#	*QUESTION*	*YES*	*NO*	*N/A*	*STANDARD*	*COMMENT*
5.6	**Identification and Authentication (IA)[1]**					
1.	Has the Tribe or TGRA developed, documented, and disseminated to all authorized personnel an agency-level identification and authentication policy that: • Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance? • Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines?	____	____	____	IA-1, a.1.(a) IA-1, a.1.(b)	
2.	Has the Tribe or TGRA developed, documented, and disseminated to all authorized personnel procedures to facilitate the implementation of the identification and authentication policy and the associated identification and authentication controls?	____	____	____	IA-1, a.2	
3.	Based on inquiry and record examination, has the Tribe or TGRA designated organizational personnel with security responsibilities to manage the development, documentation, and dissemination of the identification and authentication policy and procedures?	____	____	____	IA-1, b	
4.	Based on inquiry and record examination, does the Tribe or TGRA review and update the current identification and authentication: • Policy annually and following any security incidents involving unauthorized access to Criminal Justice Information (CJI) / Criminal History Record Information (CHRI) or systems used to process, store, or transmit CJI / CHRI? • Procedures annually and following any security incidents involving unauthorized access to CJI / CHRI or systems used to process, store, or transmit CJI / CHRI?	____ ____	____ ____	____ ____	IA-1, c.1 IA-1, c.2	

[1] These requirements are sanctionable for audit beginning October 1, 2024.

#	*QUESTION*	*YES*	*NO*	*N/A*	*STANDARD*	*COMMENT*
5.	Does the Tribe or TGRA uniquely identify and authenticate organizational users and associate that unique identification with processes acting on behalf of those users?	____	____	____	IA-2	
6.	Based on inquiry and record examination, has the Tribe or TGRA implemented multi-factor authentication for access to privileged accounts?	____	____	____	IA-2, (1)	
7.	Based on inquiry and record examination, has the Tribe or TGRA implemented multi-factor authentication for access to non-privileged accounts?	____	____	____	IA-2, (2)	
8.	Based on inquiry and record examination has the Tribe or TGRA implemented replay-resistant[2] authentication mechanisms for access to privileged and non- privileged accounts?	____	____	____	IA-2, (8)	
9.	Based on inquiry and record examination, does the Tribe or TGRA accept and electronically verify Personal Identity Verification (PIV)-compliant credentials[3]?	____	____	____	IA-2, (12)	
10.	Based on inquiry and record examination, does the Tribe or TGRA uniquely identify and authenticate agency-managed devices before establishing network connections? In the instance of local connection, the device must be approved by the TGRA and the device must be identified and authenticated prior to connection to a TGRA asset.	____	____	____	IA-3	

[2] Replay-resistant techniques include protocols that use nonces or challenges such as time synchronous or cryptographic authenticators.

[3] Acceptance of Personal Identity Verification (PIV)-compliant credentials applies to organizations implementing logical access control and physical access control systems. PIV-compliant credentials are those credentials issued by federal agencies that conform to FIPS Publication 201 and supporting guidance documents. The adequacy and reliability of PIV card issuers are authorized using [SP 800-79-2]. Acceptance of PIV-compliant credentials includes derived PIV credentials, the use of which is addressed in [SP 800-166]. The DOD Common Access Card (CAC) is an example of a PIV credential.

#	*QUESTION*	*YES*	*NO*	*N/A*	*STANDARD*	*COMMENT*
11.	Based on inquiry and record examination, does the Tribe or TGRA manage system identifiers by:					
	• Receiving authorization from organizational personnel with identifier management responsibilities to assign an individual, group, role, service, or device identifier?	____	____	____	IA-4, a	
	• Selecting an identifier that identifies an individual, group, role, service, or device?	____	____	____	IA-4, b	
	• Assigning the identifier to the intended individual, group, role, service, or device?	____	____	____	IA-4, c	
	• Preventing reuse of identifiers for one (1) year?	____	____	____	IA-4, d	
12.	Based on inquiry and record examination, does the Tribe or TGRA manage individual identifiers by uniquely identifying each individual as agency or nonagency?	____	____	____	IA-4, (4)	
13.	Based on inquiry and record examination, does the Tribe or TGRA manage system authenticators by:					
	• Verifying, as part of the initial authenticator distribution, the identity of the individual, group, role, service, or device receiving the authenticator?	____	____	____	IA-5, a	
	• Establishing initial authenticator content for any authenticators issued by the organization?	____	____	____	IA-5, b	
	• Ensuring that authenticators have sufficient strength of mechanism for their intended use?	____	____	____	IA-5, c	
	• Establishing and implementing administrative procedures for initial authenticator distribution, for lost or compromised or damaged authenticators, and for revoking authenticators?	____	____	____	IA-5, d	
	• Changing default authenticators prior to first use?	____	____	____	IA-5, e	
	• Changing or refreshing authenticators annually or when there is evidence of authenticator compromise?	____	____	____	IA-5, f	
	• Protecting authenticator content from unauthorized disclosure and modification?	____	____	____	IA-5, g	

#	*QUESTION*	*YES*	*NO*	*N/A*	*STANDARD*	*COMMENT*
	• Requiring individuals to take, and having devices implement, specific controls to protect authenticators?	____	____	____	IA-5, h	
	• Changing authenticators for group or role accounts when membership to those accounts changes?	____	____	____	IA-5, i	
	• Ensuring the following Authenticator Assurance Level 2 (AAL2) Specific Requirements:					
	o Authentication occurs by the use of either a multi-factor authenticator or a combination of two single-factor authenticators?	____	____	____	IA-5, j (1)	
	o If the multi-factor authentication process uses a combination of two single-factor authenticators, then it includes a Memorized Secret authenticator and a possession-based authenticator?	____	____	____	IA-5, j (2)	
	o Cryptographic authenticators used at AAL2 use approved cryptography?	____	____	____	IA-5, j (3)	
	o At least one authenticator used at AAL2 is replay resistant?	____	____	____	IA-5, j (4)	
	o Communication between the claimant and verifier is via an authenticated protected channel?	____	____	____	IA-5, j (5)	
	o Verifiers operated by government agencies at AAL2 are validated to meet the requirements of Federal Information Processing Standard (FIPS) 140 Level 1?	____	____	____	IA-5, j (6)	
	o Authenticators procured by government agencies are validated to meet the requirements of FIPS 140 Level 1?	____	____	____	IA-5, j (7)	
	o If a device such as a smartphone is used in the authentication process, then the unlocking of that device (typically done using a Personal Identification Number (PIN) or biometric) is NOT considered one of the authentication factors?	____	____	____	IA-5, j (8)	
	o If a biometric factor is used in authentication at AAL2, then the performance requirements stated					

#	QUESTION	YES	NO	N/A	STANDARD	COMMENT
	in IA-5 m Biometric Requirements are met?	____	____	____	IA-5, j (9)	
	○ Reauthentication of the subscriber is repeated at least once per 12 hours during an extended usage session?	____	____	____	IA-5, j (10)	
	○ Reauthentication of the subscriber is repeated following any period of inactivity lasting 30 minutes or longer?	____	____	____	IA-5, j (11)	
	○ The Credential Service Provider (CSP) employs appropriately tailored security controls from the moderate baseline of security controls defined in the CJISSECPOL?	____	____	____	IA-5, j (12)	
	○ The CSP ensures that the minimum assurance-related controls for moderate-impact systems are satisfied?	____	____	____	IA-5, j (12)	
	○ The CSP complies with records retention policies in accordance with applicable laws and regulations?	____	____	____	IA-5, j (13)	
	○ If the CSP opts to retain records in the absence of any mandatory requirements, then the CSP conducts a risk management process, including assessments of privacy and security risks to determine how long records should be retained and informs subscribers of that retention policy?	____	____	____	IA-5, j (14)	
	• Verifying privacy requirements that apply to all CSPs, verifiers, and Relying Partys (RP) as follows:					
	○ The CSP employs appropriately tailored privacy controls from the CJISSECPOL?	____	____	____	IA-5, k (1)	
	○ If the CSP 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, then the CSP					

