Patent Electronic System Access Document

(December 2018)

The **Patent Electronic System Access Document** serves as a source document for additional information on the components for accessing the patent electronic system. Patent Electronic System refers to EFS-Web, PAIR, and Patent Center. This document has four components:

1) Authentication process
2) Sponsorship process
3) Verification Policy and Identity Proofing of Registered Practitioners and Independent Inventors
4) Verification Policy and Identity Proofing of Sponsored Users

Authentication Process

USPTO.gov Accounts and MyUSPTO

The Patent Electronic System uses the United States Patent and Trademark Office's (USPTO) single sign-on (SSO) system, the USPTO.gov account, for secure authentication. USPTO.gov accounts are based on email address, and each account uses the email address as the account name or user ID.

USPTO.gov accounts can be created and managed through the MyUSPTO homepage (http://my.uspto.gov/). The MyUSPTO page allows users to create accounts, change passwords, enable two-step authentication, and record personal information, including alternate email addresses and telephone numbers.

Two-Step Authentication

USPTO.gov accounts can be secured with a two-step authentication. When the two-step authentication is enabled, the user will be presented with a challenge to enter a temporary authentication code after providing a username and password. The user can select delivery of the temporary authentication code either by email, mobile code generator app, or a phone call.

When signing in with the two-step authentication, the user can select a checkbox to indicate that the device being used is a trusted device for that account. If the user selects that the device is trusted, the user will not be presented with a two-step challenge for the next 24 hours.

Signing In and Signing Out

The USPTO.gov account is part of the MyUSPTO single sign-on system. This means that a user only needs to sign in one time to access any of the services protected by MyUSPTO. For example, if a user signs in to Patent Center with their USPTO.gov account, that user will be able to access Financial Manager without signing in a second time. Conversely, signing out from one system will sign the user out from all USPTO systems.

Roles

The following Patent Electronic System roles are assigned by the USPTO as part of the USPTO's proofing process. Users can only have one of the below roles applied to their USPTO.gov account.

Proofed Practitioner	An attorney/agent who has been proofed by the USPTO's proofing process.
Proofed Practitioner Support	A paralegal/practitioner support staff who has been sponsored by a Proofed Practitioner.
Proofed Independent Inventor	An independent (pro se) inventor who has been proofed by the USPTO's proofing process.

Please note that other systems may have roles that can be applied to a USPTO.gov account in addition to one of the above Patent Electronic System roles.

Revocation of Accounts

In some cases, accounts may be revoked. Revoked accounts cannot access the Patent Electronic System. The USPTO may revoke an account for violating the terms of use (e.g., if a user is harming the system or denying access to other users) without prior notice.

Authorization

Signed in users can access private data, which is non-public data related to applications associated with their customer numbers. Proofed Practitioner users can sponsor Practitioner Support Staff. A sponsored support staff individual will have access to the practitioner's private data and will be able to submit correspondence on behalf of the practitioner.

Authentication Steps

In order to use a USPTO.gov account with the Patent Electronic System, the following steps must be performed:

1. Create a USPTO.gov account using MyUSPTO
    a. Prove ownership of the account email address by clicking the verification link in the automated email sent by MyUSPTO
    b. Create a secure password
    c. Record personal information (i.e., telephone number, mailing address, alternate email address)
2. Enable two-step authentication
    a. Two-step authentication is required for the Patent Electronic System, and must be enabled in the MyUSPTO settings for each USPTO.gov account
    b. Two-step authentication is available using:
        i. Email
        ii. Code generator application (e.g., Oracle Mobile Authenticator, Google Authenticator), which must be configured in the MyUSPTO settings
        iii. Automated voice phone call

