National Identity Exchange Federation

Audit Policy

Version 1.0

August 18, 2014

Table of Contents

TABLE OF CONTENTS I

1 NIEF CENTER AUDITOR QUALIFICATIONS 1

2 PROCESS FOR INITIAL AUDITS OF NIEF MEMBER AGENCIES 1

3 PROCESS FOR ONGOING AUDITS OF NIEF MEMBER AGENCIES 1

4 TECHNICAL AUDIT REQUIREMENTS 2

4.1 NIST/FICAM LEVEL OF ASSURANCE 2 REQUIREMENTS FOR IDPOS 2
4.1.1 LOA 2 IDENTITY REGISTRATION AND ISSUANCE TRUST CRITERIA REQUIREMENTS 2
4.1.2 LOA 2 TOKEN TRUST CRITERIA REQUIREMENTS 9
4.1.3 LOA 2 TOKEN AND CREDENTIAL MANAGEMENT TRUST CRITERIA REQUIREMENTS 12
4.1.4 LOA 2 AUTHENTICATION PROCESS TRUST CRITERIA REQUIREMENTS 14
4.2 NIST/FICAM NON-PKI LEVEL OF ASSURANCE 3 REQUIREMENTS FOR IDPOS 16
4.2.1 LOA 3 IDENTITY REGISTRATION AND ISSUANCE TRUST CRITERIA REQUIREMENTS 16
4.2.2 LOA 3 TOKEN TRUST CRITERIA REQUIREMENTS 21
4.2.3 LOA 3 TOKEN AND CREDENTIAL MANAGEMENT TRUST CRITERIA REQUIREMENTS 22
4.2.4 LOA 3 AUTHENTICATION PROCESS TRUST CRITERIA REQUIREMENTS 24
4.3 NIEF-SPECIFIC REQUIREMENTS ABOUT LOCAL SECURITY POLICIES AND PRACTICES 26
4.4 NIEF-SPECIFIC PRIVACY REQUIREMENTS 28
4.5 ADOPTION OF FICAM PRIVACY ASSESSOR AND AUDITOR GUIDANCE 30
4.6 NIEF-SPECIFIC FINANCIAL REQUIREMENTS 30
4.7 MISCELLANEOUS NIEF-SPECIFIC REQUIREMENTS 30

5 FEES 31

6 DEFINITIONS 31

1 NIEF Center Auditor Qualifications

All audits conducted by the NIEF Center shall be performed under the supervision of the NIEF Audit Supervisor. The NIEF Audit Supervisor must hold the Certified Information Systems Auditor (CISA) designation. In addition, for each audit conducted by the NIEF Center, at least one member of the NIEF audit team must hold the Certified Information Systems Security Professional (CISSP) designation.

2 Process for Initial Audits of NIEF Member Agencies

The initial audit process for a NIEF member agency shall consist of the following steps.

1. The NIEF Center audit supervisor shall conduct an Initial Audit Interview based on the list of standard audit requirements in Section 4 of this document. The agency representative shall respond to all audit requirements truthfully and completely, and shall furnish any requested supporting details as needed, to constitute proof of compliance with the agency's written or stated policies and intentions.

2. Within two (2) weeks following the interview, the audit supervisor shall prepare an Initial Audit Report about the agency and furnish the agency with a copy of the report for review and comment.

3. Within two (2) weeks after receiving a copy of the Initial Audit Report, the agency may request changes or corrections to the report. In some cases, the audit supervisor may request additional supporting details from the agency as a precondition for making specific changes or corrections.

4. The final copy of the agency's Initial Audit Report shall be kept on file by NIEF for a period of at least five (5) years, and also made available for all NIEF member agencies to review.

3 Process for Ongoing Audits of NIEF Member Agencies

Ongoing audits of NIEF member agencies shall be conducted on an annual basis, as follows.

1. The NIEF Center audit supervisor shall conduct an Annual Audit Interview based on the list of standard audit requirements in Section 4 of this document, and shall use the agency's Initial Audit Report or its most recent Annual Audit Report as a baseline. The primary goal of this interview shall be to determine whether the agency's Initial Audit Report or its most recent Annual Audit Report still accurately represents the current state of practice for the agency, and if not, to accurately document any changes that have occurred since the agency's Initial Audit Report or its most recent Annual Audit Report was written. The agency representative shall

respond to all audit requirements truthfully and completely, and shall furnish any requested supporting details as needed, to constitute proof of compliance with the agency's written or stated policies and intentions.

2. Within two (2) weeks following the interview, the audit supervisor shall prepare an Annual Audit Report about the agency and furnish the agency with a copy of the report for review and comment.

3. Within two (2) weeks after receiving a copy of the Annual Audit Report, the agency may request changes or corrections to the report. In some cases, the audit supervisor may request additional supporting details from the agency as a precondition for making specific changes or corrections.

4. The final copy of the agency's Annual Audit Report shall be kept on file by NIEF for a period of at least five (5) years, and also made available for all NIEF member agencies to review.

4 Technical Audit Requirements

When auditing NIEF applicants and NIEF member agencies, the NIEF Center audit supervisor shall ensure that the audit includes inquiries into all of the following technical requirements, as applicable based on the agency's role or intended role within NIEF. For each NIEF technical audit requirement, the audit supervisor must answer the following questions.

1. Does the applicant or member agency have internal documented policies and procedures that align sufficiently with the NIEF technical audit requirement?

2. Does the applicant or member agency follow these internal documented policies and procedures, so as to actually comply with the NIEF technical requirement?

4.1 NIST/FICAM Level of Assurance 2 Requirements for IDPOs

These requirements apply only to FICAM Level of Assurance (LOA) 2 Identity Provider Organizations (IDPOs). They are derived from Appendix A-2 of the Federal Identity, Credentialing, and Access Management (FICAM) Trust Framework Provider Adoption Process (TFPAP) document [FICAM TFPAP].[1] Audits of IDPOs at LOA 2 may be conducted either via telephone conversation with an IDPO representative, or via an in-person interview with an IDPO representative.

4.1.1 LOA 2 Identity Registration and Issuance Trust Criteria Requirements

[1] http://www.idmanagement.gov/sites/default/files/documents/FICAM_TFS_TFPAP_0.pdf

1. The IDPO must have established and well-documented policies, procedures, and mechanisms to ensure that a trusted relationship always exists between the Registration Authority (RA) and the IDPO. In addition, well-documented mechanisms and policies must be in place to ensure each party knows the other party and its obligations.

2. The IDPO must have established and well-documented policies, procedures, and mechanisms to ensure that a trusted RA performs identity proofing of Applicants. This includes specific identifying materials and/or other information that is acceptable for proving the Applicant's identity.

3. The IDPO must have established and well-documented policies, procedures, and mechanisms to ensure that identity tokens are issued in a manner that protects the confidentiality of information, and thereby resists the threat of token issuance disclosure.

4. The IDPO must have established and well-documented policies, procedures, and mechanisms to ensure that it allows the Subscriber (user or token recipient) to authenticate the IDPO as the source of any token and credential data that he or she may receive, and thereby resist the threat of token issuance tampering.

5. The IDPO must have established and well-documented policies, procedures, and mechanisms to ensure that the individual who receives the token is the same individual who participated in the registration procedure, and thereby resist the threat of unauthorized token issuance.

6. The IDPO must have established and well-documented policies, procedures, and mechanisms to protect against a Subscriber denying registration, claiming that they did not register that token, and thereby resist the threat of repudiation of registration.

7. The IDPO must have established and well-documented policies, procedures, and mechanisms to ensure that it protects sensitive data, including Personally Identifiable Information (PII)[2], obtained during registration and identity proofing. Sensitive data collected during the registration and identity-proofing stage must be protected at all times (e.g., during transmission and storage) to ensure its security and privacy.