#	QUESTION	YES	NO	N/A	STANDARD	COMMENT
	implements measures to maintain predictability and manageability commensurate with the associated privacy risk?	____	____	____	IA-5, k (2)	
	• Confirming the following general requirements applicable to AAL2 authentication process:					
	○ CSPs provide subscriber instructions on how to appropriately protect a physical authenticator against theft or loss?	____	____	____	IA-5, l (1)	
	○ The CSP provides a mechanism to revoke or suspend the authenticator immediately upon notification from subscriber that loss or theft of the authenticator is suspected?	____	____	____	IA-5, l (2)	
	○ If required by the authenticator type descriptions in IA-5(1), then the verifier implements controls to protect against online guessing attacks?	____	____	____	IA-5, l (3)	
	○ If required by the authenticator type descriptions in IA-5(1) and the description of a given authenticator does not specify otherwise, then the verifier limits consecutive failed authentication attempts on a single account to no more than 100?	____	____	____	IA-5, l (4)	
	○ If signed attestations are used, then they are signed using a digital signature that provides at least the minimum security strength specified in the latest revision of 112 bits as of the date of this publication (9/14/2023)?	____	____	____	IA-5, 1 (5)	
	○ If the verifier and CSP are separate entities (as shown by the dotted line in Figure 7 Digital Identity Model), then communications between the verifier and CSP occur through a mutually-authenticated secure channel (such as a client-authenticated Transport Layer Security (TLS) connection)?	____	____	____	IA-5, l (6)	

#	QUESTION	YES	NO	N/A	STANDARD	COMMENT
	○ If the CSP provides the subscriber with a means to report loss, theft, or damage to an authenticator using a backup or alternate authenticator, then that authenticator is either a memorized secret or a physical authenticator?	____	____	____	IA-5, 1 (7)	
	○ If the CSP chooses to verify an address of record (i.e., email, telephone, postal) and suspend authenticator(s) reported to have been compromised, then...The suspension is reversible if the subscriber successfully authenticates to the CSP using a valid (i.e., not suspended) authenticator and requests reactivation of an authenticator suspended in this manner?	____	____	____	IA-5, 1 (8)	
	○ If and when an authenticator expires, it is NOT usable for authentication?	____	____	____	IA-5, 1 (9)	
	○ The CSP has a documented process to require subscribers to surrender or report the loss of any physical authenticator containing attribute certificates signed by the CSP as soon as practical after expiration or receipt of a renewed authenticator?	____	____	____	IA-5, 1 (10)	
	○ CSPs revoke the binding of authenticators immediately upon notification when an online identity ceases to exist (e.g., subscriber's death, discovery of a fraudulent subscriber), when requested by the subscriber, or when the CSP determines that the subscriber no longer meets its eligibility requirements?	____	____	____	IA-5, 1 (11)	
	○ The CSP has a documented process to require subscribers to surrender or report the loss of any physical authenticator containing certified attributes signed by the CSP within five (5) days after					

#	QUESTION	YES	NO	N/A	STANDARD	COMMENT
	revocation or termination takes place?	____	____	____	IA-5, l (12)	
	• Verifying the following biometric requirements:					
	o Biometrics are used only as part of multi-factor authentication with a physical authenticator (something you have)?	____	____	____	IA-5, m (1)	
	o An authenticated protected channel between sensor (or an endpoint containing a sensor that resists sensor replacement) and verifier is established?	____	____	____	IA-5, m (2)	
	o The sensor or endpoint is authenticated prior to capturing the biometric sample from the claimant?	____	____	____	IA-5, m (3)	
	o The biometric system operates with a False Match Rate (FMR) [ISO/IEC 2382-37] of 1 in 1000 or better. This FMR is achieved under conditions of a conformant attack (i.e., zero-effort impostor attempt) as defined in [ISO/IEC 30107-1]?	____	____	____	IA-5, m (4)	
	o The biometric system allows no more than 5 consecutive failed authentication attempts or 10 consecutive failed attempts if the presentation attack detection (PAD) demonstrating at least 90% resistance to presentation attacks is implemented?	____	____	____	IA-5, m (5)	
	o Once the limit on authentication failures has been reached, the biometric authenticator either:					
	▪ Imposes a delay of at least 30 seconds before the next attempt, increasing exponentially with each successive attempt?	____	____	____	IA-5, m (6) i	
	▪ Disables the biometric user authentication and offers another factor (e.g., a different biometric modality or a PIN/Passcode if it is not					

#	QUESTION	YES	NO	N/A	STANDARD	COMMENT
	already a required factor) if such an alternative method is already available?	____	____	____	IA-5, m (6) ii	
	○ The verifier makes a determination of sensor and endpoint performance, integrity, and authenticity?	____	____	____	IA-5, m (7)	
	○ If biometric comparison is performed centrally, then use of the biometric as an authentication factor is limited to one or more specific devices that are identified using approved cryptography?	____	____	____	IA-5, m (8)	
	○ If biometric comparison is performed centrally, then a separate key is used for identifying the device?	____	____	____	IA-5, m (9)	
	○ If biometric comparison is performed centrally, then biometric revocation, referred to as biometric template protection in ISO/IEC 24745, is implemented?	____	____	____	IA-5, m (10)	
	○ If biometric comparison is performed centrally, all transmission of biometrics are over the authenticated protected channel?	____	____	____	IA-5, m (11)	
	○ Biometric samples and any biometric data derived from the biometric sample such as a probe produced through signal processing are zeroized immediately after any training or research data has been derived?	____	____	____	IA-5, m (12)	
	• Confirming authenticator binding refers to the establishment of an association between a specific authenticator and a subscriber's account, enabling the authenticator to be used — possibly in conjunction with other authenticators — to authenticate for that account as follows:					
	○ Authenticators are bound to subscriber accounts by either issuance by the CSP as part of enrollment or associating a					

#	QUESTION	YES	NO	N/A	STANDARD	COMMENT
	subscriber-provided authenticator that is acceptable to the CSP?	____	____	____	IA-5, n (1)	
	o Throughout the digital identity lifecycle, CSPs maintain a record of all authenticators that are or have been associated with each identity?	____	____	____	IA-5, n (2)	
	o The CSP or verifier maintain the information required for throttling authentication attempts?	____	____	____	IA-5, n (3)	
	o The CSP also verifies the type of user-provided authenticator so verifiers can determine compliance with requirements at each AAL?	____	____	____	IA-5, n (4)	
	o The record created by the CSP contains the date and time the authenticator was bound to the account?	____	____	____	IA-5, n (5)	
	o When any new authenticator is bound to a subscriber account, the CSP ensures that the binding protocol and the protocol for provisioning the associated key(s) are done at AAL2?	____	____	____	IA-5, n (6)	
	o Protocols for key provisioning use authenticated protected channels or are performed in person to protect against Man in the Middle (MitM) attacks?	____	____	____	IA-5, n (7)	
	o Binding of multi-factor authenticators requires multi-factor authentication (or equivalent) at identity proofing?	____	____	____	IA-5, n (8)	
	o At enrollment, the CSP binds at least one, and SHOULD bind at least two, physical (something you have) authenticators to the subscriber's online identity, in addition to a memorized secret or one or more biometrics?	____	____	____	IA-5, n (9)	
	o At enrollment, authenticators at AAL2 and IAL2 are bound to the account?	____	____	____	IA-5, n (10)	
	o If enrollment and binding are being done remotely and cannot be completed in a single electronic transaction, then the applicant					