    c. The account must be permanently opted in to two-step authentication by selecting the "**I want to use the two-step authentication method every time I sign into MyUSPTO.**" checkbox
3. For the USPTO.gov accounts of registered practitioners and independent inventors, the account owner's identity must be proven by completing the Patent Electronic System proofing process. The steps for the proofing process are located at the Getting Started – New Users page at https://www.uspto.gov/patents-application-process/applying-online/getting-started-new-users. Practitioner support staff must be sponsored by a registered practitioner in order to work on behalf of the sponsoring practitioner. Identity proofing of practitioner support staff must be completed by the sponsoring practitioner according to the "Sponsorship Process" section below.
    a. When the proofing process is completed by the USPTO, a Patent Electronic System role will be assigned to the USPTO.gov account
    b. The proofed user will be added to the authorization database, which controls access to customer numbers
    c. Proofed user accounts cannot opt out of two-step authentication
    d. Proofed user accounts cannot change email addresses outside of the proofing process. In order to change the name or email address of the proofed user account, a new notarized form is required.
4. Go to the Patent Electronic System
5. Sign in
    a. The user can sign in from the Patent Electronic System directly or sign in from the MyUSPTO landing page.
        i. The sign in link is displayed in the header at the top of every page.
    b. A signed in user can access their own private data and can perform functions appropriate to their role.
    c. Revocation of Accounts
        i. Revoked accounts that sign in will not be able to access private data or filing functions and an error message will be displayed to the user.
6. Sign out
    a. A signed in user can sign out at any time on any page in the Patent Electronic System or in MyUSPTO
    b. The Patent Electronic System will automatically terminate a user's session after 30 minutes of inactivity. The user will be prompted to continue their session prior to the inactivity timeout.
    c. A user that has signed out immediately loses access to all private data.

Sponsorship Process

The sponsorship tool allows practitioners to grant or remove sponsorship for support staff individuals to work under their direction and control. The support staff individual must have already created a USPTO.gov account and opted into two-step authentication in order to be sponsored by a practitioner. After the sponsorship is complete, the support staff individual will be able to access the Patent Electronic System using their USPTO.gov account. The support staff individual will have access to all applications associated with the customer number(s) of the sponsoring practitioner. The support staff

individual must use their own credentials when accessing the Patent Electronic System and should not use the credentials (e.g., the USPTO.gov account) of the practitioner or any other individual. Each support staff individual must have their own account; accounts may not be shared among support staff.

Practitioner Sponsors Support Staff

1. Practitioner signs into USPTO.gov account
2. Using the Sponsorship Tool, Practitioner selects *Sponsor users.*
3. Practitioner enters the email address of the support staff person's USPTO.gov account.
    a. The entered email address must belong to an existing USPTO.gov user (See section for new Practitioner Support account creation). The sponsored user cannot be in a revoked status, a Patent Practitioner, or Pro Se inventor.
    b. If the email address is not associated with to a USPTO.gov account, the practitioner will receive an error message and have the option to reenter the email address.
    c. The sponsoring Patent Practitioner will review and select Practitioner Support staff from the generated list of potential sponsorships.

Each sponsoring practitioner will establish a procedure for identity proofing sponsored users and maintain a record of that procedure. Each sponsored user must present acceptable evidence of their identity. The ultimate responsibility for verification of the identity of a sponsored user rests upon the sponsoring practitioner. Verification may be performed either in-person or remotely. For further details, please refer to Verification Policy Section of this document.

In the Sponsorship tool, the practitioner selects a checkbox to certify the following:

> By sponsoring users, you acknowledge and agree to the following: The indicated Practitioner Support account(s) will be authorized in a support capacity, to all customer numbers and application information associated with your account, and you grant access through the practitioner support person's own account, to work under your direction and control in the patent electronic filing and viewing system. You are responsible under 37 CFR 11.18 for any actions that are taken under your authority by the practitioner support person using the sponsored practitioner support account. You have read and understand the Subscriber Agreement, and agree to abide by the Subscriber Agreement and the rules and policies of the USPTO regarding the Subscriber Agreement.

The Sponsoring Practitioner confirms that they want to proceed. The sponsorship is established and the support staff will have access to the customer numbers that are associated to the sponsoring practitioner.

Each sponsoring practitioner must take reasonable steps to ensure that the access of each sponsored support staff is consistent with the tasks assigned that individual. Such reasonable steps include removing sponsorship where appropriate, including where the individual leaves the practitioner's organization or the contractor's organization or when the contractor is no longer a contractor to the sponsoring practitioner.

Each sponsored support staff works under the direction and control of the sponsoring practitioner, and is an employee of the sponsoring practitioner's organization or an employee of a contractor of an

organization that is under contract to the sponsoring practitioner or the sponsoring practitioner's organization. If any practitioner who sponsored a support staff ceases practice before the USPTO for any reason, the support staff agrees to cease any access granted from that practitioner.