8. The IDPO must have established and well-documented policies, procedures, and mechanisms to ensure that all identity proofing information comes from known, trusted sources and is sufficiently protected to ensure source authentication, confidentiality and integrity.

[2] See the definition of PII in Section 6.

9. The IDPO must have established and well-documented policies, procedures, and mechanisms to ensure that either the RA or the IDPO maintains a record of each individual whose identity has been verified, including the steps taken to verify his or her identity and any information collected from the Applicant.

10. The IDPO must have established and well-documented policies, procedures, and mechanisms to ensure that it has the capability to provide records of identity proofing to SPOs as necessary, including detailed records of registration and credential issuance. Refer to applicable privacy laws, rules of evidence, etc., for what circumstances determine whether it is necessary and/or appropriate for the IDPO to provide this information.

11. The IDPO must have a written identity proofing and registration policy or practice statement that specifies the particular steps taken to verify identities, and it must submit this document to NIEF.

12. If the RA and IDPO are remotely located, and communicate over a network, then the IDPO must have established and well-documented policies, procedures, and mechanisms to ensure one of the following requirements are met.

    a. The entire registration transaction between the RA and IDPO occurs over a mutually authenticated protected session.

    b. The entire registration transaction consists of time-stamped or sequenced messages signed by their source and encrypted for their recipient.

    In all cases, the use of Approved Cryptographic Methods is required.[3]

13. The IDPO must have established and well-documented policies, procedures, and mechanisms to ensure that it can uniquely identify each Subscriber and the associated tokens and the credentials issued to that Subscriber. Also, the IDPO must have established and well-documented policies, procedures, and mechanisms to ensure that it is capable of conveying this information to Verifiers.

14. If the IDPO issues identities with pseudonymous names, then it must have established and well-documented policies, procedures, and mechanisms to ensure that either the RA or the IDPO knows the actual identity of the Subscriber. Also, if applicable, the IDPO must have established and well-documented policies, procedures, and mechanisms to specify whether the name in the credential is real or a pseudonym.

15. The IDPO must have established and well-documented policies, procedures, and mechanisms to ensure that it protects PII[4] collected as part of the registration process.

[3] See the definition of Approved Cryptographic Method in Section 6.

16. The IDPO must have established and well-documented policies, procedures, and mechanisms to require that an Applicant supply his or her full legal name, an address of record, and date of birth during the identity proofing process.

17. If the IDPO performs in-person identity proofing, then the following requirements apply.

    a. The IDPO must have established and well-documented policies, procedures, and mechanisms to ensure that each Applicant presents a verified current primary Government Picture ID that contains the Applicant's picture, and either address of record or nationality (e.g., driver's license or Passport).

    b. The IDPO must have established and well-documented policies, procedures, and mechanisms to ensure that the RA inspects the photo-ID, compares the picture to the Applicant, and records the ID number, address, and date of birth.

    c. The IDPO must have established and well-documented policies, procedures, and mechanisms to ensure that it issues credentials through one of the following processes.

        i. If the ID appears valid and the photo matches the Applicant, and the ID confirms the Applicant's address of record, then the IDPO issues credentials in a manner that confirms the ability of the Applicant to receive telephone communications or text messages at a phone number or email address associated with the Applicant in records. In addition, the IDPO must have established and well-documented policies, procedures, and mechanisms to ensure that any secret sent over an unprotected session shall be reset upon first use.

        ii. If the ID appears valid and the photo matches the Applicant, and the ID confirms the Applicant's address of record, then the IDPO sends notice of credential issuance to the Applicant's address of record.

        iii. If the ID appears valid and the photo matches the Applicant, and the ID does not confirm the Applicant's address of record, then the credential issuance process is conducted in a manner that confirms the Applicant's address of record.

        iv. If the IDPO is an employer or educational institution, then the IDPO issues credentials to employees or students in person after inspection of a corporate or school issued picture ID.

[4] See the definition of PII in Section 6.

v. If the IDPO is an employer or educational institution, then the IDPO issues credentials to employees or students through online processes, where notification is sent via the distribution channels normally used for sensitive, personal communications.

18. If the IDPO performs remote identity proofing, then the following requirements apply.

    a. The IDPO must have established and well-documented policies, procedures, and mechanisms to ensure that each Applicant presents a valid Government ID (e.g., a driver's license or Passport) number and a financial or utility account number (e.g., checking account, savings account, utility account, loan, credit card, or tax ID) with confirmation via records of either the government ID number or the account number.

    b. The IDPO must have established and well-documented policies, procedures, and mechanisms to ensure that the RA inspects both the ID number and the account number supplied by Applicant (e.g., for the correct number of digits).

    c. The IDPO must have established and well-documented policies, procedures, and mechanisms to ensure that the RA verifies the information provided by the Applicant, including ID number or account number, through record checks either with the applicable agency or institution, or through credit bureaus or similar databases, and confirms that the name, date of birth, address, and other personal information in records are on balance consistent with the application and sufficient to identify a unique individual. In addition, the IDPO must have established and well-documented policies, procedures, and mechanisms to ensure that the RA verifies utility account numbers, if provided by the Applicant, by verifying the Applicant's knowledge of recent account activity.

    d. The IDPO must have established and well-documented policies, procedures, and mechanisms to ensure that it and the RA perform address or phone number confirmation, credential issuance, and issuance notification through one of the following processes.

        i. The IDPO issues credentials in a manner that confirms the ability of the Applicant to receive mail at a physical address associated with the Applicant in records.

        ii. The IDPO issues credentials in a manner that confirms the ability of the Applicant to receive telephone communications or e-mail at the telephone number or e-mail address associated with the Applicant in records. In addition, the IDPO must have established and well-documented policies, procedures, and mechanisms to ensure that any

secret sent over an unprotected session is reset upon first use and is valid for a maximum lifetime of seven days.

iii. The IDPO issues credentials and the RA or IDPO sends notice of credential issuance to an address of record confirmed in the records check.

iv. If the IDPO is an employer or educational institution, then the IDPO issues credentials to employees or students in person by inspection of a corporate or school issued picture ID.

v. If the IDPO is an employer or educational institution, then the IDPO issues credentials to employees or students through online processes, where notification is sent via the distribution channels normally used for sensitive, personal communications.

19. The IDPO must have established and well-documented policies, procedures, and mechanisms to ensure that the same party acts as Applicant throughout the identity registration and issuance process. In addition, the IDPO must enforce one of the following policies.

    a. The Applicant shall identify himself/herself in any new electronic transaction (beyond the first transaction or encounter) by presenting a temporary secret that was established during a prior transaction or encounter, or sent to the Applicant's phone number, email address, or physical address of record.

    b. The Applicant shall identify himself/herself in person by either using a secret as described above, or through the use of a biometric that was recorded during a prior encounter.[5]

20. If the IDPO rigorously confirms the identity, education, and licensing credentials of a licensed professional in accordance with federal or state law or regulations, and through an in-person appearance prior to employment or affiliation, then the IDPO may issue e-authentication tokens and credentials to such employees and affiliates, without repeating the identity proofing process, in accordance with the following requirements.

    a. The IDPO must have established and well-documented policies, procedures, and mechanisms to ensure that the initial process for confirming the identity, education, and licensing credentials of the licensed professional includes the following steps.