#	QUESTION	YES	NO	N/A	STANDARD	COMMENT
	identifies themselves in each new binding transaction by presenting a temporary secret which was either established during a prior transaction, or sent to the applicant's phone number, email address, or postal address of record?	____	____	____	IA-5, n (11)	
	o If enrollment and binding are being done remotely and cannot be completed in a single electronic transaction, then long-term authenticator secrets are delivered to the applicant within a protected session?	____	____	____	IA-5, n (12)	
	o If enrollment and binding are being done in person and cannot be completed in a single physical encounter, the applicant identifies themselves in person by either using a secret as described in IA-5 n (12), or through use of a biometric that was recorded during a prior encounter?	____	____	____	IA-5, n (13)	
	o If enrollment and binding are being done in person and cannot be completed in a single physical encounter, temporary secrets are NOT be reused?	____	____	____	IA-5, n (14)	
	o If enrollment and binding are being done in person and cannot be completed in a single physical encounter and the CSP issues long-term authenticator secrets during a physical transaction, they are loaded locally onto a physical device that is issued in person to the applicant or delivered in a manner that confirms the address of record?	____	____	____	IA-5, n (15)	
	o Before adding a new authenticator to a subscriber's account, the CSP first requires the subscriber to authenticate at AAL2 (or a higher AAL) at which the new authenticator will be used?	____	____	____	IA-5, n (16)	
	o If the subscriber's account has only one authentication factor					

#	QUESTION	YES	NO	N/A	STANDARD	COMMENT
	bound to it, the CSP requires the subscriber to authenticate at AAL1 in order to bind an additional authenticator of a different authentication factor? o If a subscriber loses all authenticators of a factor necessary to complete multi-factor authentication and has been identity proofed at IAL2, that subscriber repeats the identity proofing process described in IA-12? o If a subscriber loses all authenticators of a factor necessary to complete multi-factor authentication and has been identity proofed at IAL2 or IAL3, the CSP requires the claimant to authenticate using an authenticator of the remaining factor, if any, to confirm binding to the existing identity? o If the CSP opts to allow binding of a new memorized secret with the use of two physical authenticators, then it requires entry of a confirmation code sent to an address of record? o If the CSP opts to allow binding of a new memorized secret with the use of two physical authenticators, then the confirmation code consists of at least 6 random alphanumeric characters generated by an approved random bit generator [SP 800-90Ar1]? o If the CSP opts to allow binding of a new memorized secret with the use of two physical authenticators, then the confirmation code is valid for a maximum of 7 days but MAY be made valid up to 21 days via an exception process to accommodate addresses outside the direct reach of the U.S. Postal	____ ____ ____ ____ ____	____ ____ ____ ____ ____	____ ____ ____ ____ ____	IA-5, n (17) IA-5, n (18) IA-5, n (19) IA-5, n (20) IA-5, n (21)	

#	QUESTION	YES	NO	N/A	STANDARD	COMMENT
	Service. Confirmation codes sent by means other than physical mail are valid for a maximum of 5 minutes?	____	____	____	IA-5, n (22)	
	• Verifying session management: The following requirements apply to applications where a session is maintained between the subscriber and relying party to allow multiple interactions without repeating the authentication event each time.					
	○ Session Binding Requirements: A session occurs between the software that a subscriber is running — such as a browser, application, or operating system (i.e., the session subject) — and the RP or CSP that the subscriber is accessing (i.e., the session host).					
	▪ A session is maintained by a session secret which is shared between the subscriber's software and the service being accessed?	____	____	____	IA-5, o (1)a	
	▪ The secret is presented directly by the subscriber's software or possession of the secret is proven using a cryptographic mechanism?	____	____	____	IA-5, o (1)b	
	▪ The secret used for session binding is generated by the session host in direct response to an authentication event?	____	____	____	IA-5, o (1) c	
	▪ A session is NOT considered at a higher AAL than the authentication event?	____	____	____	IA-5, o (1) d	
	▪ Secrets used for session binding are generated by the session host during an interaction, typically immediately following authentication?	____	____	____	IA-5, o (1) e	
	▪ Secrets used for session binding are generated by					

#	QUESTION	YES	NO	N/A	STANDARD	COMMENT
	an approved random bit generator [SP 800-90Ar1]?	____	____	____	IA-5, o (1) f	
	▪ Secrets used for session binding contain at least 64 bits of entropy?	____	____	____	IA-5, o (1) g	
	▪ Secrets used for session binding are erased or invalidated by the session subject when the subscriber logs out?	____	____	____	IA-5, o (1) h	
	▪ Secrets used for session binding are sent to and received from the device using an authenticated protected channel?	____	____	____	IA-5, o (1) i	
	▪ Secrets used for session binding time out and are not accepted after the times specified in IA-5 j (13) as appropriate for the AAL?	____	____	____	IA-5, o (1) j	
	▪ Secrets used for session binding are NOT available to insecure communications between the host and subscriber's endpoint?	____	____	____	IA-5, o (1) k	
	▪ Authenticated sessions do NOT fall back to an insecure transport, such as from https to http, following authentication?	____	____	____	IA-5, o (1) l	
	▪ URLs or POST content contain a session identifier that is verified by the RP to ensure that actions taken outside the session do not affect the protected session?	____	____	____	IA-5, o (1) m	
	▪ Browser cookies are tagged to be accessible only on secure (HTTPS) sessions?	____	____	____	IA-5, o (1) n	
	▪ Browser cookies are accessible to the minimum practical set of hostnames and paths?	____	____	____	IA-5, o (1) o	

#	QUESTION	YES	NO	N/A	STANDARD	COMMENT
	▪ Expiration of browser cookies is NOT depended upon to enforce session timeouts?	____	____	____	IA-5, o (1) p	
	▪ The presence of an OAuth access token is NOT interpreted by the RP as presence of the subscriber, in the absence of other signals?	____	____	____	IA-5, o (1) q	
	o Reauthentication Requirements					
	▪ Continuity of authenticated sessions is based upon the possession of a session secret issued by the verifier at the time of authentication and optionally refreshed during the session?	____	____	____	IA-5, o (2) a	
	▪ Session secrets are non-persistent, i.e., they are NOT retained across a restart of the associated application or a reboot of the host device?	____	____	____	IA-5, o (2) b	
	▪ Periodic reauthentication of sessions (at least every 12 hours per session) are performed to confirm the continued presence of the subscriber at an authenticated session?	____	____	____	IA-5, o (2) c	
	▪ A session is NOT extended past the guidelines in IA-5 o (2) a – j based on presentation of the session secret alone?	____	____	____	IA-5, o (2) d	
	▪ Prior to session expiration, the reauthentication time limit is extended by prompting the subscriber for the authentication factor(s) of a memorized secret or biometric[4]?	____	____	____	IA-5, o (2) e	

[4] At AAL2, a memorized secret or biometric, and not a physical authenticator, is required because the session secret is something you have, and an additional authentication factor is required to continue the session.