New Practitioner Support Access to EFS-Web and Private PAIR

1. Create a USPTO.gov account in MyUSPTO and opt into two-step authentication.
2. Ask the practitioner to sponsor. Prove identity to practitioner in accordance with NIST SP 800-63A (Digital Identity Guidelines). Please refer to the Verification Policy and Identity Proofing of Sponsored Users section for more information.
    a. If the practitioner sponsors the practitioner support staff individual, the user will have access to all customer numbers associated to the practitioner.
3. Support Staff are able to submit correspondence and access private data in the Patent Electronic System.

Removing Sponsorships

Sponsorships may be removed by either the practitioner or the support staff.

Proofed Practitioner Removes Sponsorship

1. Using the Sponsorship Tool, the practitioner removes the sponsorship of the practitioner support staff individual.
2. A warning message appears to the practitioner:
   *Are you sure you want to stop sponsoring **[Practitioner Support Account]**? Once removed, **[Practitioner Support Account]** will not be able to work on your behalf.*
3. After practitioner confirms the removal, the practitioner support staff individual will no longer have access to any customer numbers associated to the practitioner's account. The support staff individual may, however, have access to those customer numbers if other practitioners have sponsored that support staff individual and have not removed their sponsorship.

Practitioner Support Removes Sponsorship

1. Using the Sponsorship Tool, the practitioner support staff individual removes the sponsorship of the practitioner support staff individual.
2. A warning message appears to the user
3. After the practitioner support staff individual confirms the removal, the practitioner support staff individual will no longer have access to any customer numbers associated to the practitioner's account via that practitioner. The support staff individual may, however, have access to those customer numbers if other practitioners have sponsored that support staff individual and have not removed their sponsorship. Furthermore, the practitioner support staff individual may no longer access the Patent Electronic System if no other sponsorships exist.

USPTO Removes Sponsorship

The USPTO has the ability to remove access for any accounts (Practitioner, Practitioner Support, Independent Inventor) by marking the account as revoked.

a. Revoked accounts do not have access to EFS-Web Registered, Private PAIR, and Patent Center for Registered users.
b. Practitioner support staff do not have access to the accounts of sponsoring Practitioners who have been revoked.

Verification Policy and Identity Proofing of Registered Practitioners and Independent Inventors

Each registered practitioner or independent inventor is required to undergo an identity proofing and enrollment process whereby their identity evidence and attributes are collected, uniquely resolved to a single identity within a given population or context, then validated and verified. The steps for the proofing process is located at the Getting Started – New Users page at https://www.uspto.gov/patents-application-process/applying-online/getting-started-new-users.

Practitioners and independent inventors who are current PKI certificate holders who migrate using the Migration Tool to link their PKI certificate to their USPTO.gov account will be considered to have met the identity proofing requirements.

When PKI certificates can no longer be obtained, new registered practitioners and independent inventors will need to submit a Patent Electronic System Verification Form (Verification Form).