[5] Registration, identity proofing, and token and credential issuance represent different goals of the same process. In many cases, however, this process may be broken up into a number of separate physical encounters and electronic transactions. Two electronic transactions are considered to be separate if they are not part of the same protected session

i. The IDPO verifies the employee or affiliate has a current primary government picture ID that contains the applicant's picture, and either address or nationality of record (e.g., a driver's license or passport).

ii. The IDPO verifies two or more years of post-secondary education or training appropriate for the professional's position (e.g., an appropriate medical degree).

iii. The IDPO verifies that the state or federal licensure of the employee or affiliate (e.g., as a physician) is current, is based on an examination process, and includes requirements for continuing education or active professional participation as a condition of valid licensing.

b. The IDPO must have established and well-documented policies, procedures, and mechanisms to ensure that it issues e-authentication tokens and credentials to employees and affiliates either in person, or via a remote issuance process that incorporates the address and phone number confirmation as appropriate for LOA 2.

c. The IDPO must meet the corresponding Token Trust Criteria Requirements (see Section 4.1.2), Token and Credential Management Trust Criteria Requirements (see Section 4.1.3), and Authentication Process Trust Criteria Requirements (see Section 4.1.4).

d. The IDPO must deploy systems that conform to the NIEF Web Browser User-to-System Profile, which is a profile of SAML 2.0 that conforms to (and further constrains) the FICAM SAML SSO Profile.

21. The IDPO may issue derived credentials to a Claimant provided that the following requirements are met.

a. The IDPO must have established and well-documented policies, procedures, and mechanisms to ensure that, before issuing any derived credential to a Claimant, it verifies the original credential status and verifies that the corresponding token is possessed and controlled by the Claimant.

b. The IDPO should have established and well-documented policies, procedures, and mechanisms to ensure that it re-checks the status of the original credential at a later date (e.g. after a week) to confirm that the credential was not compromised at the time of issuance of the derived credential. (This guards against the case where an Attacker requests the desired credential before revocation information can be updated.)

c. The IDPO must have established and well-documented policies, procedures, and mechanisms to ensure that it records the details of the original credential used as the basis for derived credential issuance.

4.1.2 LOA 2 Token Trust Criteria Requirements

Auditor Requirements:

1. When a multi-token authentication scheme is being used, the new level of assurance must be determined in accordance with NIST SP 800-63-2 Table 7. Using multiple tokens to achieve an increased level of assurance requires the use of two different factors of authentication. Combining multiple factors and/or multiple tokens may achieve a higher assurance level than would otherwise be attained. If one factor of a multi-factor scheme or one token of a multi-token scheme has the desired properties for a given assurance level, it is considered sufficient.

2. Multi-stage authentication processes, which use a single-factor token to obtain a second token, does not constitute multi-factor authentication. The level of assurance associated with the compound solution is the assurance level of the weakest token.

IDPO Requirements:

1. The IDPO must have established and well-documented policies, procedures, and mechanisms to protect tokens that have a physical manifestation (e.g., one time password device, hardware cryptographic device) against an Attacker, and thereby resist the threat of token theft.

2. The IDPO must have established and well-documented policies, procedures, and mechanisms to protect against a Subscriber's token being copied by an Attacker, with or without his or her knowledge, and thereby resist the threat of token duplication.

3. The IDPO must have established and well-documented policies, procedures, and mechanisms to protect against an Attacker establishing a level of trust with a Subscriber in order to convince the Subscriber to reveal his or her token or token secret, and thereby resist the threat of social engineering.

4. If the IDPO issues memorized secret tokens, then the following requirements apply.

    a. The IDPO must have established and well-documented policies, procedures, and mechanisms to ensure that every memorized secret is one of the following.

        i. A randomly generated personal identification number (PIN) that has entropy equivalent to, or greater than, a PIN consisting of six or more digits.

ii. A user generated string or secret that has entropy equivalent to, or greater than, eight or more characters chosen from an alphabet of 90 or more characters.

b. The IDPO must have established and well-documented policies, procedures, and mechanisms to ensure that it implements dictionary or composition rules to constrain user-generated secrets.

c. The IDPO must have established and well-documented policies, procedures, and mechanisms to ensure that the Verifier implements a throttling mechanism that effectively limits the number of failed authentication attempts an Attacker can make on any Subscriber's account to 100 or fewer in any 30 day period.

5. If the IDPO issues pre-registered knowledge tokens, then the following requirements on such tokens apply.

   a. The IDPO must have established and well-documented policies, procedures, and mechanisms to ensure that every secret provides at least 20 bits of entropy.

   b. The IDPO must have established and well-documented policies, procedures, and mechanisms to ensure that it prohibits empty secrets, and that the entropy in every secret cannot be directly calculated. In addition, if the pre-registered knowledge questions are not supplied by a user, then the IDPO must ensure that the user selects questions from a set of at least seven questions.

   c. The IDPO must have established and well-documented policies, procedures, and mechanisms to ensure that the Verifier implements a throttling mechanism that effectively limits the number of failed authentication attempts an Attacker can make on any Subscriber's account to 100 or fewer in any 30 day period.

6. If the IDPO issues look-up secret tokens, then one of the following requirements on such tokens must be met.

   a. The IDPO must have established and well-documented policies, procedures, and mechanisms to ensure that every token authenticator has 64 bits of entropy.

   b. The IDPO must have established and well-documented policies, procedures, and mechanisms to ensure that every token authenticator has at least 20 bits of entropy, and the Verifier implements a throttling mechanism that

effectively limits the number of failed authentication attempts an Attacker can make on any Subscriber's account to 100 or fewer in any 30 day period.

7. If the IDPO issues out of band tokens, then the following requirements on such tokens apply.

    a. The IDPO must have established and well-documented policies, procedures, and mechanisms to ensure that every token is uniquely addressable and supports communication over a channel that is separate from the primary channel for e-authentication.

    b. The IDPO must have established and well-documented policies, procedures, and mechanisms to ensure that every Verifier generated secret meets one of the following requirements.

        i. It must have at least 64 bits of entropy.

        ii. It must have at least 20 bits of entropy, and the Verifier must implement a throttling mechanism that effectively limits the number of failed authentication attempts an Attacker can make on any Subscriber's account to 100 or fewer in any 30 day period.

8. If the IDPO issues single factor one-time password device tokens, then the following requirements on such tokens apply.

    a. The IDPO must have established and well-documented policies, procedures, and mechanisms to ensure that every device uses a block cipher or hash function that is an Approved Cryptographic Method[6] to combine a symmetric key stored on the device with a nonce to generate a one-time password.

    b. The IDPO must have established and well-documented policies, procedures, and mechanisms to ensure that every one-time password generated by every device has a limited lifetime, on the order of minutes.

    c. The IDPO must have established and well-documented policies, procedures, and mechanisms to ensure that every cryptographic module performing the verifier function is validated at FIPS 140-2 Level 1 or higher.[7]

    d. The IDPO must have established and well-documented policies, procedures, and mechanisms to ensure that every device generates a nonce from either a date and time or a counter generated on the device.

[6] See the definition of Approved Cryptographic Method in Section 6.
[7] http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf

9. If the IDPO issues single factor cryptographic device tokens, then it must have established and well-documented policies, procedures, and mechanisms to ensure that every cryptographic module on every device is validated at FIPS 140-2 Level 1 or higher[8], and verifier-generated token input (e.g., a nonce or challenge) has at least 64 bits of entropy.

4.1.3 LOA 2 Token and Credential Management Trust Criteria Requirements

1. If the IDPO stores files containing shared secrets related to credentials, then the following requirements apply.

    a. The IDPO must have established and well-documented policies, procedures, and mechanisms to ensure that those files are protected by access controls that limit access to administrators and only to those applications that require access.

    b. The IDPO must have established and well-documented policies, procedures, and mechanisms to ensure that the shared secrets in those files are stored using one of the following acceptable non-plaintext storage schemes.

        i. Passwords may be concatenated to a variable salt (variable across a group of passwords that are stored together) and then hashed with an algorithm that is an Approved Cryptographic Method[9] so that the computations used to conduct a dictionary or exhaustion attack on a stolen password file are not useful to attack other similar password files. The hashed passwords are then stored in the password file. The variable salt may be composed using a global salt (common to a group of passwords) and the username (unique per password) or some other technique to ensure uniqueness of the salt within the group of passwords.

        ii. Shared secrets may be stored in encrypted form using encryption algorithms and modes that are Approved Cryptographic Methods[10], and the needed secret decrypted only when immediately required for authentication.

