stored.
2. Implement IAP assertions based on existing records.
3. Assess critical groups not covered in the initial assessment and implementation. These may be groups requiring additional verification to attain a higher level assertion (e.g., LOW to MEDIUM).
4. Update policies and procedures to address any gaps identified in the assessment.

Leveraging Existing Business Processes

Higher Education entities have existing business processes and practices that can be leveraged to meet or approach REFEDS Assurance Framework claims.

The following sections outline potential existing processes already in practice at many institutions that can be evaluated for alignment with the various assurance frameworks used in RAF claims. Each institution should evaluate their own business processes to support these self-asserted assurance claims.

Note: All InCommon Participants operating an IdP meet the RAF Conformance Criteria, a prerequisite for asserting any IAP value. Those criteria align with InCommon's Baseline Expectations for Identity Providers, and the InCommon Participation Agreement legally obligates the Participant to adhere to Baseline Expectations.

Hiring and Employment Verification Processes

For U.S. institutions, Form I-9 (and optionally E-Verify) are used to determine employment eligibility at organizations. These processes are already in place and may be leveraged to support RAF IAP Medium.

Use for:

- Paid Employees

Form I-9 and E-Verify in support of IAP Medium

For U.S. institutions, the employment process to achieve I-9 compliance using E-Verify reasonably achieves RAF IAP-Medium. However, for an institution to claim this level of assurance through their employment process, the institution must reasonably bind the employment process to the issuance of the network credential, such that the office issuing the network credential must verify with the employing department that the person to whom the credential is issued is also the person who was vetted and hired by the employing office (e.g., Human Resources). U.S. institutions may only use the fact of employment validated by E-Verify for those network users who are, in fact, employees.

Exceptions: U.S. institutions may not claim this level of assurance for employees who have not gone through the I-9 and E-Verify process, for example those whose employment predates those processes[1]. Additionally, I-9 and E-Verify also do not apply to users who are not employees. However, for those exceptions, the institution may re-validate their identities by proofing the individual in-person by verifying a non-expired government-issued photo ID and recording this event. Similarly, this check of a government-issued photo-ID at the time of issuing the network credential also fulfills IAP-Medium.

E-Verify is not a required process, and as such not all institutions verify the I-9 data through E-Verify. Accomplishing I-9 by itself without E-Verify brings notably less identity assurance based on opening the list of acceptable evidences[8] to include combinations which do not have any photo ID. Institutions using I-9 without E-Verify need to supplement their identity proofing processes (e.g. checking government ID for photo ID issuance) prior to issuing network credentials in order to reasonably achieve IAP Medium.

The I-9/E-Verify process, even when tightly coupled between HR and IT departments with the network issuance process, is not sufficient to claim IAP High.

---

[1] From https://www.e-verify.gov/about-e-verify/questions-and-answers "Unless an employer is a federal contractor with a federal contract containing the FAR E-Verify clause, it cannot use E-Verify for existing employees."

Criminal Background Checks

Criminal Background Checks are commonly used to identify criminal history where those acts may prevent employment. These processes are typically greatly abstracted from the subject and may not be useful in elevating assurance. While these services may be helpful to identify and protect against the risk of a synthetic identity, they may not provide valuable information to elevate an identity from IAP Medium to High.

Campus ID Card Offices

In many cases Campus photo ID card offices' existing processes can be leveraged to perform in-person proofing of constituents. In-person proofing that verifies a non-expired government issued photo ID, such as driver's license, passport, or military ID can be leveraged along with other processes (e.g., I-9) to meet IAP Medium.

Use for:

- Paid Employees
- Students
- Affiliates
- Volunteers
- Contractors

See the recommendations on Recording Proofing Events.

Remote Proofing

Remote proofing is a process by which the subject and related identity evidence are verified when the subject and verifier are not in the same physical location. Typically this would be via video conference, or exchanging scanned copies of the identity evidence. Recommendations on how to perform this in a secure manner can be found in NIST 800-63-3 5.3.3.2 Requirements for Supervised Remote In-person Proofing.

See the recommendations on Recording Proofing Events.