#	QUESTION	YES	NO	N/A	STANDARD	COMMENT
	▪ If federated authentication is being used, then since the CSP and RP often employ separate session management technologies, there is NOT any assumption of correlation between these sessions?	____	____	____	IA-5, o (2) f	
	▪ An RP requiring reauthentication through a federation protocol — if possible within the protocol — specifies the maximum (see IA-5 j [10]) acceptable authentication age to the CSP?	____	____	____	IA-5, o (2) g	
	▪ If federated authentication if being used and an RP has specific authentication age (see IA-5 j [10]) requirements that it has communicated to the CSP, then the CSP reauthenticates the subscriber if they have not been authenticated within that time period?	____	____	____	IA-5, o (2) h	
	▪ If federated authentication is being used, the CSP communicates the authentication event time to the RP to allow the RP to decide if the assertion is sufficient for reauthentication and to determine the time for the next reauthentication event?	____	____	____	IA-5, o (2) i	
14.	Based on inquiry and record examination, does the Tribe or TGRA:					
	• Maintain a list of commonly-used, expected, or compromised passwords and update the list quarterly and when organizational passwords are suspected to have been compromised directly or indirectly?	____	____	____	IA-5, (1)(a)1	

#	*QUESTION*	*YES*	*NO*	*N/A*	*STANDARD*	*COMMENT*
	• Require immediate selection of a new password upon account recovery?	____	____	____	IA-5, (1)(a)2	
	• Allow user selection of long passwords and passphrases, including spaces and all printable characters?	____	____	____	IA-5, (1)(a)3	
	• Employ automated tools to assist the user in selecting strong password authenticators?	____	____	____	IA-5, (1)(a)4	
	• Enforce the following composition and complexity rules when agencies elect to follow basic password standards:					
	o Not be a proper name?	____	____	____	IA-5, (1)(a)5(a)	
	o Not be the same as the User ID?	____	____	____	IA-5, (1)(a)5(b)	
	o Expire within a maximum of 90 calendar days?	____	____	____	IA-5, (1)(a)5(c)	
	o Not be identical to the previous ten (10) passwords?	____	____	____	IA-5, (1)(a)5(d)	
	o Not be displayed when entered?	____	____	____	IA-5, (1)(a)5(e)	
	• If chosen by the subscriber, memorized secrets are at least 8 characters in length?	____	____	____	IA-5, (1)(a)6	
	• If chosen by the CSP or verifier using an approved random number generator, memorized secrets are at least 6 characters in length?	____	____	____	IA-5, (1)(a)7	
	• Truncation of the secret is NOT be performed?	____	____	____	IA-5, (1)(a)8	
	• Memorized secret verifiers do NOT permit the subscriber to store a "hint" that is accessible to an unauthenticated claimant?	____	____	____	IA-5, (1)(a)9	
	• Verifiers do NOT prompt subscribers to use specific types of information (e.g., "What was the name of your first pet?") when choosing memorized secrets?	____	____	____	IA-5, (1)(a)10	
	• When processing requests to establish and change memorized secrets, verifiers compare the prospective secrets against a list that contains values known to be commonly used, expected, or compromised?	____	____	____	IA-5, (1)(a)11	
	• If a chosen secret is found in the list, the CSP or verifier advises the subscriber that they need to select a different secret?	____	____	____	IA-5, (1)(a)12	
	• If a chosen secret is found in the list, the CSP or verifier provides the reason for rejection?	____	____	____	IA-5, (1)(a)13	

#	*QUESTION*	*YES*	*NO*	*N/A*	*STANDARD*	*COMMENT*
	• If a chosen secret is found in the list, the CSP or verifier requires the subscriber to choose a different value?	____	____	____	IA-5, (1)(a)14	
	• Verifiers implement a rate-limiting mechanism that effectively limits failed authentication attempts that can be made on the subscriber's account to no more than five?	____	____	____	IA-5, (1)(a)15	
	• Verifiers force a change of memorized secret if there is evidence of compromise of the authenticator?	____	____	____	IA-5, (1)(a)16	
	• The verifier uses approved encryption when requesting memorized secrets in order to provide resistance to eavesdropping and MitM attacks?	____	____	____	IA-5, (1)(a)17	
	• The verifier uses an authenticated protected channel when requesting memorized secrets in order to provide resistance to eavesdropping and MitM attacks?	____	____	____	IA-5, (1)(a)18	
	• Verifiers store memorized secrets in a form that is resistant to offline attacks?	____	____	____	IA-5, (1)(a)19	
	• Memorized secrets are salted and hashed using a suitable one-way key derivation function?	____	____	____	IA-5, (1)(a)20	
	• The salt is at least 32 bits in length and be chosen arbitrarily to minimize salt value collisions among stored hashes?	____	____	____	IA-5, (1)(a)21	
	• Both the salt value and the resulting hash is stored for each subscriber using a memorized secret authenticator?	____	____	____	IA-5, (1)(a)22	
	• If an additional iteration of a key derivation function using a salt value known only to the verifier is performed, then this secret salt value is generated with an approved random bit generator and of sufficient length?	____	____	____	IA-5, (1)(a)23	
	• If an additional iteration of a key derivation function using a salt value known only to the verifier is performed, then this secret salt value provides at least the minimum-security strength?	____	____	____	IA-5, (1)(a)24	
	• If an additional iteration of a key derivation function using a salt value known only to the verifier is performed,					

#	*QUESTION*	*YES*	*NO*	*N/A*	*STANDARD*	*COMMENT*
	then this secret salt value is stored separately from the memorized secrets?	____	____	____	IA-5, (1)(a)25	
15.	Based on inquiry and record examination, does the Tribe or TGRA verify:					
	• CSPs creating look-up secret authenticators use an approved random bit generator to generate the list of secrets?	____	____	____	IA-5, (1)(b)1	
	• Look-up secrets are at least 20 bits of entropy?	____	____	____	IA-5, (1)(b)2	
	• If look-up secrets are distributed online, then they are distributed over a secure channel in accordance with the post-enrollment binding requirements in IA-5 'n' 16 through 22?	____	____	____	IA-5, (1)(b)3	
	• Verifiers of look-up secrets prompt the claimant for the next secret from their authenticator or for a specific (e.g., numbered) secret?	____	____	____	IA-5, (1)(b)4	
	• A given secret from an authenticator is used successfully only once?	____	____	____	IA-5, (1)(b)5	
	• If a look-up secret is derived from a grid (bingo) card, then each cell of the grid is used only once?	____	____	____	IA-5, (1)(b)6	
	• Verifiers store look-up secrets in a form that is resistant to offline attacks?	____	____	____	IA-5, (1)(b)7	
	• If look-up secrets have at least 112 bits of entropy, then they are hashed with an approved one-way function?	____	____	____	IA-5, (1)(b)8	
	• If look-up secrets have less than 112 bits of entropy, then they are salted and hashed using a suitable one-way key derivation function?	____	____	____	IA-5, (1)(b)9	
	• If look-up secrets have less than 112 bits of entropy, then the salt is at least 32 bits in length and be chosen arbitrarily to minimize salt value collisions among stored hashes?	____	____	____	IA-5, (1)(b)10	
	• If look-up secrets have less than 112 bits of entropy, then both the salt value and the resulting hash is stored for each look-up secret?	____	____	____	IA-5, (1)(b)11	
	• If look-up secrets that have less than 64 bits of entropy, then the verifier implements a rate-limiting mechanism					