2. The IDPO must have established and well-documented policies, procedures, and mechanisms to ensure that long term shared authentication secrets, if used, are never revealed to any party except the Subscriber and IDPO (including Verifiers operated as a part of the IDPO). Also, the IDPO must have established and well-documented policies, procedures, and mechanisms to ensure that cryptographic protections are required for all messages between the IDPO and Verifier that

[8] http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf
[9] See the definition of Approved Cryptographic Method in Section 6.
[10] See the definition of Approved Cryptographic Method in Section 6.

contain private credentials or assert the validity of weakly bound or potentially revoked credentials, as follows.

a. Private credentials shall only be sent through a protected channel to an authenticated party to ensure confidentiality and tamper protection.

b. The IDPO may send the Verifier a message, which either asserts that a weakly bound credential is valid, or that a strongly bound credential has not been subsequently revoked. In this case, the message shall be logically bound to the credential, and the message, the logical binding, and the credential shall all be transmitted within a single integrity protected session between the Verifier and the authenticated IDPO.

c. If revocation is an issue, the integrity protected messages shall either be time stamped, or the session keys shall expire with an expiration time no longer than that of the revocation list. Alternatively, the time stamped message, binding, and credential may all be signed by the IDPO, although, in this case, the three in combination would comprise a strongly bound credential with no need for revocation.

3. The IDPO must have established and well-documented policies, procedures, and mechanisms regarding the renewal and reissuance of tokens and credentials. These policies, procedures, and mechanisms must conform to the following additional requirements.

a. The IDPO must require that proof-of-possession of the unexpired current token be demonstrated by the Claimant prior to allowing renewal and reissuance.

b. The IDPO must prohibit passwords from being renewed (passwords may be reissued).

c. After expiry of a current token and any grace period, the IDPO must prohibit that token from being renewed or reissued.

d. Upon reissuance of a token secret, the IDPO must ensure that the secret is not set to a default or reused in any manner.

e. The IDPO must ensure that all token and credential renewal and reissuance interactions occur over a protected channel such as SSL/TLS.

4. The IDPO must have established and well-documented policies, procedures, and mechanisms regarding the revocation of tokens and credentials. These policies, procedures, and mechanisms must conform to the following additional requirements.

a. If the IDPO issues credentials or tokens, it must ensure that credentials and tokens are revoked or destroyed within 72 hours after being notified that a credential is no longer valid or a token is compromised, to ensure that a Claimant using the token cannot successfully be authenticated. Note that if the IDPO issues credentials that expire automatically within 72 hours (e.g., issues fresh certificates with a 24 hour validity period each day) then it need not provide an explicit mechanism to revoke the credentials.

b. If the IDPO registers passwords, it must ensure that the revocation or de-registration of the password can be accomplished in no more than 72 hours.

5. The IDPO must have established and well-documented policies, procedures, and mechanisms regarding the maintenance of records pertaining to the registration, history, and status of each token and credential (including revocation). These policies, procedures, and mechanisms must conform to the following additional requirements.

    a. The IDPO must maintain records pertaining to the registration, history, and status of each token and credential (including revocation) for at least seven years and six months beyond the expiration or revocation (whichever is later) of the credential.

    b. If the IDPO is operated by or on behalf of an agency within the executive branch of the U.S. Government, then it must follow either the General Records Schedule established by the National Archives and Records Administration or an agency-specific schedule as applicable. Otherwise, the IDPO shall comply with its respective records retention policies in accordance with whatever laws apply to it.

6. The IDPO must have established and well-documented policies, procedures, and mechanisms for token collection, to avoid the possibility of unauthorized use of the token after it is considered out of use.

4.1.4 LOA 2 Authentication Process Trust Criteria Requirements

1. The IDPO must have established and well-documented policies, procedures, and mechanisms to protect against an Attacker performing repeated logon trials by guessing possible values of the token authenticator, and thereby resist the threat of online guessing.

2. The IDPO must have established and well-documented policies, procedures, and mechanisms to protect against an Attacker being able to replay previously captured messages (between a legitimate Claimant and a Verifier) to authenticate as that Claimant to the Verifier, and thereby resist the threat of replay.

3. The IDPO must have established and well-documented policies, procedures, and mechanisms to protect against an Attacker being able to take over an already authenticated session by eavesdropping on or predicting the value of authentication cookies used to mark HTTP requests sent by the Subscriber, and thereby resist the threat of session hijacking.

4. The IDPO must have established and well-documented policies, procedures, and mechanisms to protect against an attack in which an Attacker listens passively to the authentication protocol to capture information that can be used in a subsequent active attack to masquerade as the Claimant, and thereby resist the threat of eavesdropping. These policies, procedures, and mechanisms must require the use of an Approved Cryptographic Method[11] to resist eavesdropping.

5. The IDPO must have established and well-documented policies, procedures, and mechanisms to protect against an attack on the authentication protocol in which the Attacker positions himself in between the Claimant and Verifier so that he can intercept and alter data traveling between them, and thereby weakly resist the threat of a man-in-the-middle. Note that a protocol is said to be weakly resistant to man-in-the-middle attacks if it provides a mechanism for the Claimant to determine whether he or she is interacting with the real Verifier, but still leaves the opportunity for the non-vigilant Claimant to reveal a token authenticator (to an unauthorized party) that can be used to masquerade as the Claimant to the real Verifier.

6. The IDPO must have established and well-documented policies, procedures, and mechanisms to ensure that successful authentication requires a Claimant to prove, through a secure authentication protocol, that he or she actually possesses and controls the token.

7. The IDPO must have established and well-documented policies, procedures, and mechanisms to ensure that plaintext passwords or secrets are not transmitted across a network.

8. The IDPO must have established and well-documented policies, procedures, and mechanisms to ensure that its authentication processes provide sufficient information to its Verifier so it can uniquely identify each Subscriber and the appropriate registration information that was provided by each Subscriber at the time of registration, and verified by the RA in the issuance of the token and credential.

9. The IDPO must have established and well-documented policies, procedures, and mechanisms to ensure adequate protection of session data exchanged between the Claimant and the SPO.

[11] See the definition of Approved Cryptographic Method in Section 6.

4.2 NIST/FICAM Non-PKI Level of Assurance 3 Requirements for IDPOs

These requirements apply only to FICAM LOA 3 IDPOs. They are derived from Appendix A-3 of [FICAM TFPAP][12]. Audits of IDPOs at LOA 3 must be conducted via an in-person interview with a representative of the IDPO.

4.2.1 LOA 3 Identity Registration and Issuance Trust Criteria Requirements

1. The IDPO must have established and well-documented policies, procedures, and mechanisms to ensure that a trusted relationship always exists between the RA and the IDPO. Mechanisms and policies must be in place to ensure each party knows the other party and its obligations.

2. The IDPO must have established and well-documented policies, procedures, and mechanisms to ensure that a trusted RA performs identity proofing of Applicants. This must include specific identifying materials and/or other information that is acceptable for proving the Applicant's identity.

3. The IDPO must have established and well-documented policies, procedures, and mechanisms to ensure that identity tokens are issued in a manner that protects the confidentiality of information, and thereby resist the threat of token issuance disclosure.