Verification Policy and Identity Proofing of Sponsored Users

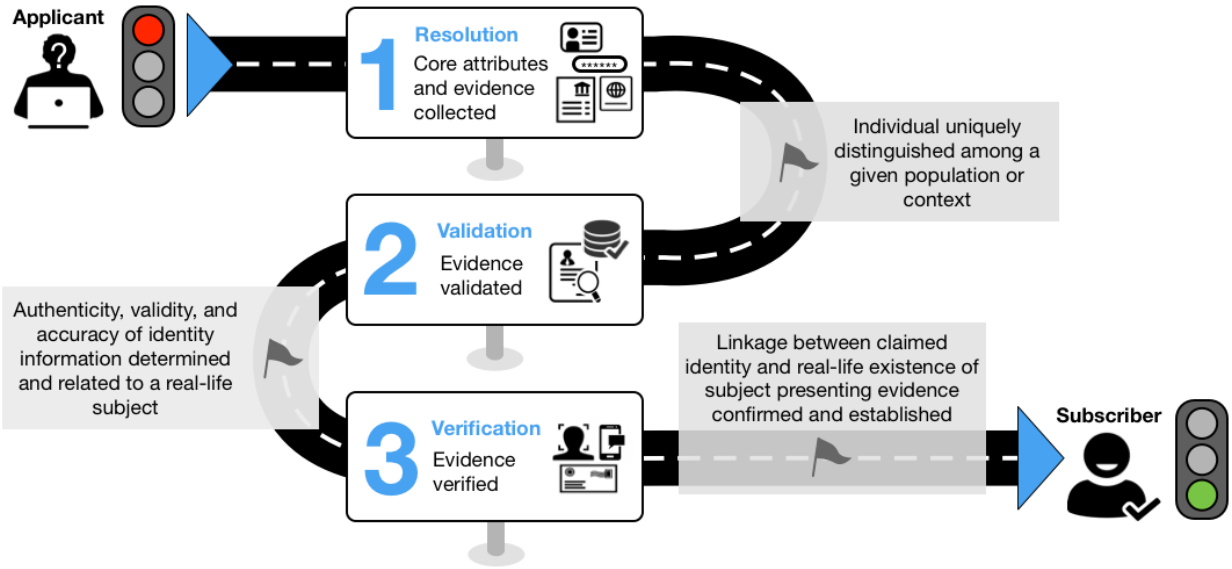
Identity Proofing of Sponsored Support Staff

In accordance with NIST SP 800-63A (Digital Identity Guidelines), the practitioner and their support staff are required to provide identity proof prior to getting access to the systems. The requirements are identified at https://pages.nist.gov/800-63-3/sp800-63a.html. Each practitioner will be responsible for verifying the identity of the person using any sponsored support staff account. Each sponsored support

staff must only be an employee of the practitioner or practitioner's organization, an individual under contract to the practitioner or the practitioner's organization, or an employee of a contractor to the practitioner or the practitioner's organization. A practitioner may only sponsor support staff individuals and may not sponsor organizations, including a company, a group, a client, a practitioner (see 37 C.F.R. 11.1), or an invention promoter (see 37 C.F.R. 4.2(a)), to become users of the Patent Electronic System. Each sponsoring practitioner will only sponsor a reasonable number of support staff to work under the direction of the sponsoring practitioner for which the sponsoring practitioner can maintain proper control.

The sole objective of the identity proofing is to ensure the user of the sponsored support staff account is who they claim to be. The two-step identification provided by the USPTO.gov account and one-time authentication code provides assurance that the user is the owner of that account; however, it is not designed to verify the real-world identity of that user. Verification of the real-world identity of sponsored support staff is the responsibility of the sponsoring practitioner.

The identity verification requirements for accessing USPTO systems are designed in view of the Digital Identity Guidelines created by the National Institute of Standards and Technology for use by government agencies in fulfilling the requirements of the Federal Information Security Management Act of 2002 (FISMA). As explained in the Digital Identity Guidelines, the basic flow for identity proofing is as follows:



Identity proofing has the following purposes:

1. Resolve a claimed identity to a single, unique identity within the context of the population of users the practitioner serves;
2. Validate that all supplied evidence is correct and genuine (e.g., not counterfeit or misappropriated), and that the claimed identity exists in the real world; and
3. Verify that the claimed identity is associated with the real person supplying the identity evidence.

Each sponsoring practitioner will establish a procedure for identity proofing sponsored support staff and maintain a record of that procedure. Each sponsored support staff must present acceptable evidence of

their identity. An example of an acceptable identity proofing process is included at Appendix A, which is merely one example of an acceptable identity proofing process. Practitioners may develop their own identity proofing process so long as it is consistent with the NIST Digital Identity Guidelines, NIST SP 800-63A, available at https://pages.nist.gov/800-63-3/. General guidelines for establishing an identity proofing process are included at Appendix B.

Resolution of Identity. Practitioners must evaluate identity documents at section 5.2.1 of the NIST Digital Identity Guidelines, NIST SP 800-63A, which is replicated in part at Appendix D. For US-based support staff individuals, use of the identity proofing process associated with USCIS Form I-9 would be considered to be consistent with the resolution of identity required by the Digital Identity Guidelines. More information on the USCIS I-9 form is available at https://www.uscis.gov/i-9; a list of acceptable identity documents is provided at Appendix C.