Dedicated Identity Proofing Services

Some user populations may not be covered by any of the existing processes above. In these cases, establishing a request process for on-campus or remote proofing may be required, in order to obtain the claim level required by the services they are accessing. This process could also be utilized where a user with an existing network credential at a lower level, may elevate their access as necessary.

Use for:

- Unpaid Collaborators
- Online students
- Visiting Scholars
- Elevating IAP levels

Campuses may wish to establish a new office, or expand the service offering of an existing office (e.g., ID Card Office), to provide identity proofing services. The procedures and documentation, auditability, etc. should all be considered when establishing an identity proofing service.

Third-parties provide identity proofing services for a fee. These services are currently beyond the scope of this document.

Process Recommendations and Other Considerations

Credential Binding

Care must be taken to ensure the "chain of custody" in account binding to an identity. As referenced elsewhere in this document, the person to whom the network credential is issued must in fact be the same person who was proofed. For example, if ID proofing happened at campus ID card issuance and that campus ID card is used to establish the network credential.

Common practices to establish and maintain credential binding are to use address-of-record (email, physical) communication to exchange a one-time secret to establish primary credentials, or have the individual handling the employment/student onboarding process assist with binding the credentials to the user. After credentials are obtained, institutional policies should forbid the sharing of credentials and clearly inform the user that they are responsible for their credentials and to report suspicious activity.

Recording Proofing Events

When proofing occurs, these events should be tracked for record keeping and auditing. It is important that the date of these events be recorded, and that a documented procedure or process was followed. For RAFv1, it is not required to store copies of the identity evidence itself.

Employee Relationships that Pre-date E-Verify

Institutions may have paid employees with employment relationships that predate employment verification processes, especially E-Verify and REAL ID drivers license standards. For these individuals, an institution may make a risk-based decision to consider these subjects as meeting the proofing requirements and evidences required at the time, in combination with their long-standing delivery of paychecks to their accounts, as meeting a specific IAP claim level. Other institutions may wish to re-proof the identities and establish a common baseline for all subjects which meet the relevant IAP level. The approach taken should consider not only the risk to the local institution, but also the risk to external service providers dependent on such claims.

Account Recovery and Password Resets

Care must be taken to ensure that account recovery and password reset processes happen in a manner consistent with the assurance bound to the credential and maintain the established chain of custody. If resets are necessary that do not meet the appropriate assurance level, the assurance level cannot be asserted until the identity is re-proofed.

Institutions should have a documented remote proofing process to support credential reset processes, and training on this process should be completed by all Help Desk associates which support the credential reset processes.

For more information on account recovery best practices, see information from NIST 800-63-3 6.1.2.3 on Replacement of a Lost Authentication Factor.

Campus ID Card Early Assignment

Caution should be taken when campus ID cards are assigned and recorded in the card database prior to in-person proofing. In this case, assignment of a campus ID card may not be a direct indicator that the identity proofing was ever performed. In these instances, checking to see if the card has been used may be an alternative signal that the proofing process has taken place and the user is in possession of the card.