4. The IDPO must have established and well-documented policies, procedures, and mechanisms to allow the Subscriber (user or token recipient) to authenticate the IDPO as the source of any token and credential data that he or she may receive, and thereby resist the threat of token issuance tampering.

5. The IDPO must have established and well-documented policies, procedures, and mechanisms to ensure that the individual who receives the token is the same individual who participated in the registration procedure, and thereby resist the threat of unauthorized token issuance.

6. The IDPO must have established and well-documented policies, procedures, and mechanisms to protect against a Subscriber denying registration, claiming that they did not register that token, and thereby resist the threat of repudiation of registration.

7. The IDPO must have established and well-documented policies, procedures, and mechanisms to protect sensitive data, including PII[13], obtained during registration and identity proofing. Sensitive data collected during the registration and identity-proofing stage must be protected at all times (e.g., during transmission and storage) to ensure its security and privacy.

[12] http://www.idmanagement.gov/sites/default/files/documents/FICAM_TFS_TFPAP_0.pdf
[13] See the definition of PII in Section 6.

8. The IDPO must have established and well-documented policies, procedures, and mechanisms to ensure that all identity proofing information (which may include background investigations of the Applicant) comes from known, trusted sources and is sufficiently protected to ensure authentication, confidentiality and integrity.

9. The IDPO must have established and well-documented policies, procedures, and mechanisms to ensure that either the RA or the IDPO maintains a record of each individual whose identity has been verified, and the steps taken to verify his or her identity, including any information collected from the Applicant.

10. The IDPO must have established and well-documented policies, procedures, and mechanisms to ensure that it has the capability to provide records of identity proofing to SPOs as necessary, including detailed records of registration and credential issuance.

11. The IDPO must have a written identity proofing and registration policy or practice statement that specifies the particular steps taken to verify identities, and it must submit this document to NIEF.

12. If the RA and IDPO are remotely located, and communicate over a network, then the IDPO must have established and well-documented policies, procedures, and mechanisms to ensure that the entire registration transaction between the RA and IDPO is cryptographically authenticated using an authentication protocol that meets NIST LOA 3 requirements, and that any secrets transmitted are encrypted using an Approved Cryptographic Method[14].

13. The IDPO must have established and well-documented policies, procedures, and mechanisms to ensure that the IDPO can uniquely identify each Subscriber and the associated tokens and the credentials issued to that Subscriber. Also, the IDPO must have established and well-documented policies, procedures, and mechanisms to ensure that it is capable of conveying this information to Verifiers and SPOs.

14. The IDPO must have established and well-documented policies, procedures, and mechanisms to ensure that the names associated with Subscribers are meaningful (verified real names, not pseudonyms).

15. The IDPO must have established and well-documented policies, procedures, and mechanisms to ensure that PII collected during registration and identity proofing is protected.

16. The IDPO must have established and well-documented policies, procedures, and mechanisms to require that an Applicant supply his or her full legal name, an address of record, and date of birth during the identity proofing process.

[14] See the definition of Approved Cryptographic Method in Section 6.

17. If the IDPO performs in-person identity proofing, then the following requirements apply.

    a. The IDPO must have established and well-documented policies, procedures, and mechanisms to require that each Applicant presents a verified current primary Government Picture ID that contains the Applicant's picture, and either address of record or nationality (e.g., driver's license or Passport).

    b. The IDPO must have established and well-documented policies, procedures, and mechanisms to require the RA to inspect the photo-ID; compare the picture to the Applicant; record the ID number, address and date of birth; and verify via the issuing government agency or through credit bureaus or similar databases that the name, date of birth, address and other personal information in record are consistent with the application.

    c. IDPO must have established and well-documented policies, procedures, and mechanisms to ensure that if the ID appears valid and the photo matches the Applicant, then credentials issuance is conducted through one of the following processes.

        i. If the personal information in the Applicant's records includes a telephone number, then the conducts credential issuance in a manner that confirms the Applicant's ability to receive communications at the telephone number, and establishes a level of non-repudiation equivalent to recording the Applicant's voice.

        ii. If the ID confirms the Applicant's address of record, then the IDPO shall issue credentials and ensure that notice of credential issuance is sent to the Applicant's address of record.

        iii. If the ID does not confirm the Applicant's address of record, then the IDPO ensures that credential issuance is conducted in a manner that confirms the Applicant's address of record.

18. If the IDPO performs remote identity proofing, then the following requirements apply.

    a. The IDPO must have established and well-documented policies, procedures, and mechanisms to require that each Applicant presents a valid Government ID (e.g., a driver's license or Passport) number and a financial or utility account number (e.g., checking account, savings account, loan, or credit card) with confirmation via records of both numbers.

    b. The IDPO must have established and well-documented policies, procedures, and mechanisms to require the RA to verify the information provided by

Applicant, including ID number and account number, through record checks either with the applicable agencies or institutions, or through credit bureaus or similar databases, and confirm that name, date of birth, address, and other personal information in records are consistent with the application and sufficient to identify a unique individual.

c. If the IDPO allows the use of utility accounts numbers in the identity proofing process, then it must have established and well-documented policies, procedures, and mechanisms to require that utility account numbers are confirmed by verifying the Applicant's knowledge of recent account activity.

d. The IDPO must have established and well-documented policies, procedures, and mechanisms to require that the RA perform address confirmation and notification through one of the following processes.

   i. Issue credentials in a manner that confirms the ability of the Applicant to receive mail at a physical address that is in the Applicant's records.

   ii. If personal information in records includes both an electronic address and a physical address that are linked together with the Applicant's name, and are consistent with the information provided by the Applicant, then issue credentials in a manner that confirms the ability of the Applicant to receive SMS, voice, or email messages sent to the electronic address. In addition, any secret sent over an unprotected session must be reset upon first use and must be valid for a maximum lifetime of seven days.

e. The IDPO may allow the requirement for a financial or utility account number to be satisfied by a cellular or landline telephone service account only if the IDPO has established and well-documented policies, procedures, and mechanisms to ensure the phone is associated in records with the Applicant's name and address, and the Applicant demonstrates that he/she is able to send or receive messages at the phone number.

19. The IDPO must have established and well-documented policies, procedures, and mechanisms to ensure that the same party acts as Applicant throughout the identity registration and issuance process. [15] In addition, the IDPO must enforce one of the following policies.

    a. The Applicant shall identify himself/herself in any new electronic transaction by presenting a temporary secret that was established during a prior transaction or encounter, or sent to the Applicant's phone number, email

[15] Registration, identity proofing, and token and credential issuance represent different goals of the same process. In many cases, however, this process may be broken up into a number of separate physical encounters and electronic transactions. Two electronic transactions are considered to be separate if they are not part of the same protected session.

address, or physical address of record. Permanent secrets shall only be issued to the Applicant within a protected session.

b. The Applicant shall identify himself/herself in person by either using a secret as described above, or through the use of a biometric that was recorded during a prior encounter. Temporary secrets shall not be reused. If the IDPO issues permanent secrets during a physical transaction, then they shall be 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.