Validation of Identity Evidence and Real World Presence. Once the practitioner obtains the identity evidence, the accuracy, authenticity, and integrity of the evidence and related information is checked against authoritative sources in order to determine that the presented evidence is genuine, authentic, and not a counterfeit, fake, or forgery; contains information that is correct; and contains information that relates to a real-life subject. Acceptable methods for validating identity evidence are set forth at section 5.2.2 of the NIST Digital Identity Guidelines, NIST SP 800-63A.

Verification of Identity. Once the practitioner has obtained and validated identity evidence from the support staff individual, the final step is verification of the real-life existence of the support staff individual. Acceptable methods for verifying identity evidence are set forth at sections 5.3.1 and 5.3.2 of the NIST Digital Identity Guidelines, NIST SP 800-63A.

Appendix A: Example of an Acceptable Identity Proofing Process

The following example is based on the Digital Identity Guidelines, NIST SP 800-63A, Section 4.1, as a sample of the interactions during the identity proofing process. The term "CSP" refers to "credential service provider," which is the role of the practitioner in sponsoring support staff individuals.

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 1a 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, the identification numbers follow standard formats, and that the physical and digital security features are valid.
    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 to take a photo of themselves, with liveness checks, to match 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 practitioner uses the sponsorship tool to associate the applicant with the applicant's USPTO.gov account. 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.

Note: The identity proofing process can be delivered by multiple service providers. It is possible, but not expected, that a single organization, process, technique, or technology will fulfill these process steps.

Appendix B: Guidelines for Procedures for Identity Proofing of Sponsored Support Staff

The general requirements for identity proofing sponsored support staff are as follows:

1. Identity proofing SHALL NOT be performed to determine suitability or entitlement to gain access to services or benefits.
2. Collection of personally identifiable information (PII) SHALL be limited to the minimum necessary to validate the existence of the claimed identity and associate the claimed identity with the support staff providing identity evidence for appropriate identity resolution, validation,

and verification. This MAY include attributes that correlate identity evidence to authoritative sources and to provide Relying Party (RP) with attributes used to make authorization decisions.

3. The practitioner SHALL provide explicit notice to the support staff at the time of collection regarding the purpose for collecting and maintaining a record of the attributes necessary for identity proofing, including whether such attributes are voluntary or mandatory to complete the identity proofing process, and the consequences for not providing the attributes.
4. If practitioner processes attributes for purposes other than identity proofing, authentication, or attribute assertions (collectively "identity service"), related fraud mitigation, or to comply with law or legal process, practitioner SHALL implement measures to maintain predictability and manageability commensurate with the privacy risk arising from the additional processing. Measures MAY include providing clear notice, obtaining subscriber consent, or enabling selective use or disclosure of attributes. When practitioner use consent measures, practitioner SHALL NOT make consent for the additional processing a condition of the identity service.
5. The practitioner SHALL provide mechanisms for redress of support staff individuals' complaints or problems arising from the identity proofing. These mechanisms SHALL be easy for support staff to find and use. The practitioner SHALL assess the mechanisms for their efficacy in achieving resolution of complaints or problems.
6. The identity proofing and enrollment processes SHALL be performed according to an applicable written policy or standard operating procedures that specifies the particular steps taken to verify identities. The standard operating procedures SHALL include control information detailing how the practitioner handles proofing errors that result in a support staff person not being successfully enrolled. For example, the number of retries allowed, proofing alternatives (e.g., in-person if remote fails), or fraud counter-measures when anomalies are detected.
7. The practitioner SHALL maintain a record, including audit logs, of all steps taken to verify the identity of the support staff and SHALL record the types of identity evidence presented in the proofing process. The practitioner shall retain audit logs for a period of 5 years. The practitioner SHALL conduct a risk management process, including assessments of privacy and security risks to determine:
    a. Any steps that it will take to verify the identity of the applicant beyond any mandatory requirements specified herein;
    b. The PII, including any biometrics, images, scans, or other copies of the identity evidence that the practitioner will maintain as a record of identity proofing (Note: specific federal requirements may apply); and
    c. USPTO may request these records and audit logs if there is a necessity as part of a Cybersecurity investigation, and/or an Office of Inspector General Audit.
8. All PII collected as part of the enrollment process SHALL be protected to ensure confidentiality, integrity, and attribution of the information source.
9. The entire proofing transaction, including transactions that involve a third party, SHALL occur over an authenticated protected channel.
10. The practitioner SHOULD obtain additional confidence in identity proofing using fraud mitigation measures (e.g., inspecting geolocation, examining the device characteristics of the applicant, evaluating behavioral characteristics, checking vital statistic repositories such as the Death Master File [DMF], so long as any additional mitigations do not substitute for the mandatory requirements contained herein. In the event the practitioner uses fraud mitigation measures, the practitioner SHALL conduct a privacy risk assessment for these mitigation measures. Such assessments SHALL include any privacy risk mitigations (e.g., risk acceptance or transfer, limited retention, use limitations, notice) or other technological mitigations (e.g., cryptography), and be documented per requirement (item #7) above.

11. In the event a practitioner ceases to conduct identity proofing and enrollment processes, the practitioner SHALL be responsible for fully disposing of or destroying any sensitive data including PII, or its protection from unauthorized access for the duration of retention.
12. The practitioner SHOULD NOT collect the Social Security Number (SSN) unless it is necessary for performing identity resolution, and identity resolution cannot be accomplished by collection of another attribute or combination of attributes.

Appendix C: Acceptable Documents for Use in Resolving the Identity of US-Based Sponsored Support Staff

The following is a list of acceptable documents that may be used in resolving the identity of sponsored support staff residing in the United States. All documents must be unexpired. Support staff individuals may present **one selection from List A or a combination of one selection from List B and one selection from List C**. Rather than selecting documents from this list, other documents may be presented so long as they are in accordance with the NIST Digital Identity Guidelines (see Appendix D).

LIST A DOCUMENTS THAT ESTABLISH <u>BOTH</u> IDENTITY AND EMPLOYMENT AUTHORIZATION	LIST B DOCUMENTS THAT ESTABLISH IDENTITY	LIST C DOCUMENTS THAT ESTABLISH EMPLOYMENT AUTHORIZATION
1. U.S. Passport or U.S. Passport Card	1. Driver's license or ID card issued by a State or outlying possession of the United States provided it contains a photograph or information such as name, date of birth, gender, height, eye color, and address	**1.** A Social Security Account Number card, unless the card includes one of the following restrictions: (1) NOT VALID FOR EMPLOYMENT (2) VALID FOR WORK ONLY WITH INS AUTHORIZATION (3) VALID FOR WORK ONLY WITH DHS AUTHORIZATION
2. Permanent Resident Card or Alien Registration Receipt Card (Form I-551)	2. ID card issued by federal, state or local government agencies or entities, provided it contains a photograph or information such as name, date of birth, gender, height, eye color, and address	**2.** Certification of report of birth issued by the Department of State (Forms DS-1350, FS-545, FS-240)
3. Foreign passport that contains a temporary I-551 stamp or temporary I-551 printed notation on a machine- readable immigrant visa	3. School ID card with a photograph	**3.** Original or certified copy of birth certificate issued by a State, county, municipal authority, or territory of the United States bearing an official seal
4. Employment Authorization Document that contains a photograph (Form I-766)	4. Voter's registration card	4. Native American tribal document
5. For a nonimmigrant alien authorized to work for a specific employer because of his or her status: a. Foreign passport; and b. Form I-94 or Form I-94A that has the following: (1) The same name as the passport; and (2) An endorsement of the alien's nonimmigrant status as long as that period of endorsement has not yet expired and the proposed employment is not in conflict with any restrictions or limitations identified on the form.	5. U.S. Military card or draft record	5. U.S. Citizen ID Card (Form I-197)

6. Passport from the Federated States of Micronesia (FSM) or the Republic of the Marshall Islands (RMI) with Form I-94 or Form I-94A indicating nonimmigrant admission under the Compact of Free Association Between the United States and the FSM or RMI	6. Military dependent's ID card	6. Identification Card for Use of Resident Citizen in the United States (Form I-179)
	7. U.S. Coast Guard Merchant Mariner Card	
	8. Native American tribal document	
	9. Driver's license issued by a Canadian government authority	

Appendix D: Acceptable Documents for Use in Resolving the Identity of Sponsored Support Staff

The general requirements for collection of identity evidence of sponsored support staff are set forth in this section, which is based upon Section 5.2.1 of the NIST Digital Identity Guidelines, NIST SP 800-63A, available at https://pages.nist.gov/800-63-3/.