Technical Requirements

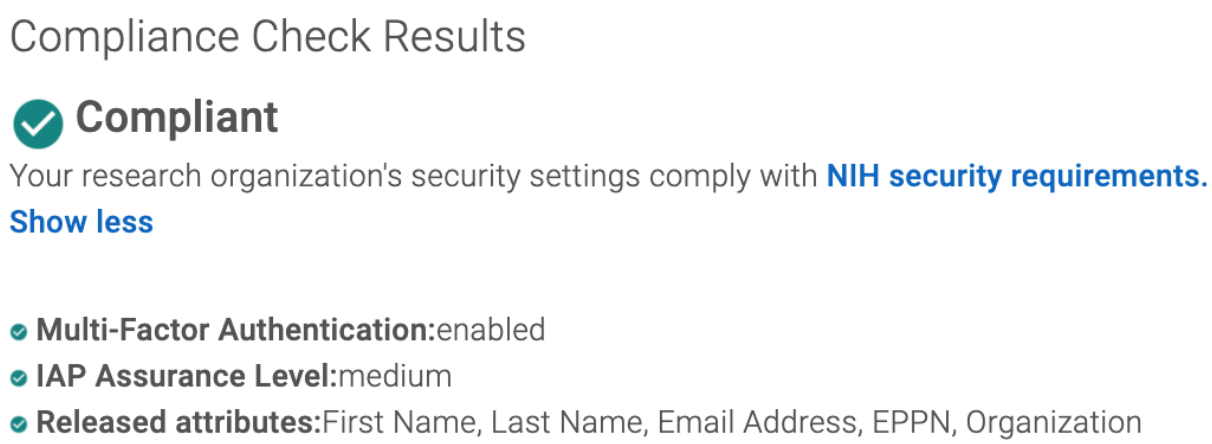
Identity Provider Operators will need to implement various technical changes in order to assert the appropriate RAF IAP claim levels. Specifically, ensure that the data pertaining to the relevant business processes is exposed to Identity & Access Management infrastructure, including single-sign-on services. The means of accomplishing this will vary based on institutional systems and preferences, but in general, use the data from the systems of record to compose an IAP assurance claim policy for each corresponding claim level and store this as an attribute in the directory.

For storing assurance values, the eduPerson[13] schema includes eduPersonAssurance[14], a multi-valued attribute which can be populated for an entry within the campus AD/LDAP directory. The specific values should conform to the recommendations within the RAF documents. Alternatively, a group membership indicating RAF IAP could be populated within your directory. Once this attribute is placed within reach of the federated single-sign-on environment, testing the technical integrations to assert the relevant values can begin.

The configuration of eduPersonAffiliation attribute assertion will vary based on IT architectures and Identity Provider software. For Shibboleth Identity Providers, the concepts of Attribute Resolution[15] and Attribute Filter[16] (release) are well documented within the Shibboleth Wiki. For Microsoft Active Directory Federation Services (ADFS), administrators will create a Claim Rule[17] to send eduPersonAssurance attribute.

Testing and Validation

NIH has provided a simple website to test various attribute assertions, including the RAF IAP values. A test subject which meets the required assurance framework criteria should visit the compliance check site[18], select their Identity Provider, and begin the login process. Successful logins can be verified by examining the output. A sample of this output is provided below:



Compliant
Your research organization's security settings comply with NIH security requirements.

Compliant Multi-Factor Authentication: enabled
Compliant IAP Assurance Level: medium
Compliant Released attributes: First Name, Last Name, Email Address, EPPN, Organization
Missing attributes: none

For Identity Providers - Mapping Common Institutional Roles and Associated Identity Proofing to REFEDS Assurance IAP

The following guide is intended to provide a quick mapping from an eduPersonAssurance or audience type to an existing process which could be leveraged to map a REFEDS Assurance Framework claim.

How to use this tool:

- Consider a person for whom you need to assert REFEDS Assurance IAP value,
- Identify all applicable role(s) that person has within your institution,
- Use the decision trees below to determine the appropriate value to assert for each role,
- Assert ALL applicable REFEDS Assurance IAP values for that person during federated SSO.

Use Case 1: the person has administrative access to enterprise applications:

The REFEDS Assurance Framework defines an IAP value allowing an organization to signal that a credential is managed in a way that qualifies the user to access the Home Organisation's internal administrative systems. The premise is that if the Home Organisation deems the assurance level good enough for accessing internal systems locally in the Home Organisation, the assurance level may be good enough for accessing some external resources, too. It is assumed that the Home Organisation has made a risk based decision on what exactly are the assurance level requirements for those accounts. (See IAP LOCAL ENTERPRISE for additional details, including which systems might be considered "critical internal administrative systems").

The InCommon Participation Agreement legally obligates each Participant to adhere to Baseline Expectations. In particular, Baseline Expectations requires that the credentials used in federated logins are the same as or at least as trustworthy as those used to access the organization's internal systems. Organizations that rely on these credentials for access to its critical internal systems have made a risk based decision.