#	*QUESTION*	*YES*	*NO*	*N/A*	*STANDARD*	*COMMENT*
	that effectively limits the number of failed authentication attempts that can be made on the subscriber's account?	____	____	____	IA-5, (1)(b)12	
	• The verifier uses approved encryption when requesting look-up secrets in order to provide resistance to eavesdropping and MitM attacks?	____	____	____	IA-5, (1)(b)13	
	• The verifier uses an authenticated protected channel when requesting look-up secrets in order to provide resistance to eavesdropping and MitM attacks?	____	____	____	IA-5, (1)(b)14	
16.	Based on inquiry and record examination, does the Tribe or TGRA verify:					
	• The out-of-band authenticator establishes a separate channel with the verifier in order to retrieve the out-of-band secret or authentication request?	____	____	____	IA-5, (1)(c)1	
	• Communication over the secondary channel is encrypted unless sent via the public switched telephone network (PSTN)?	____	____	____	IA-5, (1)(c)2	
	• Methods that do not prove possession of a specific device, such as voice-over-IP (VoIP) or email, are NOT used for out-of-band authentication?	____	____	____	IA-5, (1)(c)3	
	• If PSTN is not being used for out-of-band communication, then the out-of-band authenticator uniquely authenticates itself by establishing an authenticated protected channel with the verifier?	____	____	____	IA-5, (1)(c)4	
	• If PSTN is not being used for out-of-band communication, then the out-of-band authenticator communicates with the verifier using approved cryptography?	____	____	____	IA-5, (1)(c)5	
	• If PSTN is not being used for out-of-band communication, then the key used to authenticate the out-of-band device is stored in suitably secure storage available to the authenticator application (e.g., keychain storage, TPM, TEE, secure element)[5]?	____	____	____	IA-5, (1)(c)6	
	• If the PSTN is used for out-of-band authentication and a secret is sent to the					

[5] The secret key associated with an out-of-band device or authenticator application is critical to the determination of "something you have" and needs to be well protected.

#	*QUESTION*	*YES*	*NO*	*N/A*	*STANDARD*	*COMMENT*
	out-of-band device via the PSTN, then the out-of-band authenticator uniquely authenticates itself to a mobile telephone network using a SIM card or equivalent that uniquely identifies the device?	____	____	____	IA-5, (1)(c)7	
	• If the out-of-band authenticator sends an approval message over the secondary communication channel, it either accepts transfer of a secret from the primary channel to be sent to the verifier via the secondary communications channel, or present a secret received via the secondary channel from the verifier and prompt the claimant to verify the consistency of that secret with the primary channel, prior to accepting a yes/no response from the claimant which it sends to the verifier?	____	____	____	IA-5, (1)(c)8	
	• The verifier does NOT store the identifying key itself, but uses a verification method (e.g., an approved hash function or proof of possession of the identifying key) to uniquely identify the authenticator?	____	____	____	IA-5, (1)(c)9	
	• Depending on the type of out-of-band authenticator, one of the following takes place: transfer of a secret to the primary channel, transfer of a secret to the secondary channel, or verification of secrets by the claimant?	____	____	____	IA-5, (1)(c)10	
	• If the out-of-band authenticator operates by transferring the secret to the primary channel, then the verifier transmits a random secret to the out-of-band authenticator and then wait for the secret to be returned on the primary communication channel?	____	____	____	IA-5, (1)(c)11	
	• If the out-of-band authenticator operates by transferring the secret to the secondary channel, then the verifier displays a random authentication secret to the claimant via the primary channel and then wait for the secret to be returned on the secondary channel from the claimant's out-of-band authenticator?	____	____	____	IA-5, (1)(c)12	
	• If the out-of-band authenticator operates by verification of secrets by the claimant,					

#	QUESTION	YES	NO	N/A	STANDARD	COMMENT
	then the verifier displays a random authentication secret to the claimant via the primary channel, send the same secret to the out-of-band authenticator via the secondary channel for presentation to the claimant, and then wait for an approval (or disapproval) message via the secondary channel?	____	____	____	IA-5, (1)(c)13	
	• The authentication is considered invalid if not completed within 10 minutes?	____	____	____	IA-5, (1)(c)14	
	• Verifiers accept a given authentication secret only once during the validity period?	____	____	____	IA-5, (1)(c)15	
	• The verifier generates random authentication secrets with at least 20 bits of entropy?	____	____	____	IA-5, (1)(c)16	
	• The verifier generates random authentication secrets using an approved random bit generator?	____	____	____	IA-5, (1)(c)17	
	• If the authentication secret has less than 64 bits of entropy, the verifier implements a rate-limiting mechanism that effectively limits the number of failed authentication attempts that can be made on the subscriber's account as described in IA-5 l (3) through (4)?	____	____	____	IA-5, (1)(c)18	
	• If out-of-band verification is to be made using the PSTN, then the verifier verifies that the pre-registered telephone number being used is associated with a specific physical device?	____	____	____	IA-5, (1)(c)19	
	• If out-of-band verification is to be made using the PSTN, then changing the pre-registered telephone number is considered to be the binding of a new authenticator and only occurs as described in IA-5 n (16) through (22)?	____	____	____	IA-5, (1)(c)20	
	• If PSTN is used for out-of-band authentication, then the CSP offers subscribers at least one alternate authenticator that is not RESTRICTED and can be used to authenticate at the required AAL?	____	____	____	IA-5, (1)(c)21	
	• If PSTN is used for out-of-band authentication, then the CSP provides meaningful notice to subscribers regarding the security risks of the					

#	*QUESTION*	*YES*	*NO*	*N/A*	*STANDARD*	*COMMENT*
	RESTRICTED authenticator and availability of alternative(s) that are not RESTRICTED?	____	____	____	IA-5, (1)(c)22	
	• If PSTN is used for out-of-band authentication, then the CSP addresses any additional risk to subscribers in its risk assessment?	____	____	____	IA-5, (1)(c)23	
	• If PSTN is used for out-of-band authentication, then the CSP develops a migration plan for the possibility that the RESTRICTED authenticator is no longer acceptable at some point in the future and include this migration plan in its digital identity acceptance statement?	____	____	____	IA-5, (1)(c)24	
17.	Based on inquiry and record examination, does the Tribe or TGRA verify:					
	• The secret key and its algorithm provides at least the minimum security strength of 112 bits as of the date of this publication?	____	____	____	IA-5, (1)(d)1	
	• The nonce is of sufficient length to ensure that it is unique for each operation of the device over its lifetime?	____	____	____	IA-5, (1)(d)2	
	• One-time Password (OTP) authenticators — particularly software-based OTP generators —do NOT facilitate the cloning of the secret key onto multiple devices?	____	____	____	IA-5, (1)(d)3	
	• The authenticator output has at least 6 decimal digits (approximately 20 bits) of entropy?	____	____	____	IA-5, (1)(d)4	
	• If the nonce used to generate the authenticator output is based on a real-time clock, then the nonce is changed at least once every 2 minutes?	____	____	____	IA-5, (1)(d)5	
	• The OTP value associated with a given nonce is be accepted only once?	____	____	____	IA-5, (1)(d)6	
	• The symmetric keys used by authenticators are also present in the verifier and is strongly protected against compromise?	____	____	____	IA-5, (1)(d)7	
	• If a single-factor OTP authenticator is being associated with a subscriber account, then the verifier or associated CSP uses approved cryptography to either generate and exchange or to obtain the					