The support staff individual must present to the sponsoring practitioner:

- One piece of SUPERIOR or STRONG evidence depending on strength of original proof and validation occurs with issuing source, **OR**
- Two pieces of STRONG evidence, **OR**
- One piece of STRONG evidence plus two (2) pieces of FAIR evidence.

Strength	Qualities of Identity Evidence
Unacceptable	No acceptable identity evidence provided.
Weak	• The issuing source of the evidence did not perform identity proofing. • The issuing process for the evidence means that it can reasonably be assumed to have been delivered into the possession of the applicant. • The evidence contains: o At least one reference number that uniquely identifies itself or the person to whom it relates, **OR** o The issued identity evidence contains a photograph or biometric template (of any modality) of the person to whom it relates.
Fair	• The issuing source of the evidence confirmed the claimed identity through an identity proofing process. • The issuing process for the evidence means that it can reasonably be assumed to have been delivered into the possession of the person to whom it relates. • The evidence: o Contains at least one reference number that uniquely identifies the person to whom it relates, **OR** o Contains a photograph or biometric template (any modality) of the person to whom it relates, **OR**

	○ Can have ownership confirmed through Knowledge Based Verification. • Where the evidence includes digital information, that information is protected using approved cryptographic or proprietary methods, or both, and those methods ensure the integrity of the information and enable the authenticity of the claimed issuing source to be confirmed. • Where the evidence includes physical security features, it requires proprietary knowledge to be able to reproduce it. • The issued evidence is unexpired.
Strong	• The issuing source of the evidence confirmed the claimed identity through written procedures designed to enable it to form a reasonable belief that it knows the real-life identity of the person. Such procedures are subject to recurring oversight by regulatory or publicly-accountable institutions. For example, the Customer Identification Program guidelines established in response to the USA PATRIOT Act of 2001 or the Red Flags Rule, under Section 114 of the Fair and Accurate Credit Transaction Act of 2003 (FACT Act). • The issuing process for the evidence ensured that it was delivered into the possession of the subject to whom it relates. • The issued evidence contains at least one reference number that uniquely identifies the person to whom it relates. • The full name on the issued evidence must be the name that the person was officially known by at the time of issuance. Not permitted are pseudonyms, aliases, an initial for surname, or initials for all given names. • The: ○ Issued evidence contains a photograph or biometric template (of any modality) of the person to whom it relates, OR ○ Applicant proves possession of an AAL2 authenticator, or equivalent, bound to an IAL2 identity, at a minimum. • Where the issued evidence includes digital information, that information is protected using approved cryptographic or proprietary methods, or both, and those methods ensure the integrity of the information and enable the authenticity of the claimed issuing source to be confirmed. • Where the issued evidence contains physical security features, it requires proprietary knowledge and proprietary technologies to be able to reproduce it. • The evidence is unexpired.
Superior	• The issuing source of the evidence confirmed the claimed identity by following written procedures designed to enable it to have high confidence that the source knows the real-life identity of the subject. Such procedures are subject to recurring oversight by regulatory or publicly accountable institutions. • The issuing source visually identified the applicant and performed further checks to confirm the existence of that person. • The issuing process for the evidence ensured that it was delivered into the possession of the person to whom it relates. • The evidence contains at least one reference number that uniquely identifies the person to whom it relates. • The full name on the evidence must be the name that the person was officially known by at the time of issuance. Not permitted are pseudonyms, aliases, an initial for surname, or initials for all given names.

	• The evidence contains a photograph of the person to whom it relates. • The evidence contains a biometric template (of any modality) of the person to whom it relates. • The evidence includes digital information, the information is protected using approved cryptographic or proprietary methods, or both, and those methods ensure the integrity of the information and enable the authenticity of the issuing source to be confirmed. • The evidence includes physical security features that require proprietary knowledge and proprietary technologies to be able to reproduce it. • The evidence is unexpired.