20. If the IDPO rigorously confirms the identity, education, and licensing credentials of a licensed professional in accordance with federal or state law or regulations, and through an in-person appearance prior to employment or affiliation, then the IDPO may issue e-authentication tokens and credentials to such employees and affiliates, without repeating the identity proofing process, in accordance with the following requirements.

    a. The IDPO must have established and well-documented policies, procedures, and mechanisms to ensure that the initial process for confirming the identity, education, and licensing credentials of the licensed professional includes the following steps.

        i. The IDPO verifies the employee or affiliate has a current primary government picture ID that contains the applicant's picture, and either address or nationality of record (e.g., a driver's license or passport).

        ii. The IDPO verifies two or more years of post-secondary education or training appropriate for the professional's position (e.g., an appropriate medical degree).

        iii. The IDPO verifies that the state or federal licensure of the employee or affiliate (e.g., as a physician) is current, is based on an examination process, and includes requirements for continuing education or active professional participation as a condition of valid licensing.

    b. The IDPO must have established and well-documented policies, procedures, and mechanisms to ensure that it issues e-authentication tokens and credentials to employees and affiliates either in person, or via a remote issuance process that incorporates the address and phone number confirmation as appropriate for LOA 3.

    c. The IDPO must meet the corresponding Token Trust Criteria Requirements (see Section 4.1.2), Token and Credential Management Trust Criteria Requirements (see Section 4.1.3), and Authentication Process Trust Criteria Requirements (see Section 4.1.4).

d. The IDPO must deploy systems that conform to the NIEF Web Browser User-to-System Profile, which is a profile of SAML 2.0 that conforms to (and further constrains) the FICAM SAML SSO Profile.

21. If the IDPO issues PKI credentials, then it must have established and well-documented policies, procedures, and mechanisms to ensure that it issues these credentials from a certificate authority that is cross-certified with the Federal Bridge Certification Authority (FBCA) under the FBCA Certificate Policy, Common Certificate Policy, or a policy mapped to one of those policies.

4.2.2 LOA 3 Token Trust Criteria Requirements

Auditor Requirements:

1. When a multi-token authentication scheme is being used, the new level of assurance must be determined in accordance with NIST SP 800-63-2 Table 7. Using multiple tokens to achieve an increased level of assurance requires the use of two different factors of authentication. Combining multiple factors and/or multiple tokens may achieve a higher assurance level than would otherwise be attained. If one factor of a multi-factor scheme or one token of a multi-token scheme has the desired properties for a given assurance level, it is considered sufficient. LOA 3 can be achieved using two tokens rated at LOA 2 that represent two different authentication factors. Since the use of biometrics as a stand-alone token for remote authentication is not addressed, achieving LOA 3 with separate LOA 2 tokens requires the use of something you have and something you know.

2. Multi-stage authentication processes, which use a single-factor token to obtain a second token, must not constitute multi-factor authentication. The level of assurance associated with the compound solution is the assurance level of the weakest token.

IDPO Requirements:

1. The IDPO must have established and well-documented policies, procedures, and mechanisms to protect tokens that have a physical manifestation (e.g., one time password device, hardware cryptographic device) against an Attacker, and thereby resist the threat of token theft.

2. The IDPO must have established and well-documented policies, procedures, and mechanisms to protect against a Subscriber's token being copied by an Attacker, with or without his or her knowledge, and thereby resist the threat of token duplication.

3. The IDPO must have established and well-documented policies, procedures, and mechanisms to protect against an Attacker establishing a level of trust with a

Subscriber in order to convince the Subscriber to reveal his or her token or token secret, and thereby resist the threat of social engineering.

4. If the IDPO issues multi-factor software cryptographic tokens, then the following requirements on such tokens apply.

    a. The IDPO must have established and well-documented policies, procedures, and mechanisms to ensure that the tokens are validated at FIPS 140-2 Level 1 or higher.

    b. The IDPO must have established and well-documented policies, procedures, and mechanisms to ensure that each authentication requires entry of the password or other activation data and the unencrypted copy of the authentication key is erased after each authentication.

    c. The IDPO must have established and well-documented policies, procedures, and mechanisms to ensure that verifier-generated token inputs (e.g., a nonce or challenge) has at least 64 bits of entropy.

4.2.3 LOA 3 Token and Credential Management Trust Criteria Requirements

1. If the IDPO stores files containing shared secrets related to credentials, then the following requirements apply.

    a. The IDPO must have established and well-documented policies, procedures, and mechanisms to ensure that those files are protected by access controls that limit access to administrators and only to those applications that require access.

    b. The IDPO must have established and well-documented policies, procedures, and mechanisms to ensure that the shared secrets in those files are stored in an encrypted form, according to the following guidelines.

        i. The encryption key for the shared secret file must be encrypted under a key held in a FIPS 140-2 Level 2 or higher validated hardware cryptographic module or any FIPS 140-2 Level 3 or 4 cryptographic module and decrypted only as immediately required for an authentication operation.

        ii. Shared secrets must be protected as a key within the boundary of a FIPS 140-2 Level 2 or higher validated hardware cryptographic module or any FIPS 140-2 Level 3 or 4 cryptographic module and must not be exported in plaintext from the module.[16]

[16] http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf

2. The IDPO must have established and well-documented policies, procedures, and mechanisms to allow Verifiers or Relying Parties to ensure that the credentials that it issues are valid. Note that according to FICAM guidelines, such mechanisms may include on-line validation servers or the involvement of IDPO servers that have access to status records in authentication transactions. Temporary session authentication keys may be generated from long-term shared secret keys by IDPOs and distributed to third party Verifiers, as a part of the verification services offered by the IDPO, but long-term shared secrets shall not be shared with any third parties, including third party Verifiers. The use of Approved Cryptographic Methods[17] is required for all operations.

3. The IDPO must have established and well-documented policies, procedures, and mechanisms to ensure that renewal and reissuance can only occur prior to expiration of the current credential. In addition, the IDPO must have established and well-documented policies, procedures, and mechanisms to require Claimants to authenticate to the IDPO using the existing token and credential in order to renew or reissue the credential. In addition, the IDPO must have established and well-documented policies, procedures, and mechanisms to require that all interactions occur over a protected channel such as SSL/TLS.

4. The IDPO must have established and well-documented policies, procedures, and mechanisms to ensure that it can revoke credentials and tokens within 24 hours. Also, the IDPO must have established and well-documented policies, procedures, and mechanisms to help Verifiers to ensure that the tokens they rely upon are either freshly issued (within 24 hours) or still valid.

5. The IDPO must have established and well-documented policies, procedures, and mechanisms regarding the maintenance of records pertaining to the registration, history, and status of each token and credential (including revocation). In addition, the following requirements apply on this topic.

    a. The IDPO must maintain records pertaining to the registration, history, and status of each token and credential (including revocation) for at least seven years and six months beyond the expiration or revocation (whichever is later) of the credential.

    b. If the IDPO is operated by or on behalf of an agency within the executive branch of the U.S. Government, then it must follow either the General Records Schedule established by the National Archives and Records Administration or an agency-specific schedule as applicable.

    c. All other IDPOs must comply with their respective records retention policies in accordance with whatever laws apply to those entities.

[17] See the definition of Approved Cryptographic Method in Section 6.

6. The IDPO must have established and well-documented policies, procedures, and mechanisms for token collection, to avoid the possibility of unauthorized use of the token after it is considered out of use.

4.2.4 LOA 3 Authentication Process Trust Criteria Requirements

1. The IDPO must have established and well-documented policies, procedures, and mechanisms to protect against an Attacker performing repeated logon trials by guessing possible values of the token authenticator, and thereby resist the threat of online guessing.

2. The IDPO must have established and well-documented policies, procedures, and mechanisms to protect against an Attacker being able to replay previously captured messages (between a legitimate Claimant and a Verifier) to authenticate as that Claimant to the Verifier, and thereby resist the threat of replay.

3. The IDPO must have established and well-documented policies, procedures, and mechanisms to protect against an Attacker being able to take over an already authenticated session by eavesdropping on or predicting the value of authentication cookies used to mark HTTP requests sent by the Subscriber, and thereby resist the threat of session hijacking.