#	*QUESTION*	*YES*	*NO*	*N/A*	*STANDARD*	*COMMENT*
	secrets required to duplicate the authenticator output?	____	____	____	IA-5, (1)(d)8	
	• The verifier uses approved encryption when collecting the OTP?	____	____	____	IA-5, (1)(d)9	
	• The verifier uses an authenticated protected channel when collecting the OTP?	____	____	____	IA-5, (1)(d)10	
	• If a time-based OTP is used, it has a defined lifetime (recommended 30 seconds) that is determined by the expected clock drift — in either direction — of the authenticator over its lifetime, plus allowance for network delay and user entry of the OTP?	____	____	____	IA-5, (1)(d)11	
	• Verifiers accepts a given time-based OTP only once during the validity period?	____	____	____	IA-5, (1)(d)12	
	• If the authenticator output has less than 64 bits of entropy, the verifier implements a rate-limiting mechanism that effectively limits the number of failed authentication attempts that can be made on the subscriber's account as described in IA-5 l (3) through (4)?	____	____	____	IA-5, (1)(d)13	
	• If the authenticator is multi-factor, then each use of the authenticator requires the input of the additional factor?	____	____	____	IA-5, (1)(d)14	
	• If the authenticator is multi-factor and a memorized secret is used by the authenticator for activation, then that memorized secret is a randomly chosen numeric secret at least 6 decimal digits in length or other memorized secret meeting the requirements of IA-5 (1)(a)?	____	____	____	IA-5, (1)(d)15	
	• If the authenticator is multi-factor, then use of a memorized secret for activation is rate limited as specified in IA-5 l (3) through (4)?	____	____	____	IA-5, (1)(d)16	
	• If the authenticator is multi-factor and is activated by a biometric factor, then that factor meets the requirements of IA-5 m, including limits on the number of consecutive authentication failures?	____	____	____	IA-5, (1)(d)17	
	• If the authenticator is multi-factor, then the unencrypted key and activation secret or biometric sample — and any biometric data derived from the biometric sample such as a probe produced through signal					

#	*QUESTION*	*YES*	*NO*	*N/A*	*STANDARD*	*COMMENT*
	processing — is zeroized immediately after an OTP has been generated?	____	____	____	IA-5, (1)(d)18	
	• If the authenticator is multi-factor, the verifier or CSP establishes, via the authenticator source, that the authenticator is a multi-factor device?	____	____	____	IA-5, (1)(d)19	
	• In the absence of a trusted statement that it is a multi-factor device, the verifier treats the authenticator as single-factor, in accordance with IA-5 (1) (d) (1) through (13)?	____	____	____	IA-5, (1)(d)20	
18.	Based on inquiry and record examination, does the Tribe or TGRA verify:					
	• If the cryptographic authenticator is software based, the key is stored in suitably secure storage available to the authenticator application?	____	____	____	IA-5, (1)(e)1	
	• If the cryptographic authenticator is software based, the key is strongly protected against unauthorized disclosure by the use of access controls that limit access to the key to only those software components on the device requiring access?	____	____	____	IA-5, (1)(e)2	
	• If the cryptographic authenticator is software based, it does NOT facilitate the cloning of the secret key onto multiple devices?	____	___	____	IA-5, (1)(e)3	
	• If the authenticator is single-factor and hardware-based, secret keys unique to the device can NOT be exportable (i.e., cannot be removed from the device)?	____	____	____	IA-5, (1)(e)4	
	• the authenticator is hardware-based, the secret key and its algorithm provides at least the minimum-security length of 112 bits as of the date of this publication (9/14/2023)?	____	____	____	IA-5, (1)(e)5	
	• If the authenticator is hardware-based, the challenge nonce is at least 64 bits in length?	____	____	____	IA-5, (1)(e)6	
	• If the authenticator is hardware-based, approved cryptography is used?	____	____	____	IA-5, (1)(e)7	
	• Cryptographic keys stored by the verifier are protected against modification?	____	____	____	IA-5, (1)(e)8	

#	*QUESTION*	*YES*	*NO*	*N/A*	*STANDARD*	*COMMENT*
	• If symmetric keys are used, cryptographic keys stored by the verifier are protected against disclosure?	____	____	____	IA-5, (1)(e)9	
	• The challenge nonce is at least 64 bits in length?	____	____	____	IA-5, (1)(e)10	
	• The challenge nonce is either unique over the authenticator's lifetime or statistically unique (i.e., generated using an approved random bit generator)?	____	____	____	IA-5, (1)(e)11	
	• The verification operation uses approved cryptography?	____	____	____	IA-5, (1)(e)12	
	• If a multi-factor cryptographic software authenticator is being used, then each authentication requires the presentation of the activation factor?	____	____	____	IA-5, (1)(e)13	
	• If the authenticator is multi-factor, then any memorized secret used by the authenticator for activation is a randomly chosen numeric secret at least 6 decimal digits in length or other memorized secret meeting the requirements of IA-5 (1) (a)?	____	____	____	IA-5, (1)(e)14	
	• If the authenticator is multi-factor, then use of a memorized secret for activation is rate limited as specified in IA-5 l (3) through (4)?	____	____	____	IA-5, (1)(e)15	
	• If the authenticator is multi-factor and is activated by a biometric factor, then that factor meets the requirements of IA-5 m, including limits on the number of consecutive authentication failures?	____	____	____	IA-5, (1)(e)16	
	• If the authenticator is multi-factor, then the unencrypted key and activation secret or biometric sample — and any biometric data derived from the biometric sample such as a probe produced through signal processing — is zeroized immediately after an authentication transaction has taken place?	____	____	____	IA-5, (1)(e)17	
19.	Based on inquiry and record examination, does the Tribe or TGRA, for public key-based authentication:					
	• Enforce authorized access to the corresponding private key?	____	____	____	IA-5, (2)(a)1	
	• Map the authenticated identity to the account of the individual or group?	____	____	____	IA-5, (2)(a)2	

#	*QUESTION*	*YES*	*NO*	*N/A*	*STANDARD*	*COMMENT*
	Based on inquiry and record examination, does the Tribe or TGRA do the following, when public key infrastructure (PKI) is used:					
	• Validate certificates by constructing and verifying a certification path to an accepted trust anchor, including checking certificate status information?	____	____	____	IA-5, (2)(b)1	
	• Implement a local cache of revocation data to support path discovery and validation?	____	____	____	IA-5, (2)(b)2	
20.	Based on inquiry and record examination, does the Tribe or TGRA protect authenticators commensurate with the security category of the information to which use of the authenticator permits access?	____	____	____	IA-5, (6)	
21.	Based on inquiry and record examination, does the Tribe or TGRA obscure feedback of authentication information during the authentication process to protect the information from possible exploitation and use by unauthorized individuals?	____	____	____	IA-6	
22.	Based on inquiry and record examination, does the Tribe or TGRA, implement mechanisms for authentication to a cryptographic module that meet the requirements of applicable laws, executive orders, directives, policies, regulations, standards, and guidelines for such authentication?	____	____	____	IA-7	
23.	Based on inquiry and record examination, does the Tribe or TGRA, uniquely identify and authenticate non-organizational users or processes acting on behalf of non-organizational users?	____	____	____	IA-8	
24.	Based on inquiry and record examination, does the Tribe or TGRA, accept and electronically verify Personal Identity Verification (PIV)-compliant credentials from other federal, state, local, tribal, or territorial (SLTT) agencies?	____	____	____	IA-8, (1)	

#	*QUESTION*	*YES*	*NO*	*N/A*	*STANDARD*	*COMMENT*
25.	Based on inquiry and record examination, does the Tribe or TGRA:					
	• Accept only external authenticators that are NIST (National Institute of Standards and Technology)-compliant?	____	____	____	IA-8, (2)(a)	
	• Document and maintain a list of accepted external authenticators?	____	____	____	IA-8, (2)(b)	
26.	Based on inquiry and record examination, does the Tribe or TGRA conform to the following profiles for identity management: Security Assertion Markup Language (SAML) or OpenID Connect?	____	____	____	IA-8, (4)	
27.	Based on inquiry and record examination, does the Tribe or TGRA require users to re-authenticate when: roles, authenticators, or credentials change, security categories of systems change, the execution of privileged functions occur, or every 12 hours?	____	____	____	IA-11	
28.	Based on inquiry and record examination, does the Tribe or TGRA:					
	• Identity proof users that require accounts for logical access to systems based on appropriate identity assurance level requirements as specified in applicable standards and guidelines?	____	____	____	IA-12, a	
	• Resolve user identities to a unique individual?	____	____	____	IA-12, b	
	• Collect, validate, and verify identity evidence?	____	____	____	IA-12, c	
29.	Based on inquiry and record examination, does the Tribe or TGRA require evidence of individual identification be presented to the registration authority?	____	____	____	IA-12, (2)	
30.	Based on inquiry and record examination, does the Tribe or TGRA:					
	• Require that the presented identity evidence be validated and verified through agency-defined resolution, validation, and verification methods?	____	____	____	IA-12, (3)a	

#	*QUESTION*	*YES*	*NO*	*N/A*	*STANDARD*	*COMMENT*
	• Identity proofing is NOT be performed to determine suitability or entitlement to gain access to services or benefits?	____	____	____	IA-12, (3)b	
	• Collection of Personal Identifiable Information (PII) is limited to the minimum necessary to resolve to a unique identity in a given context?	____	____	____	IA-12, (3) c.1	
	• Collection of PII is limited to the minimum necessary to validate the existence of the claimed identity and associate the claimed identity with the applicant providing identity evidence for appropriate identity resolution, validation, and verification?	____	____	____	IA-12, (3) c.2	
	• The CSP provides explicit notice to the applicant 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?	____	____	____	IA-12, (3)d	
	• If CSPs process 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, then CSPs implement measures to maintain predictability and manageability commensurate with the privacy risk arising from the additional processing?	____	____	____	IA-12, (3)e	
	• If the CSP employs consent as part of its measures to maintain predictability and manageability, …then it will NOT make consent for the additional processing a condition of the identity service?	____	____	____	IA-12, (3)f	
	• The CSP provides mechanisms for redress of applicant complaints or problems arising from the identity proofing?	____	____	____	IA-12, (3)g	
	• The CSP assesses the [redress] mechanisms for their efficacy in achieving resolution of complaints or problems?	____	____	____	IA-12, (3)h	

#	*QUESTION*	*YES*	*NO*	*N/A*	*STANDARD*	*COMMENT*
	• The identity proofing and enrollment processes is performed according to an applicable written policy or *practice statement* that specifies the particular steps taken to verify identities?	____	____	____	IA-12, (3)i	
	• The *practice statement* includes control information detailing how the CSP handles proofing errors that result in an applicant not being successfully enrolled?	____	____	____	IA-12, (3)j	
	• The CSP maintains a record, including audit logs, of all steps taken to verify the identity of the applicant as long as the identity exists in the information system?	____	____	____	IA-12, (3)k	
	• The CSP records the types of identity evidence presented in the proofing process?	____	____	____	IA-12, (3)l	
	• The CSP conducts a risk management process, including assessments of privacy and security risks to determine:					
	o Any steps that it will take to verify the identity of the applicant beyond any mandatory requirements specified herein?	____	____	____	IA-12, (3) m.1	
	o The PII, including any biometrics, images, scans, or other copies of the identity evidence that the CSP will maintain as a record of identity proofing (Note: Specific federal requirements may apply)?	____	____	____	IA-12, (3) m.2	
	o The schedule of retention for these records[6]?	____	____	____	IA-12, (3) m.3	
	• All PII collected as part of the enrollment process is protected to ensure confidentiality, integrity, and attribution of the information source?	____	____	____	IA-12, (3)n	
	• The entire proofing transaction, including transactions that involve a third party, occurs over authenticated protected channels?	____	____	____	IA-12, (3)o	
	• If the CSP uses fraud mitigation measures, then the CSP conducts a					

[6] CSPs may be subject to specific retention policies in accordance with applicable laws, regulations, or policies, including any National Archives and Records Administration (NARA) records retention schedules that may apply.

#	QUESTION	YES	NO	N/A	STANDARD	COMMENT
	privacy risk assessment[7] for these mitigation measures?	____	____	____	IA-12, (3)p	
	• In the event a CSP ceases to conduct identity proofing and enrollment processes, then the CSP is responsible for fully disposing of or destroying any sensitive data including PII, or its protection from unauthorized access for the duration of retention?	____	____	____	IA-12, (3)q	
	• An enrollment code is comprised of one of the following: o Minimally, a random six character alphanumeric or equivalent entropy. For example, a code generated using an approved random number generator or a serial number for a physical hardware authenticator?	____	____	____	IA-12, (3) s.1	
	o A machine-readable optical label, such as a Quick Response (QR) Code, that contains data of similar or higher entropy as a random six character alphanumeric?	____	____	____	IA-12, (3) s.2	
	• Training requirements for personnel validating evidence is based on the policies, guidelines, or requirements of the CSP or RP?	____	____	____	IA-12, (3)t	
	• As applicable, this criterion applies to CSPs that provide identity proofing and enrollment services to minors (under the age of 18): o If the CSP provides identity proofing and enrollment services to minors (under the age of 18), then…the CSP gives special consideration to the legal restrictions of interacting with minors unable to meet the evidence requirements of identity proofing [to ensure compliance with the Children's Online Privacy Protection Act of 1998 (COPPA), and other laws, as applicable]?	____	____	____	IA-12, (3)u	

[7] Such assessments included 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 IA-12(3) k – m.

#	QUESTION	YES	NO	N/A	STANDARD	COMMENT
	• The CSP has the operator view the biometric source (e.g., fingers, face) for presence of non-natural materials and perform such inspections as part of the proofing process[8]?	____	____	____	IA-12, (3)v	
	• The CSP collects biometrics in such a way that ensures that the biometric is collected from the applicant, and not another subject[9]? All biometric performance requirements in IA-5 m (1) through (12) apply[10].	____	____	____	IA-12, (3)w	
	• The CSP supports in-person or remote identity proofing, or both?	____	____	____	IA-12, (3)x	
	• The CSP collects at least one of the following identity evidence from the applicant:					
	○ One piece of SUPERIOR or STRONG evidence if the evidence's issuing source, during its identity proofing event, confirmed the claimed identity by collecting two or more forms of SUPERIOR or STRONG evidence and the CSP validates the evidence directly with the issuing source[11]?	____	____	____	IA-12, (3) y.1	
	○ Two pieces of STRONG evidence?	____	____	____	IA-12, (3) y.2	
	○ One piece of STRONG evidence plus two pieces of FAIR evidence?	____	____	____	IA-12, (3) y.3	
	• The CSP validates each piece of evidence with a process that can achieve the same strength as the evidence presented (see requirements referenced above for IA-12, (3) y). For example, if two forms of STRONG identity evidence are presented, each piece of evidence will be validated at a strength of STRONG?	____	____	____	IA-12, (3)z	

[8] Requirements 'v' and 'w' apply to the collection of biometric characteristics for in-person (physical or supervised remote) identity proofing and are mandatory at Identity Assurance Level (IAL)3. These criteria also apply to CSPs that optionally choose to collect biometric characteristics through in-person identity proofing and enrollment at IAL2.
[9] Id.
[10] See CJISD-ITS-DOC-08140-5.9.3, pages 65-67.
[11] See CJISD-ITS-DOC-08140-5.9.3, Figure 8 – Notional Strengths of Evidence Types, pages 113-115.

#	*QUESTION*	*YES*	*NO*	*N/A*	*STANDARD*	*COMMENT*
	• The CSP verifies identity evidence as follows: ○ At a minimum, the applicant's binding to identity evidence must be verified by a process that is able to achieve a strength of STRONG[12]?	____	____	____	IA-12, (3) aa	
	• For Identity Assurance Level (IAL) 2 remote proofing: The collection of biometric characteristics for physical or biometric comparison of the applicant to the strongest piece of identity evidence provided to support the claimed identity performed remotely adheres to all requirements as specified in IA-5 m?	____	____	____	IA-12, (3) bb	
	• Knowledge-based verification (KBV) is NOT be used for in-person (physical or supervised remote) identity verification?	____	____	____	IA-12, (3) cc	
	• The CSP employs appropriately tailored security controls, to include control enhancements, from the moderate or high baseline of security controls defined in the CJISSECPOL?	____	____	____	IA-12, (3) dd	
	• The CSP ensures that the minimum assurance-related controls for moderate-impact systems are satisfied?	____	____	____	IA-12, (3) dd	
	• Supervised Remote Identity Proofing: Supervised remote identity proofing is intended to provide controls for comparable levels of confidence and security to in-person IAL3 identity proofing for identity proofing processes that are performed remotely. Supervised remote identity proofing is optional for CSPs; that is, if a CSP chooses to use supervised remote identity proofing, then the following requirements, (1) through (8), would apply. It should be noted that the term "supervised remote identity proofing" has specialized meaning and is used only to refer to the specialized equipment and the following control requirements, (1) through (8). In addition to those requirements presented in this document, as well as the applicable					

[12] See CJISD-ITS-DOC-08140-5.9.3, Figure 11 – Verification Methods and Strengths, page 119.

#	QUESTION	YES	NO	N/A	STANDARD	COMMENT
	identity validation and verification requirements, CSPs that provide supervised remote identity proofing services must demonstrate conformance with the requirements contained in this section. The following requirements for supervised remote proofing apply specifically to IAL3. If the equipment/facilities used for supervised remote proofing are used for IAL2 identity proofing, the following requirements, (1) through (8), for supervised remote proofing do not apply. In this case, the requirements for conventional remote identity proofing are applicable.					
	○ Supervised remote identity proofing and enrollment transactions meet the following requirements, in addition to the IAL3 validation and verification requirements specified in IA-12(3)s?	____	____	____	IA-12, (3) ee.1	
	○ The CSP monitors the entire identity proofing session, from which the applicant does NOT depart — for example, by a continuous high-resolution video transmission of the applicant?	____	____	____	IA-12, (3) ee.2	
	○ The CSP has a live operator participate remotely with the applicant for the entirety of the identity proofing session?	____	____	____	IA-12, (3) ee.3	
	○ The CSP requires all actions taken by the applicant during the identity proofing session to be clearly visible to the remote operator?	____	____	____	IA-12, (3) ee.4	
	○ The CSP requires that all digital validation of evidence (e.g., via chip or wireless technologies) is performed by integrated scanners and sensors?	____	____	____	IA-12, (3) ee.5	
	○ The CSP requires operators to have undergone a training program to detect potential fraud and to properly perform a					

#	QUESTION	YES	NO	N/A	STANDARD	COMMENT
	supervised remote proofing session?	____	____	____	IA-12, (3) ee.6	
	○ The CSP employs physical tamper detection and resistance features appropriate for the environment in which it is located?	____	____	____	IA-12, (3) ee.7	
	○ The CSP ensures that all communications occur over a mutually authenticated protected channel?	____	____	____	IA-12, (3) ee.8	
	• Trusted Referee: The use of trusted referees is optional for CSPs; that is, if a CSP chooses to use trusted referees for identity proofing and enrollment, then the following requirements, (1) through (3), would apply. The use of trusted referees is intended to assist in the identity proofing and enrollment for populations that are unable to meet IAL2 identity proofing requirements, or otherwise would be challenged to perform identity proofing and enrollment process requirements. Such populations may include, but are not limited to disabled individuals; elderly individuals; homeless individuals; individuals with little or no access to online services or computing devices; unbanked and individuals with little or no credit history; victims of identity theft; children under 18; and immigrants.					
	In addition to those requirements presented in the General section of this requirement, as well as the applicable IAL requirements, CSPs that use trusted referees in their identity proofing services must demonstrate conformance with the requirements contained here:					
	○ If the CSP uses trusted referees, then…The CSP has established a written policy and procedures as to how a trusted referee is determined and the lifecycle by which the trusted referee retains their status as a valid referee, to include any restrictions, as well as					

#	QUESTION	YES	NO	N/A	STANDARD	COMMENT
	any revocation and suspension requirements?	____	____	____	IA-12, (3) ff.1	
	o If the CSP uses trusted referees, then…The CSP proofs the trusted referee at the same IAL as the applicant proofing?	____	____	____	IA-12, (3) ff.2	
	o If the CSP uses trusted referees, then…The CSP determines the minimum evidence required to bind the relationship between the trusted referee and the applicant?	____	____	____	IA-12, (3) ff.3	
31.	Based on inquiry and record examination, does the Tribe or TGRA:					
	• Require that a registration code or notice of proofing be delivered through an out-of-band channel to verify the users address (physical or digital) of record?	____	____	____	IA-12, (5)a	
	• Verify the CSP confirms the address of record?	____	____	____	IA-12, (5)b	
	• Issuing source(s) or authoritative source(s) are valid records to confirm an address? Self-asserted address data that has not been confirmed in records are NOT be used for confirmation.	____	____	____	IA-12, (5)c	
	• Note that IAL2-7 applies only to in-person proofing at IAL2. If the CSP performs in-person proofing for IAL2 and provides an enrollment code directly to the subscriber for binding to an authenticator at a later time, then the enrollment code…is valid for a maximum of seven (7) days?	____	____	____	IA-12, (5)d	
	• For remote identity proofing at IAL2, verify the CSP sends an enrollment code to a confirmed address of record for the applicant?	____	____	____	IA-12, (5)e	
	• For remote identity proofing at IAL2, verify the applicant presents a valid enrollment code to complete the identity proofing process?	____	____	____	IA-12, (5)f	
	• Note that the following enrollment code validity periods apply to enrollment codes sent to confirmed addresses of record for IAL2 remote in-person proofing only. Enrollment codes shall have the following maximum validities:					

#	QUESTION	YES	NO	N/A	STANDARD	COMMENT
	○ 10 days, when sent to a postal address of record within the contiguous United States?	____	____	____	IA-12, (5) g.1	
	○ 30 days, when sent to a postal address of record outside the contiguous United States?	____	____	____	IA-12, (5) g.2	
	○ 10 minutes, when sent to a telephone of record (SMS or voice)?	____	____	____	IA-12, (5) g.3	
	○ 24 hours, when sent to an email address of record?	____	____	____	IA-12, (5) g.4	
	• If the enrollment code sent to the confirmed address of record as part of the remote identity proofing process at IAL2 is also intended to be an authentication factor, then…it is reset upon first use?	____	____	____	IA-12, (5)h	
	• If the CSP performs remote proofing at IAL2 and optionally sends notification of proofing in addition to sending the required enrollment code, then…The CSP ensures the enrollment code and notification of proofing are sent to different addresses of record?	____	____	____	IA-12, (5)i	