When a user signs in to a federated application, if the credential used is the same as the one they use to access these critical internal systems, the IdP should assert the `/IAP/local-enterprise` value in addition to any other applicable eduPersonAssurance values in the SAML assertion.

Use Case 2: the person is an employee:

Question	Yes	No
1. Is the person a current paid employee of the institution? A person is a "current paid employee" if they are paid from the institution's payroll system, and are considered an "active employee" at the sign-in time.	Continue to 2	Continue to 4
2. Has the person completed the I-9 employee verification process? All US workers hired after 1986 must complete the I-9 employment eligibility form required by the Immigration Reform and Control Act of 1986. Employees who were hired before 1986 may not have completed I-9	Continue to 3	Continue to 4

3. Was the I-9 process completed with in-person verification of a government issued photo ID, AND proof of photo ID verification is recorded in your organization's system of record?	Assert
	
	`/IAP/medium`
	`/IAP/low`
	
	Skip to End
		Assert
		
		`/IAP/low`
		
		Skip to End

4. Has the person undergone any other in-person verification of a government issued photo ID, AND proof of photo ID verification is recorded in your organization's system of record?	Assert
	
	`/IAP/medium`
	`/IAP/low`
		Assert
		
		`/IAP/low`

End		

Use Case 3: the person is a student:

Question	Yes	No
1. Does your campus ID Card Office have a documented procedure to perform in-person verification of a government issued photo ID prior to issuing a campus ID Card?	Continue to 2	Continue to 3

2. Is the student in possession of their assigned ID card?	Assert
	
	`/IAP/medium`
	`/IAP/low`
		Continue to 3

3. Has the person undergone any other in-person verification of a government issued photo ID, AND proof of photo ID verification is recorded in your organization's system of record?	Assert
	
	`/IAP/medium`
	`/IAP/low`
		Assert
		
		`/IAP/low`

End		

Other affiliation use cases are left as an exercise for the user.

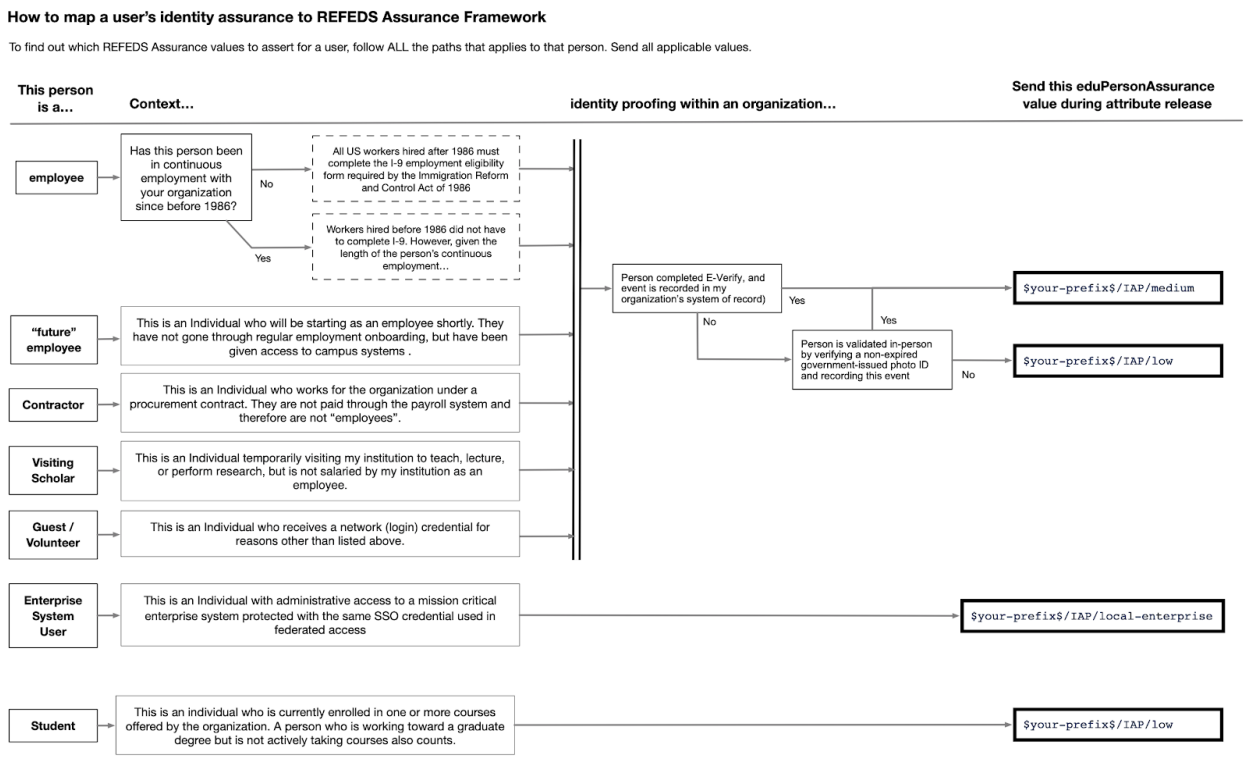
Example:

Josephine B. is a MBA student at Hogwarts Academy. She also works part time in the procurement office as a buyer. When Josephine became a part-time employee at the start of 2019, HR inspected her drivers license, but did not record proof of that event.

As part of her job, she has administrative access to Hogwarts' procurement system.

When Josephine signs into a federated application, Howgart's IdP should assert the following IAP values for Josephine:

Value	Reason
`/IAP/low`	Josephine is an employee, went through I-9 employment verification, but the campus does not have records of ID Proofing using a government issued ID; Josephine's credential meets /IAP/low, but not /IAP/medium
`/IAP/local-enterprise`	Josephine has administrative access to a critical internal administrative system. It is appropriate to assert /IAM/local-enterprise



[How to map a user's identity assurance to REFEDS Assurance Framework][19]

Appendices

Appendix A: Quick Implementation Guide

The need for, and concepts pertaining to, identity assurance are not new. InCommon has a long history of support for identity trust frameworks, dating back to 2012. What is new, is a major US government agency and resource provider announcing the requirement and support for expressing assurance via an international framework (the REFEDS Assurance Framework v1). Services protected by the NIH may begin requesting assurance levels as soon as June 2021.

The following is a summary of guidance from the Assured Access Working Group on implementing the REFEDS Assurance Framework v1.

How Do I Get Started?

We recognize that designing and operating an identity assurance program is a complex endeavor that will require significant time and effort from multiple stakeholders in your institution. This is a journey measured in years, not months. There is no expectation that institutions will immediately meet the highest levels of identity assurance. Right now, we are asking you to start the planning process and begin taking the first steps.

Using this guide as support, institutions should establish a task force consisting of stakeholders from IT and major person data stewards to:

- identify existing identity proofing business processes on your campus;
- assess alignment with and implement the REFEDS Assurance Framework (RAF) for subsets of the population;
- develop strategy, identify funding, and devise implementation plan to communicate a user's identity proofing levels using the values defined in the REFEDS Assurance Framework.

Order of Implementation

IdP Operators should examine and compose groups for the RAF claim levels in the following order:

LOCAL-ENTERPRISE

- Identify those with self-service access, or those in scope for NIH research
    - Access to self-service HR/Payroll system to control paycheck deposit
    - Grant awardees and collaborators
    - Research administrators

- Are the identity processes for the above populations the same as as broad eduPersonAffiliation roles, e.g. faculty/staff/student? If so, apply local-enterprise to all of those relevant eduPersonAffiliation populations.

LOW

- Control of an email account can be used as “address of record” verification. If you run an email server, or control over a self-asserted email address is verified, these individuals qualify for low.
- Ensure identifiers, including email addresses, are not reassigned.

MEDIUM

- A government issued photo ID must be verified.
  * Form I-9 and E-Verify only qualify if the identity evidence provided meets this requirement. This cannot be assumed.
- Campus ID card offices should verify government issued ID.
- Ensure credentials are bound to the user.
- Password resets must ensure equivalent proofing, or re-proofing and binding of the identity to credential.
- Policies must forbid sharing of accounts and credentials.

HIGH

- Verify evidences against their government source.
  * E-Verify meets this if the identity evidence was a driver’s license (REAL ID), or passport, including anti-tamper methods.

Timeline

InCommon has published a timeline of events and will provide updates as new information is shared from the National Institutes of Health and related Service Providers. See the following web page for more information:
https://spaces.at.internet2.edu/display/federation/get-nih-ready/[20]

Appendix B: Resources

1. “AAWG RAF Architecture,” https://docs.google.com/drawings/d/1BYhVNrGdL5sHSUsmi42vtp9rfCI1DIciyUlQHIHJOtQ/edit?usp=sharing
2. “REFEDS Assurance Framework,” https://refeds.org/assurance
3. “Internet2 InCommon Glossary,” https://spaces.at.internet2.edu/display/federation/Glossary
4. “Form I-9, Employment Eligibility Verification,” https://www.uscis.gov/i-9
5. “E-Verify,” https://www.e-verify.gov/

6. “NIH RePORT,” https://report.nih.gov/award/index.cfm
7. Form I-9 Training and Webinars: https://www.uscis.gov/i-9-central/form-i-9-resources/form-i-9-training
8. Form I-9 Acceptable Documents: https://www.uscis.gov/i-9-central/form-i-9-acceptable-documents
9. “NIST 800-63-3 5.3.3.2 Requirements for Supervised Remote In-person Proofing,” https://pages.nist.gov/800-63-3/sp800-63a.html#-5332-requirements-for-supervised-remote-in-person-proofing
10. “NIST 800-63-2 (deprecated),” https://csrc.nist.gov/publications/detail/sp/800-63/2/archive/2013-08-29
11. “Interoperable Global Trust Federation (IGTF),” https://www.igtf.net/
12. “eIDAS (electronic IDentification, Authentication and trust Services),” https://www.eid.as/
13. “REFEDS eduPerson Schema,” https://refeds.org/eduperson
14. “eduPersonAssurance,” https://wiki.refeds.org/pages/viewpage.action?pageId=44957737#eduPerson201602-eduPersonAssurance
15. “Shibboleth IdP Attribute Resolver,” https://wiki.shibboleth.net/confluence/display/IDP4/AttributeResolverConfiguration
16. “Shibboleth IdP Attribute Filter,” https://wiki.shibboleth.net/confluence/display/IDP4/AttributeFilterConfiguration
17. “Microsoft ADFS Create a Rule to Send LDAP Attributes as Claims,” https://docs.microsoft.com/en-us/windows-server/identity/ad-fs/operations/create-a-rule-to-send-ldap-attributes-as-claims
18. “NIH Compliance Login Check,” https://auth.nih.gov/CertAuthV3/forms/compliancecheck.aspx
19. “How to map a user’s identity assurance to REFEDS Assurance Framework,” https://drive.google.com/file/d/14fLqzV8G8Qh9y3D9hl0YkY5i7PilQ7uw/view?usp=sharing
20. Timeline of Events: https://spaces.at.internet2.edu/display/federation/get-nih-ready/#getnihready-WhenDoesAllThisHappen

Appendix C: Risks and Liabilities

An SP relies on a chosen type of identity assurance claim provided via federated access by users’ home organizations as one means to manage exposure to some degree of risk they believe they incur by relying on federated access to their service. What might be the consequences if some identity assurance claims in fact overstate the degree of identity assurance associated with the present user, and who might be impacted by those consequences?

The immediate consequence is that the SP’s risk exposure has not been addressed to the degree they intended. If the SP chooses not to simply accept this underperformance, the courses of action open to them are rather limited. If there is a contract in force between the SP

and the home organization, its terms and conditions may identify the course of action that both parties agree to follow. Otherwise the SP might choose one of the following:

1. They can collegially engage with an implicated home organization to try to correct the situation.
2. They can engage InCommon's help to try to correct the situation with an implicated home organization.
3. They can pursue some form of uncollegial action against the home organization, using whatever standing they have with the home organization as leverage to address the situation.
4. They can replace federated access with another form of user access to their service, either for users at an implicated home organization, or categorically.

A contract is the only way the home organization can be held legally liable for the accuracy of its identity assurance claims. In cases where there is no bilateral contract between the SP and the home organization, the only operative contract is the InCommon Participation Agreement. That obligates Participants to agree to follow InCommon's Dispute Resolution Process when a concern is brought to InCommon regarding the Participant's activity within the federation. The Dispute Resolution Process always brings a resolution to a concern that triggers it. It proceeds by phases, starting with supportive outreach. If the concern is not resolved with a support-oriented engagement, the next phase is to engage CTAB, who will work with the home organization to understand the issue and arrive at a mitigation plan and time frame for its implementation. If that approach fails, CTAB recommends to the InCommon Steering Committee to remove affected entities from the federation, ie, the home organization's IdP in this case.

So, if the SP chooses to formally raise a concern with InCommon about the accuracy of a home organization's identity assurance claims, Incommon will follow the Dispute Resolution Process, which precipitates collaborative work with the home organization to correct the issue, with the worst case scenario being removal of the home organization's IdP from the federation in case collaboration fails.

This essentially addresses the third bullet above. The first bullet reduces the value of federation for users at the affected home organization, or possibly at all home organizations having users of the SP, and it might also impact the reputation of the home organization, albeit in a very narrow and technical manner (it likely won't make headlines in the New York Times).

The second bulleted action is intended to resolve the issue without conflict and consequently without additional risk or liability to either party.

The fourth and last case, being an unknown, carries the potential of worst-case negative impact to the home organization, potentially harming the SP as well. We won't speculate about what the conclusion of this course of action might be, but we do observe that this approach is

exceedingly rare among organizations mutually engaged in the research and scholarship mission.

Returning to consider contracts between the SP and the home organization, it may be that a Data Use Agreement, a Grant Award Contract, or an operational agreement exists between the parties. In such contracts, security obligations are generally incumbent on the party hosting any sensitive data that is subject to the agreement. There are two use cases that may be an exception to this:

- Initial data transfer from the SP to the Home Organization, where it will reside thereafter. In this case, the SP's procedures are necessarily followed in conducting the transfer. Any risk remains theirs.
- The SP hosts the data and authorizes users' federated access to analyze it there. It is possible that this use case is what motivates the SP's reliance on identity assurance in the first place, in which case we're back to the preceding analysis.

Appendix D: Considerations on NIST 800-63-3 Identity Assurance Levels (IALs) and RAF

Many IdPs in the federation work with SPs who are U.S. Federal Government organizations. This section is written to help the IdPs understand Information Security requirements placed on Federal Information Systems and how the RAF fits in. This section will also help Federal Information System owners assess what RAF IAPs might mean and how the RAF might be understood in the context of the system accreditation and authorization in the context of the NIST Risk Management Framework (RMF) specified in NIST SP 800-37 and Federal Information Security Management Act (FISMA) requirements implemented through security control baselines specified in NIST SP 800-53. Supporting these documents is the NIST SP 800-63-3 series, which includes 800-63A on Identity Assurance Levels (IALs), 800-63B on Authentication Assurance Levels (AALs), and 800-63C on Federation Assurance Levels (FALs). This discussion, in the context of RAF, is focused on 800-63-3 (what assurance levels are required based on what is in the information system) and 63A, what each IAL entails.

Federal SPs are guided by 800-63-3; the RAF reference to NIST assurance levels is through the Kantara criteria based on the previous version, NIST 800-63-2. There are two main differences, the first of which is that in 800-63-2, identity, authentication and federation assurance levels were not broken out into discrete aspects of assurance. The second is that 63-2 had four assurance levels (ALs 1 through 4) and 63-3 has three assurance levels. The 800-63-3 levels are not linear (as shown in the Assurance spectrum above), and there is a significant gap between IAL-1 and IAL-2. Practically speaking, the old AL-2 was done away with, the old AL-1 maps to the new IAL-1, but the new IAL-2 is more assured than the old AL-3.

Federal agencies determine the required assurance levels based on the kind of information the Information System (IS) contains. The Information System Owner (ISO) assesses the impact incurred if the information were to suffer a violation of integrity, confidentiality, or availability. Impacts are assessed against the following perspectives: (1) inconvenience, distress or damage to standing reputation; (2) financial loss or agency liability; (3) harm to agency programs or public interests; (4) unauthorized release of sensitive information; (5) personal safety; and (6) civil or criminal violations. Each perspective is assessed at an impact level, according to the guidance, at “none”, “low”, “moderate”, or “high”, as specified in FIPS PUB 199 (describing how to assess impact categories) and NIST 800-60 Vols 1 and 2 (a guide for mapping specific types of information into security categories). A high in any one category “watermarks” the entire system as “high.” Based on this analysis, the Information System Owner knows to select either the FISMA LOW, MODERATE, or HIGH control baselines in NIST 800-53 while developing the System Security Plan to submit to the Authorizing Official for an Authorization to Operate (ATO).

Why is this relevant to non-governmental IdPs? Because many IdPs have members who need to be federated into government ISs (such as those hosted by NIH or NIAID). When a government agency has an IS that is assessed to a LOW impact level, IAL-1 is sufficient for system access. The RAF equivalent would be IAP-LOW.

However, many federal IS’s will be assessed to a MODERATE baseline, which calls for IAL-2. RAF IAP HIGH, which includes Kantara criteria based on the old NIST AL-3, doesn’t quite reach the level of assurance of IAL-2. (The main difference between IAP HIGH and IAL-2 comes down to the number of evidences required in identity proofing, and not requiring biometric comparison to a live photo or video capture for remote proofing.)

If the institution decides to implement IAL-2 directly, the simplest way would be to require in-person proofing with two pieces of “strong” evidence (as defined by NIST 800-63A), which could be two forms of government photo ID prior to issuing a network credential. The check would include an inspection of the person against the photo, and of the card itself to verify a reasonable expectation that the card is not a forgery (*e.g.,* through inspecting anti-tamper methods such as holograms, watermarks, laser etchings, *etc.*,) This check could occur at the campus ID card office, or at the office issuing the credential. Another way is to require a Real-ID compliant photo ID or better, as long the institution can verify the ID with the issuing source. (This verification check with the issuing source on a “strong” evidence precludes the need for a second piece of identity evidence).

If the IdP’s institution decides to use RAF as the means to signal to the federal SP its identity assurance level, then the IdP should achieve and signal IAP HIGH. Whether that is sufficient will depend on the SP’s own risk assessment.

For SPs considering whether IAP HIGH is sufficient to access information assessed at the MODERATE impact level, the ISO’s Authorizing Official will need to determine if the risk delta is acceptable, and if not, what additional compensating controls the SP will require.

Given that IAP HIGH shows a reasonable equivalence between Kantara AL-3 and eIDAS Substantial (EU standards), and the eIDAS is also authoritatively equivalent to NIST in the international arena (in that it grants leeway to each sovereign nation to define how “authoritative” verifications are implemented), it could be seen as reasonable to accept IAP HIGH as close enough to IAL-2 in order to achieve the benefits of federated partnerships based on the particular research or government function provided by the IS. If this is not considered sufficient by the AO, then additional compensating measures could include requiring IdPs to achieve and signal RAF IAP HIGH + RAF LOCAL-ENTERPRISE as an additional assurance. Federal SPs could also implement additional risk mitigation measures in their user registration process. For example, an SP might require an invite-only approach where an IdP’s user needs to be invited in by someone authoritative who already personally knows that person (such as a Principle Investigator requesting access for a team member), in addition to the IdP assertion of RAF HIGH and RAF LOCAL-ENTERPRISE. Ultimately, however, these variables will be subject to the ISO’s Authorizing Official.

On a final note regarding NIST IALs, the RAF IAPs do not achieve IAL-3; it is unlikely that a Federal Agency will grant federated access to any FISMA HIGH system without levying additional identity proofing measures. It is important to remember that RAF IAP HIGH approaches the requirements at FISMA MODERATE (IAL-2), and is not reasonably close to the identity assurance required for FISMA HIGH without additional compensating measures specified by the SP.