4. The IDPO must have established and well-documented policies, procedures, and mechanisms to protect against an attack in which an Attacker listens passively to the authentication protocol to capture information that can be used in a subsequent active attack to masquerade as the Claimant, and thereby resist the threat of eavesdropping. These policies, procedures, and mechanisms must require the use of Approved Cryptographic Methods[18] to resist eavesdropping.

5. The IDPO must have established and well-documented policies, procedures, and mechanisms to protect against a phishing attack in which the Subscriber is lured (usually through an email) to interact with a counterfeit Verifier, and tricked into revealing information that can be used to masquerade as that Subscriber to the real Verifier. In addition, the IDPO must have established and well-documented policies, procedures, and mechanisms to protect against a pharming attack in which an Attacker corrupts an infrastructure service such as DNS (Domain Name Service) causing the Subscriber to be misdirected to a forged Verifier/SPO, and revealing sensitive information, downloading harmful software or contributing to a fraudulent act.

6. The IDPO must have established and well-documented policies, procedures, and mechanisms to protect against an attack on the authentication protocol in which the Attacker positions himself in between the Claimant and Verifier so that he can intercept and alter data traveling between them, and thereby weakly resist the

[18] See the definition of Approved Cryptographic Method in Section 6.

threat of a man-in-the-middle. Note that a protocol is said to be weakly resistant to man-in-the-middle attacks if it provides a mechanism for the Claimant to determine whether he or she is interacting with the real Verifier, but still leaves the opportunity for the non-vigilant Claimant to reveal a token authenticator (to an unauthorized party) that can be used to masquerade as the Claimant to the real Verifier.

7. The IDPO must have established and well-documented policies, procedures, and mechanisms to ensure that at least two authentication factors are used when authenticating Claimants.

8. The IDPO must have established and well-documented policies, procedures, and mechanisms to ensure that successful authentication requires a Claimant to prove, through a secure, cryptographic authentication protocol, that he or she actually possesses and controls a token or series of tokens allowed at LOA 3.

9. The IDPO must have established and well-documented policies, procedures, and mechanisms to ensure that strong cryptographic mechanisms are used to protect token secrets and authenticators.

10. The IDPO must have established and well-documented policies, procedures, and mechanisms to ensure that long term shared authentication secrets, if used, are never revealed to any party except the Claimant and IDPO. However, session (temporary) shared secrets may be provided to Verifiers by the IDPO, possibly via the Claimant.

11. The IDPO must have established and well-documented policies, procedures, and mechanisms to ensure that plaintext passwords or secrets are not transmitted across a network.

12. The IDPO must have established and well-documented policies, procedures, and mechanisms to ensure that its authentication processes provide sufficient information to its Verifier so it can uniquely identify each Subscriber and the appropriate registration information that was provided by each Subscriber at the time of registration, and verified by the RA in the issuance of the token and credential.

13. The IDPO must have established and well-documented policies, procedures, and mechanisms to ensure adequate protection of data transmitted between the Claimant and the SPO. Protection mechanisms must address transmission confidentiality and integrity.

14. The IDPO must have established and well-documented policies, procedures, and mechanisms to ensure that Approved Cryptographic Methods[19] are used for all operations including the transfer of session data.

4.3 NIEF-Specific Requirements about Local Security Policies and Practices

These requirements apply to all NIEF applicants and member agencies. They are derived from the Security Practices Checklist that each NIEF applicant is required to submit as part of its application package. If the agency is, or is applying to become, a FICAM LOA 2 IDPO or a FICAM LOA 3 IDPO, then it MUST meet each of these requirements. All other NIEF member agencies SHOULD meet these requirements.

1. **Access Control (AC)** – The agency has well-documented policies, procedures, and mechanisms to limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems) and to the types of transactions and functions that authorized users are permitted to exercise.

2. **Awareness and Training (AT)** – The agency has well-documented policies, procedures, and mechanisms to: (i) ensure that managers and users of organizational information systems are made aware of the security risks associated with their activities and of the applicable laws, Executive Orders, directives, policies, standards, instructions, regulations, or procedures related to the security of organizational information systems; and (ii) ensure that organizational personnel are adequately trained to carry out their assigned information security-related duties and responsibilities.

3. **Audit and Accountability (AU)** – The agency has well-documented policies, procedures, and mechanisms to: (i) create, protect, and retain information system audit records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful, unauthorized, or inappropriate information system activity; and (ii) ensure that the actions of individual information system users can be uniquely traced to those users so they can be held accountable for their actions.

4. **Certification, Accreditation, and Security Assessments (CA)** – The agency has well-documented policies, procedures, and mechanisms to: (i) periodically assess the security controls in organizational information systems to determine whether the controls are effective in their application; (ii) develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in organizational information systems; (iii) authorize the operation of organizational information systems and any associated information system connections; and (iv) monitor information system security controls on an ongoing basis to ensure the continued effectiveness of the controls.

[19] See the definition of Approved Cryptographic Method in Section 6.

5. **Configuration Management (CM)** – The agency has well-documented policies, procedures, and mechanisms to: (i) establish and maintain baseline configurations and inventories of organizational information systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles; and (ii) establish and enforce security configuration settings for information technology products employed in organizational information systems.

6. **Contingency Planning (CP)** – The agency has well-documented policies, procedures, and mechanisms to establish, maintain, and effectively implement plans for emergency response, backup operations, and post-disaster recovery for organizational information systems to ensure the availability of critical information resources and the continuity of operations in emergency situations.

7. **Identification and Authentication (IA)** – The agency has well-documented policies, procedures, and mechanisms to identify information system users, processes acting on behalf of users, or devices and authenticate (or verify) the identities of those users, processes, or devices, as a prerequisite to allowing access to organizational information systems.

8. **Incident Response (IR)** – The agency has well-documented policies, procedures, and mechanisms to: (i) establish an operational incident handling capability for organizational information systems that includes adequate preparation, detection, analysis, containment, recovery, and user response activities; and (ii) track, document, and report incidents to appropriate organizational officials and/or authorities.

9. **Maintenance (MA)** – The agency has well-documented policies, procedures, and mechanisms to: (i) perform periodic and timely maintenance on organizational information systems; and (ii) provide effective controls on the tools, techniques, mechanisms, and personnel used to conduct information system maintenance.

10. **Media Protection (MP)** – The agency has well-documented policies, procedures, and mechanisms to: (i) protect information system media, both paper and digital; (ii) limit access to information on information system media to authorized users; and (iii) sanitize or destroy information system media before disposal or release for reuse.

11. **Physical and Environmental Protection (PE)** – The agency has well-documented policies, procedures, and mechanisms to: (i) limit physical access to information systems, equipment, and the respective operating environments to authorized individuals; (ii) protect the physical plant and support infrastructure for information systems; (iii) provide supporting utilities for information systems; (iv) protect information systems against environmental hazards; and (v) provide appropriate environmental controls in facilities containing information systems.

12. **Planning (PL)** – The agency has well-documented policies, procedures, and mechanisms to develop, document, periodically update, and implement security plans for organizational information systems that describe the security controls in place or planned for the information systems and the rules of behavior for individuals accessing the information systems.

13. **Personnel Security (PS)** – The agency has well-documented policies, procedures, and mechanisms to: (i) ensure that individuals occupying positions of responsibility within organizations (including third-party service providers) are trustworthy and meet established security criteria for those positions; (ii) ensure that organizational information and information systems are protected during and after personnel actions such as terminations and transfers; and (iii) employ formal sanctions for personnel failing to comply with organizational security policies and procedures.

14. **Risk Assessment (RA)** – The agency has well-documented policies, procedures, and mechanisms to periodically assess the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals, resulting from the operation of organizational information systems and the associated processing, storage, or transmission of organizational information.

15. **System and Services Acquisition (SA)** – The agency has well-documented policies, procedures, and mechanisms to: (i) allocate sufficient resources to adequately protect organizational information systems; (ii) employ system development life-cycle processes that incorporate information security considerations; (iii) employ software usage and installation restrictions; and (iv) ensure that third-party providers employ adequate security measures to protect information, applications, and/or services outsourced from the organization.

16. **System and Communications Protection (SC)** – The agency has well-documented policies, procedures, and mechanisms to: (i) monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems; and (ii) employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational information systems.

17. **System and Information Integrity (SI)** – The agency has well-documented policies, procedures, and mechanisms to: (i) identify, report, and correct information and information system flaws in a timely manner; (ii) provide protection from malicious code at appropriate locations within organizational information systems; and (iii) monitor information system security alerts and advisories and take appropriate actions in response.

4.4 NIEF-Specific Privacy Requirements

These requirements are derived from the NIEF Privacy Policy. For each applicable requirement, a NIEF member agency either MUST or SHOULD have established and well-documented policies, procedures, and mechanisms to ensure its compliance with the requirement, depending on whether the requirement is marked as REQUIRED or RECOMMENDED. Applicability to specific types of agencies is noted for each requirement.

1. **Opt-In**

    a. [REQUIRED For FICAM LOA 2 IDPOs and FICAM LOA 3 IDPOs; RECOMMENDED for Non-FICAM IDPOs] – Ensure that the IDPO obtains positive confirmation from the End User before any End User information is transmitted to any NIEF Service Provider Organization (SPO) or Federal relying party systems. The IDPO must obtain confirmation at "run-time" (just before the information is transmitted).

    b. [REQUIRED For FICAM LOA 2 IDPOs and FICAM LOA 3 IDPOs; RECOMMENDED for Non-FICAM IDPOs] – Ensure that the End User can see each attribute that is to be transmitted as part of the Opt-In process. The IDPO must allow the End User to see this information at run-time.

    c. [RECOMMENDED For FICAM LOA 2 IDPOs, FICAM LOA 3 IDPOs, and Non-FICAM IDPOs] – Allow the End User to opt out of individual attributes for each transaction.

2. **Minimal Attribute Release** [REQUIRED For FICAM LOA 2 IDPOs, FICAM LOA 3 IDPOs, and APOs; RECOMMENDED for Non-FICAM IDPOs] – Ensure that NIEF-facing systems transmit only attributes that were explicitly requested by a NIEF SPO or NIEF Member Organization. Ensure that Federal relying party facing systems transmit only attributes that were explicitly requested by a Federal relying party.

3. **Activity Tracking** [REQUIRED For FICAM LOA 2 IDPOs, FICAM LOA 3 IDPOs, and APOs; RECOMMENDED for Non-FICAM IDPOs] – Ensure that the IDPO does not disclose information on End User activities with NIEF SPOs or Federal relying parties to any party, or use the information for any purpose other than federated authentication, audit, and privilege management.

4. **Adequate Notice**

    a. [REQUIRED For FICAM LOA 2 IDPOs and FICAM LOA 3 IDPOs; RECOMMENDED for Non-FICAM IDPOs] – Ensure that the IDPO provides the End User with adequate notice regarding federated authentication. Note that "Adequate Notice" includes a general description of the authentication event, any transaction(s) with the NIEF SPO or Federal relying party, the purpose of the transaction(s), and a description of any disclosure or transmission of PII to any party.

b. [RECOMMENDED For FICAM LOA 2 IDPOs, FICAM LOA 3 IDPOs, and Non-FICAM IDPOs] – Incorporate the IDPO's Adequate Notice policies, procedures, and mechanisms into its Opt-In process.

5. **Termination** [REQUIRED For FICAM LOA 2 IDPOs, FICAM LOA 3 IDPOs, and APOs; RECOMMENDED for Non-FICAM IDPOs] – Ensure that the agency continues to protect any sensitive data about the End User, e.g., within audit logs or elsewhere, in the event that it ceases to provide its services to the End User.

6. **Appropriate Attribute Request and Usage** [REQUIRED For All NIEF Members] – Ensure that the agency requests only those attributes that it requires for the purposes of making authorization decisions, dynamically provisioning accounts, performing audit logging, or forwarding the attributes to another NIEF member for these purposes. In addition, ensure that the agency uses requested attributes only for the purposes of making authorization decisions, dynamically provisioning accounts, performing audit logging or forwarding the attributes to another NIEF member for these purposes.

4.5 Adoption of FICAM Privacy Assessor and Auditor Guidance

NIEF has accepted FICAM Privacy Guidance for Trust Framework Assessors and Auditors Version 1.0 as an assessment guide. The guide should be used by Assessors and Auditors when determining whether an IDPO intending to interact with Federal agency applications should be approved, and during re-assessment audits required for renewal of a certification. The full guide can be found on the Federal Identity, Credential and Access Management home page or by following this link.

http://www.idmanagement.gov/sites/default/files/documents/Guidance_for_Assessors.pdf

4.6 NIEF-Specific Financial Requirements

1. FICAM LOA 2 IDPOs and FICAM LOA 3 IDPOs must provide evidence of Directors & Officers (D&O) liability insurance at a minimum level of $1 million, as well as Errors & Omissions (E&O) liability insurance at a minimum level of $2 million.

2. It is recommended that all other NIEF applicants and member agencies carry general liability insurance in an amount sufficient to manage the financial risks associated with their participation in NIEF.

4.7 Miscellaneous NIEF-Specific Requirements

If the agency is, or is applying to become, a FICAM LOA 2 IDPO or a FICAM LOA 3 IDPO, then it MUST have well-documented policies, procedures, and mechanisms to ensure that it meets each of these requirements. All other NIEF member agencies SHOULD meet these requirements.

1. Ensure that the agency will notify the NIEF Center and submit appropriate updated documentation to the NIEF Center in a timely fashion (no later than 72 hours before the change is scheduled to take effect) if any of its submitted local policies or procedures documents should change, as documented in the NIEF Operational Policies and Procedures document. Please note that for Trusted Identity Broker Organizations (TIBOs), this includes any policies, procedures, and mechanisms that the agency has established regarding IDPOs that it brokers into NIEF.

2. Ensure the adequate protection of private key material corresponding to certificates that belong to the agency and appear within the NIEF Trust Fabric. This includes all applicable aspects of key material protection, including physical access to facilities and servers, logical access to servers via networks, logical access control mechanisms, background checks for staff members, etc. This requirement is derived from the NIEF Center Certificate Policy.

3. Ensure that the agency's NIEF-facing systems conform to the rules for "Import and Consumption of Trust Fabric by Federation Members", as documented in the NIEF Cryptographic Trust Model spec.

4. Ensure that the agency's NIEF-facing systems conform to the rules for "Minimum Required Cryptographic Algorithms and Modules", as documented in the NIEF Cryptographic Trust Model spec. Also, the agency's NIEF-facing systems must use FIPS 140-2 validated cryptographic modules for all encryption and digital signature operations.

In addition, the agency may submit supplementary audit reports or auditors' letters of opinion to the NIEF Center, as further proof of its compliance with its basic IT and security policies beyond the scope of identity federation and inter-agency trust. This is encouraged, but not required.

5 Fees

NIEF may, at its discretion, charge a fee for audit services performed. Please contact the NIEF Executive Director for more information.

6 Definitions

This section contains definitions for certain key words used throughout this document.

Approved Cryptographic Method - An algorithm or technique that is either (1) specified in a FIPS or NIST Recommendation, or (2) adopted in a FIPS or NIST Recommendation.

PII (Personally Identifiable Information) - Information which can be used to distinguish or trace an individual's identity, such as their name, social security number, biometric

records, etc. alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc.