CONFORMANCE CRITERIA for NIST SP 800-63A *ENROLLMENT AND IDENTITY PROOFING* and NIST SP 800-63B *AUTHENTICATION AND LIFECYCLE MANAGEMENT*

June 2020

Comments on this publication may be submitted to: dig-comments@nist.gov.

National Institute of Standards and Technology
U.S. Department of Commerce

Special Publication 800-63B Conformance Criteria

Synopsis

All normative requirements for NIST Special Publication (SP) 800-63A *Enrollment and Identity Proofing* and SP 800-63B *Authentication and Lifecycle Management* are presented in those volumes. Pursuant to Office of Management and Budget Policy Memorandum M-19-17, these Conformance Criteria present non-normative informational guidance on all normative requirements contained in those volumes for the assurance levels IAL2 and IAL3 and AAL2 and AAL3. The normative text from those volumes is restated in the Conformance Criteria for clarity of presentation. The complete set of conformance criteria are informative and intended to provide non-normative supplemental guidance to federal agencies and other organizations to facilitate implementation and assessment. The supplemental guidance is intended to provide information to clarify the normative requirement/control and provide non-normative information about how to meet conformance for purposes of implementation and assessment.

Comments or questions on the Conformance Criteria may be sent to dig-comments@nist.gov.

Introduction

This document presents conformance criteria for NIST Special Publication 800-63B *Authentication and Lifecycle Management*. This set of conformance criteria presents all normative requirements and controls for SP 800-63B for assurance levels AAL2 and AAL3.

The conformance criteria are enumerated to facilitate referencing and indexing. Similar to the indexing of the inventory of controls for NIST Special Publication 800-53 *Security and Privacy Controls for Federal Information Systems and Organizations*, the enumeration of the conformance criteria is separated into sections for criteria that apply to specific functional areas in SP 800-63A and -63B; this also is intended to facilitate referencing and indexing. An index is also provided for the complete set of conformance criteria to facilitate reference to specific topics and criteria.

All the conformance criteria are presented in the following format:

- **Requirement –** presentation of the normative requirement/control statement from SP 800-63A and SP 800-63B.
- **Supplemental guidance** – presentation of informative guidance to facilitate the understanding, implementation and assessment for each criterion.
- **Assessment objective** – Presentation of the intended objective and outcome from the assessment of conformance for each criterion.
- **Potential assessment methods and objects** – Presentation of suggested methodologies for performing conformance assessment for each criterion.
- **Potential test methods** – Where applicable, presentation of suggested test methodologies for performing conformance testing for applicable criteria.

As described above, each conformance criterion presents the normative requirement/control statement from SP 800-63B. All normative requirements are presented in SP 800-63B and are restated in the conformance criteria for clarity of presentation. The complete set of conformance criteria are informative and intended to provide non-normative supplemental guidance for implementation and assessment. The supplemental guidance is intended to provide information to clarify the normative requirement/control and provide information about how to meet conformance for purposes of implementation and assessment. The assessment objective is intended to present the requirements and controls in terms of outcomes. SP 800-63-3 applies the NIST Risk Management Framework to identity systems and operations. The risk management framework advances the principle that organizations should have the flexibility to apply and tailor controls and requirements to best meet the risk environment of the organization, its systems and operations, target populations and use cases. Therefore, the conformance criteria are not intended to be prescriptive; rather, the criteria are intended to present the intended outcomes for the requirements and controls and allow flexibility in both the implementation and assessment of the criteria. Potential assessment and test methods are presented as suggested means to achieve/assess conformance to the requirement but should be considered suggestions rather than prescribed methods. Assessors have flexibility and responsibility to determine the most appropriate conformance assessment methods for the specific organization, system and operations, and risk environment.

While NIST Special Publications and guidance materials such as these conformance criteria are intended for federal agencies, the potential audiences and uses for the conformance criteria include:

- Federal agencies for the implementation of SP 800-63-3 and assessment of implementation, risks, and controls in meeting Federal Information Security Modernization Act (FISMA) requirements and responsibilities
- Credential Service providers for the implementation of services and products to meet conformance requirements of SP 800-63-3
- Organizations and services that perform assessment and, potentially, certification of conformance with SP 800-63-3 requirements
- Audit organizations that offer and provide audit services for determining federal agency or external non-federal service provider conformance to SP 800-63-3 requirements and controls
- The General Services Administration to facilitate activities to address the responsibility in Office of Management and Budget Policy Memo M-19-17: "*Determine the feasibility, in coordination with OMB, of establishing or leveraging a public or private sector capability for accrediting ICAM products and services available on GSA acquisition vehicles, and confirm the capability leverages NIST developed criteria for 800-63 assurance levels. This capability should support and not duplicate existing Federal approval processes*."

These conformance criteria are publicly available at the NIST Identity and Access Management Resource Center: https://www.nist.gov/topics/identity-access-management. NIST anticipates that this resource may be periodically updated based on federal agency and industry experience and feedback. Questions and comments on these resources may be sent to dig-comments@nist.gov.

Digital Identity Model Roles

SP 800-63-3 Figure 4-1 presents the *Digital Identity Model* and describes the various entities and interactions that comprise the model as illustrated below.

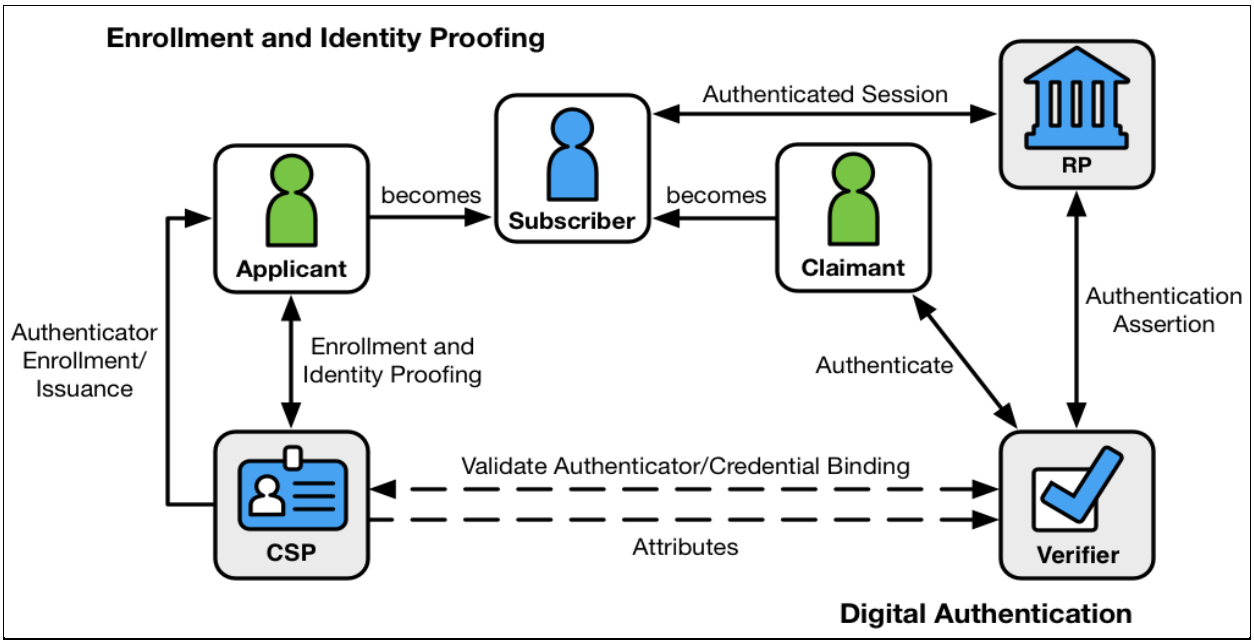

Figure 4-1 Digital Identity Model

SP 800-63A presents requirements, controls and activities to perform the identity proofing and enrollment activities depicted on the left side of Figure 4-1 *The Digital Identity Model.* After successful identity proofing, the applicant is enrolled as a subscriber in the digital identity system. As illustrated the interactions for identity proofing and enrollment are between the applicant and the Credential Service Provider (CSP). The SP 800-63A requirements and controls and, therefore, all the SP 800-63A conformance criteria apply directly to the CSP.

As illustrated on the right side of the model, following successful identity proofing in the CSP's digital identity system, the subscriber registers authenticator(s) to their account to complete enrollment. The subscriber can then prove possession and control of those authenticator(s) for digital authentication transactions. This is a functional model to illustrate the activities involved for enrollment, identity proofing and authentication and presents three entities that may interact with the subscriber for digital authentication transactions – the Relying Party (RP), Verifier, and Credential Service Provider (CSP). In this functional model, the RP, CSP and Verifier roles are depicted separately; however, all of the functional roles shown may be provided by a single entity or combinations among the three roles of RP, CSP, and Verifier. The SP 800-63B Conformance Criteria are applicable to all three roles. These roles may be performed by a single entity or may represent separate entities. In most scenarios, federal agencies serve in all three roles of *The Digital Identity Model* -- RP, CSP and Verifier. The exception to this is when a third party, such as the GSA login.gov service, provides federation services on behalf of federal agencies.

Digital identity service providers outside the federal government that voluntarily adopt SP 800-63-3 as a standard will need to examine the roles performed for digital authentication to determine the applicability of the SP 800-63B Conformance Criteria to their specific implementation.

Conditional Requirements

Some requirements in SP 800-63A and SP 800-63B are conditional based on circumstances. These requirements are characterized as follows; IF (a conditional circumstance occurs), THEN this requirement(s) shall apply. Conditional Conformance Criteria follow the same pattern in the statement of the normative requirement: IF (this conditional circumstance occurs). THEN the normative requirement and conformance criterion shall apply. Conditional conformance criteria are presented in the same format as all other criteria. Assessors will need to determine whether the conditional circumstance occurs for a specific implementation in order to determine the applicability of the conditional conformance criterion to that implementation.

Federal Agency Unique Requirements

Some requirements in SP 800-63A and SP 800-63B apply uniquely to federal agencies and the conformance criteria for these requirements clearly indicate this status. In general, these conformance criteria do not apply to entities external to the federal government that have voluntarily chosen to adopt the SP 800-63A and SP 800-63B standards or are otherwise applying the conformance criteria to the services that they provide.

Organization of criteria

The conformance criteria presented below are organized into categories roughly as SP 800-63B is organized. Not all categories will need to be evaluated in all situations. For example, the authenticator-specific criteria only apply to CSPs and verifiers that support the indicated authenticator type.

The categories are as follows:

Category	**Applicability**
AAL2	CSPs and verifiers doing authentication at AAL2
AAL3	CSPs and verifiers doing authentication at AAL3
PRIV	All CSPs, verifiers, and RPs (privacy criteria)
MS	CSPs and verifiers supporting use of memorized secrets as authenticators or as activation factors for multi-factor authenticators
LUS	CSPs and verifiers supporting look-up secret authenticators
OOB	CSPs and verifiers supporting out-of-band authenticators
OTP	CSPs and verifiers supporting single- and multi-factor OTP authenticators, including both hardware and software-based authenticators
CRYP	CSPs and verifiers supporting single- and multi-factor cryptographic authenticators (both hardware- and software-based
GEN	All CSPs and verifiers (general requirements)
BIO	All CSPs and verifiers using biometric verification for authentication, including activation of multi-factor authenticators
VIR	Verifiers implementing verifier impersonation resistance (required at AAL3)
BIND	All CSPs (requirements for binding authenticators)
SESS	All CSPs and RPs (session management requirements)

REAUTH	All CSPs, verifiers, and RPs (reauthentication requirements)

Index to AAL2 Criteria

There are 15 requirements that apply to all CSPs and verifiers supporting authentication at AAL2.

ID	63B Section		ID	63B Section
AAL2-1	4.2.1		AAL2-9	4.2.2
AAL2-2	4.2.1		AAL2-10	4.2.3
AAL2-3	4.2.2		AAL2-11	4.2.3
AAL2-4	4.2.2		AAL2-12	4.2.3
AAL2-5	4.2.2		AAL2-13	4.2.4
AAL2-6	4.2.2		AAL2-14	4.2.5
AAL2-7	4.2.2		AAL2-15	4.2.5
AAL2-8	4.2.2			

Index to AAL2 Criteria

There are 20 requirements that apply to all CSPs and verifiers supporting authentication at AAL2.

ID	63B Section		ID	63B Section
AAL3-1	4.3		AAL3-11	4.3.2
AAL3-2	4.3		AAL3-12	4.3.2
AAL3-3	4.3		AAL3-13	4.3.2
AAL3-4	4.3.1		AAL3-14	4.3.3
AAL3-5	4.3.2		AAL3-15	4.3.3
AAL3-6	4.3.2		AAL3-16	4.3.3
AAL3-7	4.2.2		AAL3-17	4.3.3
AAL3-8	4.3.2		AAL3-18	4.3.4
AAL3-9	4.3.2		AAL3-19	4.3.5
AAL3-10	4.3.2		AAL3-20	4.3.5

Index to Privacy Criteria

There are 3 privacy requirements that apply to all CSPs, verifiers, and RPs.

ID	63B Section		ID	63B Section
PRIV-1	4.3		PRIV-3	4.3.2
PRIV-2	4.3			4.3.2

Index to Memorized Secret Criteria

There are 20 requirements that apply to all CSPs and verifiers supporting use of memorized secrets as authenticators or as activation factors for multi-factor authenticators.

ID	63B Section		ID	63B Section
MS-1	5.1.1.2		MS-11	5.1.1.2
MS-2	5.1.1.2		MS-12	5.1.1.2
MS-3	5.1.1.2		MS-13	5.1.1.2
MS-4	5.1.1.2		MS-14	5.1.1.2
MS-5	5.1.1.2		MS-15	5.1.1.2
MS-6	5.1.1.2		MS-16	5.1.1.2
MS-7	5.1.1.2		MS-17	5.1.1.2
MS-8	5.1.1.2		MS-18	5.1.1.2
MS-9	5.1.1.2		MS-19	5.1.1.2
MS-10	5.1.1.2		MS-20	5.1.1.2

Index to Look-Up Secret Criteria

There are 14 requirements that apply to all CSPs and verifiers supporting look-up secrets as authenticators.

ID	63B Section		ID	63B Section
LUS-1	5.1.2.1		LUS-8	5.1.2.2
LUS-2	5.1.2.1		LUS-9	5.1.2.2
LUS-3	5.1.2.1		LUS-10	5.1.2.2
LUS-4	5.1.2.2		LUS-11	5.1.2.2
LUS-5	5.1.2.2		LUS-12	5.1.2.2
LUS-6	5.1.2.2		LUS-13	5.1.2.2
LUS-7	5.1.2.2		LUS-14	5.1.2.2

Index to Out-of-Band Criteria

There are 20 requirements that apply to all CSPs and verifiers supporting use out-of-band authenticators.

ID	63B Section		ID	63B Section
OOB-1	5.1.3.1		OOB-13	5.1.3.2
OOB-2	5.1.3.1		OOB-14	5.1.3.2
OOB-3	5.1.3.1		OOB-15	5.1.3.2
OOB-4	5.1.3.1		OOB-16	5.1.3.2
OOB-5	5.1.3.1		OOB-17	5.1.3.2
OOB-6	5.1.3.1		OOB-18	5.1.3.2
OOB-7	5.1.3.1		OOB-19	5.1.3.3
OOB-8	5.1.3.1		OOB-20	5.1.3.3
OOB-9	5.1.3.2		OOB-21	5.2.10

OOB-10	5.1.3.2		OOB-22	5.2.10
OOB-11	5.1.3.2		OOB-23	5.2.10
OOB-12	5.1.3.2		OOB-24	5.2.10

Index to OTP Authenticator Criteria

There are 20 requirements that apply to all CSPs and verifiers supporting single- and multi-factor OTP authenticators.

ID	63B Section		ID	63B Section
OTP-1	5.1.4.1, 5.1.5.1		OTP-11	5.1.4.2, 5.1.5.2
OTP-2	5.1.4.1, 5.1.5.1		OTP-12	5.1.4.2, 5.1.5.2
OTP-3	5.1.4.1, 5.1.5.1		OTP-13	5.1.4.2, 5.1.5.2
OTP-4	5.1.4.1, 5.1.5.1		OTP-14	5.1.5.1
OTP-5	5.1.4.1, 5.1.5.1		OTP-15	5.1.5.1
OTP-6	5.1.4.1, 5.1.5.1		OTP-16	5.1.5.1
OTP-7	5.1.4.2, 5.1.5.2		OTP-17	5.1.5.1
OTP-8	5.1.4.2, 5.1.5.2		OTP-18	5.1.5.1
OTP-9	5.1.4.2, 5.1.5.2		OTP-19	5.1.5.2
OTP-10	5.1.4.2, 5.1.5.2		OTP-20	5.1.5.2

Index to Cryptographic Authenticator Criteria

There are 17 requirements that apply to all CSPs and verifiers supporting cryptographic authenticators.

ID	63B Section		ID	63B Section
CRYP-1	5.1.4.1, 5.1.5.1		CRYP-10	5.1.7.2
CRYP-2	5.1.6.1, 5.1.8.1		CRYP-11	5.1.7.2
CRYP-3	5.1.6.1, 5.1.8.1		CRYP-12	5.1.7.2
CRYP-4	5.1.7.1		CRYP-13	5.1.8.1

CRYP-5	5.1.7.1, 5.1.9.1		CRYP-14	5.1.8.1, 5.1.9.1
CRYP-6	5.1.7.1, 5.1.9.1		CRYP-15	5.1.8.1, 5.1.9.1
CRYP-7	5.1.7.1, 5.1.9.1		CRYP-16	5.1.8.1, 5.1.9.1
CRYP-8	5.1.7.2		CRYP-17	5.1.8.1, 5.1.9.1
CRYP-9	5.1.7.2			

Index to General Authentication Criteria

There are 12 requirements that apply to all CSPs and verifiers.

ID	63B Section		ID	63B Section
GEN-1	5.2.1		GEN-7	6.2
GEN-2	5.2.1		GEN-8	6.2
GEN-3	5.2.2		GEN-9	6.3
GEN-4	5.2.2		GEN-10	6.3
GEN-5	5.2.6		GEN-11	6.4
GEN-6	5.2.6		GEN-12	6.4

Index to Biometric Criteria

There are 12 requirements that apply to all CSPs and verifiers using biometric verification for authentication, including activation of multi-factor authenticators.
.

ID	63B Section		ID	63B Section
BIO-1	5.2.3		BIO-7	5.2.3
BIO-2	5.2.3		BIO-8	5.2.3
BIO-3	5.2.3		BIO-9	5.2.3
BIO-4	5.2.3		BIO-10	5.2.3
BIO-5	5.2.3		BIO-11	5.2.3
BIO-6	5.2.3		BIO-12	5.2.3

Index to Verifier Impersonation Resistance Criteria

There are 6 requirements that apply to all verifiers implementing verifier impersonation resistance (required at AAL3).

ID	63B Section		ID	63B Section
VIR-1	5.2.5		VIR-4	5.2.5
VIR-2	5.2.5		VIR-5	5.2.5

VIR-3	5.2.5		VIR-6	5.2.5

Index to Authenticator Binding Criteria

There are 25 authenticator binding requirements that apply to all CSPs.

ID	63B Section		ID	63B Section
BIND-1	6.1		BIND-14	6.1.1
BIND-2	6.1		BIND-15	6.1.1
BIND-3	6.1		BIND-16	6.1.1
BIND-4	6.1		BIND-17	6.1.2.1
BIND-5	6.1		BIND-18	6.1.2.2
BIND-6	6.1		BIND-19	6.1.2.3
BIND-7	6.1		BIND-20	6.1.2.3
BIND-8	6.1		BIND-21	6.1.2.3
BIND-9	6.1.1		BIND-22	6.1.2.3
BIND-10	6.1.1		BIND-23	6.1.2.3
BIND-11	6.1.1		BIND-24	6.1.2.3
BIND-12	6.1.1		BIND-25	6.1.2.3
BIND-13	6.1.1			

Index to Session Management Criteria

There are 17 session management requirements that apply to all CSPs and RPs.

ID	63B Section		ID	63B Section
SESS-1	7.1		SESS-10	7.1#7
SESS-2	7.1		SESS-11	7.1#8
SESS-3	7.1		SESS-12	7.1#8
SESS-4	7.1		SESS-13	7.1
SESS-5	7.1#1		SESS-14	7.1.1#1
SESS-6	7.1#2		SESS-15	7.1.1#2
SESS-7	7.1#2		SESS-16	7.1#4
SESS-8	7.1#3		SESS-17	7.1.2
SESS-9	7.1#6			

Index to Reauthentication Criteria

There are 10 reauthentication requirements that apply to all CSPs and RPs.

ID	63B Section		ID	63B Section
REAUTH-1	7.2		REAUTH-6	7.2
REAUTH-2	7.2		REAUTH-7	7.2.1
REAUTH-3	7.2		REAUTH-8	7.2.1

REAUTH-4	7.2		REAUTH-9	7.2.1
REAUTH-5	7.2		REAUTH-10	7.2.1

1 AAL2 CSP Conformance Criteria

All CSPs authenticating claimants at AAL2 SHALL be assessed on the following criteria:

AAL2-1	**REQUIREMENT**: Authentication SHALL occur by the use of either a multi-factor authenticator or a combination of two single-factor authenticators. (4.2.1) **SUPPLEMENTAL GUIDANCE**: A multi-factor authenticator requires two factors to execute a single authentication event, such as a cryptographically-secure device with an integrated biometric sensor that is required to activate the device. Nine different authenticator types are recognized, representing something you know (a memorized secret), something you have (a physical authenticator), or combinations of physical authenticators with either memorized secrets or biometric modalities (something you are). Multi-factor (MF) authentication is required at AAL2. MF authentication at AAL2 may be performed using the following AAL2 permitted authenticator types: MF OTP Device, MF Crypto Software, or MF Crypto Device; or a memorized secret used in combination with the following permitted single-factor authenticators: Look-Up Secret, Out-of-Band authenticator, SF OTP Device, SF Crypto Software, or SF Crypto Device. **ASSESSMENT OBJECTIVE:** Determine if the CSP requires the use of two single-factor authenticators or one multi-factor authenticator in all cases at AAL2. **POTENTIAL ASSESSMENT METHODS AND OBJECTS**: **Examine**: the CSP's *documented policies* for a statement describing the authenticators that are permitted for use at AAL2 to determine that either two single-factor authenticators or one multi-factor authenticator is always required.

AAL2-2	**REQUIREMENT**: If the multi-factor authentication process uses a combination of two single-factor authenticators, then it SHALL include a Memorized Secret authenticator and a possession-based authenticator. (4.2.1) **SUPPLEMENTAL GUIDANCE**: Multifactor authentication requires the use of two different authentication factors. See AAL2-1 for permitted authenticator types at AAL2. Because of the requirement (5.2.3) that use of biometrics be tightly bound with one or more specific physical authenticators, the use of separate authenticators must include the other two authentication factors. Accordingly, biometric sensors and verifiers are not recognized as authenticators by themselves.

	ASSESSMENT OBJECTIVE: Determine that all combinations of single-factor authenticators usable at AAL2 include both a memorized secret and a possession-based authenticator, **POTENTIAL ASSESSMENT METHODS AND OBJECTS**: **Examine**: the CSP's *documented policies or practices* for a statement describing the combinations of single-factor authenticators that are accepted and determine that all such combinations consist of a memorized secret and a possession-based (physical) authenticator.

AAL2-3	**REQUIREMENT**: Cryptographic authenticators used at AAL2 SHALL use approved cryptography. (4.2.2) **SUPPLEMENTAL GUIDANCE**: As defined in Appendix A of SP 800-63-3, cryptography is considered approved if it is specified or adopted in a FIPS or NIST recommendation. Since verifiers and cryptographic authenticators must use the same algorithms to successfully authenticate, assessment of the verifier also assesses the authenticators that may be used. **ASSESSMENT OBJECTIVE:** Determine that only secure, well-vetted cryptographic algorithms are being used. **POTENTIAL ASSESSMENT METHODS AND OBJECTS**: **Examine**: one or both of the following: ● *documented policies or practices* to determine that only approved cryptographic algorithms can be used. ● The *system's functionality* to observe the cryptographic algorithm(s) being accepted and determine whether the algorithms are approved.

AAL2-4	**REQUIREMENT**: At least one authenticator used at AAL2 SHALL be replay resistant. (4.2.2) **SUPPLEMENTAL GUIDANCE**: Replay resistance is a characteristic of most, although not all, physical authenticators. A given output of the authenticator is required to be accepted for only one authentication transaction. For example, the output of a time-based OTP device or an out-of-band device is considered replay resistant if it can only be used for at most one authentication transaction during its validity period. If it can be used for more than one during this period, it is not replay resistant. Challenge-response protocols used by cryptographic authenticators are considered replay resistant provided that the challenge nonce is not reused. As specified in Section 5.1.2, look-up secrets are replay resistant because they can be used only once. Memorized secrets and biometric modalities are not considered replay resistant.

	ASSESSMENT OBJECTIVE: Ensure that the authentication transaction cannot be replayed by an attacker. **POTENTIAL ASSESSMENT METHODS AND OBJECTS**: **Examine**: If the transaction involves the use of a cryptographic protocol responding to a challenge nonce sent by the verifier, the authenticator is considered replay resistant. **Test**: If verifying a physical authenticator that does not implement a cryptographic challenge/response protocol, attempt to authenticate more than once using the same authenticator output (during its validity period, if time-based). If a subsequent authentication succeeds, the test of replay resistance has failed.

AAL2-5	**REQUIREMENT**: Communication between the claimant and verifier SHALL be via an authenticated protected channel. (4.2.2) **SUPPLEMENTAL GUIDANCE**: Communication between claimant and verifier is required to be via an encrypted channel that authenticates the verifier to provide confidentiality of the authenticator output and resistance to MitM attacks. This is typically accomplished using the Transport Level Security (TLS) protocol. Mutual authentication of the communication channel is not required unless that is part of the process of authenticating the claimant. Accordingly, the verifier is only responsible the use of an appropriately secure communications protocol. **ASSESSMENT OBJECTIVE:** Determine that the communication channel meets the requirements of an authenticated protected channel as defined in SP 800-63-3 Appendix A. **POTENTIAL ASSESSMENT METHODS AND OBJECTS**: **Examine**: the verifier's API documentation to ensure that TLS or a similarly secure protocol is used in conjunction with an approved encryption protocol (see AAL2-3).

AAL2-6	**REQUIREMENT**: Verifiers operated by government agencies at AAL2 SHALL be validated to meet the requirements of FIPS 140 Level 1. (4.2.2) **SUPPLEMENTAL GUIDANCE**: Verifiers operated by or on behalf of government agencies are required to be validated to meet FIPS 140 requirements. The FIPS 140 requirements generally apply to cryptographic modules (both hardware and software). **ASSESSMENT OBJECTIVE:** Determine that FIPS 140 Level 1 validation has been obtained.

	POTENTIAL ASSESSMENT METHODS AND OBJECTS: **Examine**: the verifier's certification of FIPS 140 level 1 (or higher) compliance.

AAL2-7	**REQUIREMENT**: Authenticators procured by government agencies SHALL be validated to meet the requirements of FIPS 140 Level 1. (4.2.2) **SUPPLEMENTAL GUIDANCE**: The FIPS 140 requirements generally apply to cryptographic modules (both hardware and software). While authenticators are not directly the responsibility of the CSP (particularly in the case of bring-your-own authenticators), the CSP is still responsible for ensuring that a sufficiently strong and FIPS 140 validated authenticator is being used. Binding of CSP-supplied authenticators that are known to meet validation criteria is sufficient. **ASSESSMENT OBJECTIVE:** Determine that authenticators having FIPS 140 certification are being supplied to subscribers. **POTENTIAL ASSESSMENT METHODS AND OBJECTS**: **Examine**: the CSP or verifier's specifications for the procurement of authenticators to determine that FIPS 140 level 1 (or higher) compliance is required.

AAL2-8	**REQUIREMENT**: If a device such as a smartphone is used in the authentication process, then the unlocking of that device (typically done using a PIN or biometric) SHALL NOT be considered one of the authentication factors. (4.2.2) **SUPPLEMENTAL GUIDANCE**: This requirement applies to multi-factor authenticators resident on a smartphone or similar device; single-factor authenticators on such devices would only provide a single (physical) authentication factor. Unlocking of a device such as a smartphone may be done for any number of reasons unrelated to authentication, and such devices are normally in an unlocked state for a period of time thereafter. Human action such as entry of a memorized secret or presentation of a biometric factor needs to be provided that is directly associated with the authentication event. Generally, it is not possible for a verifier to know that the device had been locked or if the unlock process met the requirements for the relevant authenticator type. **ASSESSMENT OBJECTIVE:** Determine that smartphones and similar devices require human action directly associated with the authentication process. **POTENTIAL ASSESSMENT METHODS AND OBJECTS**: **Test**: Attempt to authenticate using supported smartphones and similar devices

	and observe that presentation of an authentication factor (memorized secret or biometric factor) is required at the time of authentication.

AAL2-9	**REQUIREMENT**: If a biometric factor is used in authentication at AAL2, then the performance requirements stated in Section 5.2.3 SHALL be met, and the verifier SHOULD make a determination that the biometric sensor and subsequent processing meet these requirements. (4.2.2) **SUPPLEMENTAL GUIDANCE**: Detailed conformance criteria applicable to the use of biometrics are contained in section BIO- below. Since verification of biometric factors is not deterministic due to measurement errors in collection of the biometric information, evaluation of performance, and, most importantly, false accept rate, is important to ensure security of the authentication process. **ASSESSMENT OBJECTIVE:** Determine that sensors and processing used for biometric authentication factors meet relevant requirements. **POTENTIAL ASSESSMENT METHODS AND OBJECTS**: **Examine**: Vendor documentation, including test data, to determine that the performance of the sensor/processing combination used with biometric factors that are accepted.

AAL2-10	**REQUIREMENT**: Reauthentication of the subscriber SHALL be repeated at least once per 12 hours during an extended usage session. (4.2.3) **SUPPLEMENTAL GUIDANCE**: Reauthentication is required to mitigate the risks associated with an authenticated endpoint that has been abandoned by the subscriber or has been misappropriated by an attacker while authenticated. At AAL2, providing a memorized secret or biometric factor is sufficient for reauthentication prior to the expiration time. **ASSESSMENT OBJECTIVE:** Determine that reauthentication requirements are met. **POTENTIAL ASSESSMENT METHODS AND OBJECTS**: **Test**: Authenticate, then idle for 30 minutes and determine that reauthentication is required. Maintain a session for at least 12 hours and observe that reauthentication is required. **Examine**: verifier or CSP documentation to determine that required reauthentication requirements are enforced.

AAL2-11	**REQUIREMENT**: Reauthentication of the subscriber SHALL be repeated following any period of inactivity lasting 30 minutes or longer. (4.2.3)

	SUPPLEMENTAL GUIDANCE: Reauthentication is required to mitigate the risks associated with an authenticated endpoint that has been abandoned by the subscriber or has been misappropriated by an attacker while authenticated. At AAL2, providing a memorized secret or biometric factor is sufficient for reauthentication prior to the expiration time. **ASSESSMENT OBJECTIVE:** Determine that reauthentication requirements are met. **POTENTIAL ASSESSMENT METHODS AND OBJECTS**: **Test**: Authenticate, then idle for 30 minutes and determine that reauthentication is required. Maintain a session for at least 12 hours and observe that reauthentication is required. **Examine**: verifier or CSP documentation to determine that required reauthentication requirements are enforced.

AAL2-12	**REQUIREMENT**: The session SHALL be terminated (i.e., logged out) when either the extended usage or inactivity time limit is reached. (4.2.3) **SUPPLEMENTAL GUIDANCE**: If reauthentication is not performed in accordance with requirements AAL2-10 and AAL2-11, the session needs to be logged out at that time. **ASSESSMENT OBJECTIVE:** Determine that active sessions are logged out if reauthentication requirements are not met. **POTENTIAL ASSESSMENT METHODS AND OBJECTS**: **Test**: Authenticate, then idle for 30 minutes and determine that the session is logged out. Maintain a session for at least 12 hours and determine that the session is logged out. **Examine**: verifier or CSP documentation to determine that active sessions are logged out at the expiration of their reauthentication time.

AAL2-13	**REQUIREMENT**: The CSP SHALL employ appropriately tailored security controls from the moderate baseline of security controls defined in SP 800-53 or equivalent federal (e.g., FEDRAMP) or industry standard. The CSP SHALL ensure that the minimum assurance-related controls for *moderate-impact* systems or equivalent are satisfied. (4.2.4) **SUPPLEMENTAL GUIDANCE**: NIST SP 800-53 provides a comprehensive catalog of controls, three security control baselines (low, moderate, and high impact), and guidance for tailoring the appropriate baseline to specific needs and risk environments for federal information systems. These controls are the

	operational, technical, and management safeguards to maintain the integrity, confidentiality, and security of federal information systems and are intended to be used in conjunction with the NIST risk management framework outlined in SP 800-37 and SP 800-63-3 section 5 Digital Identity Risk Management. NIST SP 800-53 presents security control baselines determined by the security categorization of the information system (low, moderate or high) from NIST FIPS 199 Standards for Security Categorization of Federal Information and Information Systems. For IAL2, the moderate baseline controls (see https://nvd.nist.gov/800-53/Rev4/impact/moderate) may be considered the starting point for the selection, enhancement, and tailoring of the security controls presented. Guidance on tailoring the control baselines to best meet the organization's risk environment, systems and operations is presented in SP 800-53 section 3.2. Tailoring Baseline Security Controls. While SP 800-53 and other NIST Special Publications in the SP-800-XXX series apply to federal agencies for the implementation of the Federal information Security Management Act (FISMA), non-federal entities providing services for federal information services also are subject to FISMA and should similarly use SP 800-53 and associated publications for appropriate controls. Non-federal entities may be subject to and conformant with other applicable controls systems and processes for information system security (e.g., FEDRAMP, ISO/IEC 27001. SP-63A allows the application of equivalent controls from such standards and processes to meet conformance with this criterion. **ASSESSMENT OBJECTIVE:** Determine that the CSP employs appropriately tailored security controls to include control enhancements from the moderate or high baseline of security controls defined in SP 800-53 or equivalent federal (e.g., FEDRAMP) or industry standard **POTENTIAL ASSESSMENT METHODS AND OBJECTS**: **Examine**: the CSP's *documentation* to determine it employs appropriately tailored security controls to include control enhancements, from the moderate or high baseline of security controls defined in SP 800-53 or equivalent federal process (such as FEDRAMP) or industry standard

AAL2-14	**REQUIREMENT**: The CSP shall comply with records retention policies in accordance with applicable laws and regulations. (4.2.5) **SUPPLEMENTAL GUIDANCE**: It is recommended that CSPs document any specific retention policies they are subject to, in accordance with applicable laws, regulations, or policies, including any National Archives and Records Administration (NARA) records retention schedules that may apply. The CSP is responsible for the proper handling, protection, and retention or disposal of any sensitive data it collects, even after it ceases to provide identity proofing and enrollment services. A CSP may document its policies and

	procedures for the management of the data is collects in a data handling plan or other document. **ASSESSMENT OBJECTIVE:** Determine that the CSP has documented records retention policies based on laws and regulations applicable to the CSP's jurisdiction and scope. **POTENTIAL ASSESSMENT METHODS AND OBJECTS**: **Examine**: the CSP's records retention policy and evaluate its applicability with laws and regulations. Where applicable, audit a sample of retained records to ensure that their retention is consistent with policy.

AAL2-15	**REQUIREMENT**: If the CSP opts to retain records in the absence of any mandatory requirements, then the CSP shall conduct a risk management process, including assessments of privacy and security risks to determine how long records should be retained and SHALL inform subscribers of that retention policy. (4.2.5) **SUPPLEMENTAL GUIDANCE**: This is a conditional requirement and depends on the basis for CSP records retention. Absent clear jurisdictional requirements, risk management processes, including privacy and security risk assessment, need to be performed for records retention decisions. The records retention duration is required to be derived from a risk-based decision process. **ASSESSMENT OBJECTIVE:** Determine that a risk-based decision process for records retention was used, and that privacy and security factors were included. **POTENTIAL ASSESSMENT METHODS AND OBJECTS**: **Examine**: evidence to determine risk-based decision for records retention was used, and that notice to subscribers is provided.

2 AAL3 CSP Conformance Criteria

All CSPs authenticating claimants at AAL3 SHALL be assessed on the following criteria:

AAL3-1	**REQUIREMENT**: AAL3 authentication SHALL use a hardware-based authenticator. (4.3) **SUPPLEMENTAL GUIDANCE**: Authentication at AAL3 requires a multifactor authenticator that meets these requirements or a combination of two (or in rare cases, three) authenticators that include at least one authenticator with each of these characteristics. In the case of "bring-your-own" authenticators, the CSP must have a basis for determining that the necessary authenticator(s) meet these requirements. **ASSESSMENT OBJECTIVE:** Determine if the CSP requires the use of a hardware-based authenticator in all cases at AAL3. **POTENTIAL ASSESSMENT METHODS AND OBJECTS**: **Examine**: the CSP's *documented policies* for a statement describing the authenticators that are permitted for use at AAL3 to determine that a hardware-based authenticator is always required.

AAL3-2	**REQUIREMENT**: In order to authenticate at AAL3, claimants SHALL prove possession and control of two distinct authentication factors through secure authentication protocol(s). (4.3) **SUPPLEMENTAL GUIDANCE**: Multi-factor authentication can be accomplished either through the use of a multi-factor authenticator or a combination of authenticators. A multi-factor authenticator requires two factors to execute a single authentication event, such as a cryptographically-secure device with an integrated biometric sensor that is required to activate the device. Nine different authenticator types are recognized, representing something you know (a memorized secret), something you have (a physical authenticator), or combinations of physical authenticators with either memorized secrets or biometric modalities (something you are). Permitted combinations of authenticators are given in Section 4.3.1 and requirement AAL3-3 below. **ASSESSMENT OBJECTIVE:** Determine if the CSP requires the use of a two distinct authentication factors. **POTENTIAL ASSESSMENT METHODS AND OBJECTS**: **Examine**: the CSP's *documented policies* for a statement describing the authenticators that are permitted for use at AAL3 to determine that all authenticator combinations include the use of two distinct authentication factors.

AAL3-3	**REQUIREMENT**: Authentication at AAL3 SHALL use approved cryptographic techniques. (4.3) **SUPPLEMENTAL GUIDANCE**: As defined in Appendix A of SP 800-63-3, cryptography is considered approved if it is specified or adopted in a FIPS or NIST recommendation. Since verifiers and cryptographic authenticators must use the same algorithms to successfully authenticate, assessment of the verifier also assesses the authenticators that may be used. **ASSESSMENT OBJECTIVE:** Determine that only secure, well-vetted cryptographic algorithms are being used. **POTENTIAL ASSESSMENT METHODS AND OBJECTS**: **Examine**: one or both of the following: ● *documented policies or practices* to determine that only approved cryptographic algorithms can be used. ● the *system's functionality* to observe the cryptographic algorithm(s) being accepted and determine whether the algorithms are approved.

AAL3-4	**REQUIREMENT**: Authentication at AAL3 SHALL use a permitted authenticator or combination of authenticators. (4.3.1) **SUPPLEMENTAL GUIDANCE**: The requirements for authentication at AAL3 lead to the use of only specific combinations of authenticator types. Multi-factor (MF) authentication at AAL3 may be performed using the following AAL3 permitted authenticator types and combinations: MF Crypto Device, SF Crypto Device used in combination with Memorized Secret, MF OTP Device used in combination with SF Crypto device or software, SF OTP Device used in combination with MF Crypto Software, SF OTP Device used in combination with SF Crypto Software and memorized secret. **ASSESSMENT OBJECTIVE:** Determine if only AAL3 permitted authenticators and combinations of authenticators are used. **POTENTIAL ASSESSMENT METHODS AND OBJECTS**: **Examine**: one or both of the following: ● *documented policies or practices* to determine authenticator types that can be used. ● the *system's functionality* to observe the authenticator types being accepted.

AAL3-5	**REQUIREMENT**: Communication between the claimant and verifier SHALL be via an authenticated protected channel. (4.3.2) **SUPPLEMENTAL GUIDANCE**: Communication between claimant and verifier is required to be via an encrypted channel that authenticates the verifier

	to provide confidentiality of the authenticator output and resistance to MitM attacks. This is typically accomplished using the Transport Level Security (TLS) protocol. Mutual authentication of the communication channel is not required unless that is part of the process of authenticating the claimant. Accordingly, the verifier is only responsible the use of an appropriately secure communications protocol. **ASSESSMENT OBJECTIVE:** Determine that the communication channel meets the requirements of an authenticated protected channel as defined in SP 800-63-3 Appendix A. **POTENTIAL ASSESSMENT METHODS AND OBJECTS**: **Examine**: the verifier's API documentation to ensure that TLS or a similarly secure protocol is used in conjunction with an approved encryption protocol (see AAL3-2).

AAL3-6	**REQUIREMENT**: At least one cryptographic authenticator used at AAL3 SHALL be verifier impersonation resistant. (4.3.2) **SUPPLEMENTAL GUIDANCE**: Verifier impersonation resistance provides a high degree of protection to man-in-the-middle attacks. Detailed requirements for verifier impersonation resistance are in criteria VIR-*. **ASSESSMENT OBJECTIVE:** Determine if cryptographic devices used provide the correct output only to the intended relying party. **POTENTIAL ASSESSMENT METHODS AND OBJECTS**: **Examine**: verifier documentation to establish how a strong binding is maintained between the verifier output, the communication channel being used, and the relying party. **Test:** Attempt to authenticate through a man-in-the-middle element. The authentication must fail in the presence of a man in the middle.

AAL3-7	**REQUIREMENT**: At least one cryptographic authenticator used at AAL3 SHALL be replay resistant. (4.3.2) **SUPPLEMENTAL GUIDANCE**: Replay resistance is a characteristic of most, although not all, physical authenticators. A given output of the authenticator is required to be accepted for only one authentication transaction. For example, the output of a time-based OTP device or an out-of-band device is considered replay resistant if it can only be used for at most one authentication transaction during its validity period. If it can be used for more than one during this period, it is not replay resistant.

	Challenge-response protocols used by cryptographic authenticators are considered replay resistant provided that the challenge nonce is not reused. **ASSESSMENT OBJECTIVE:** Determine that the authentication response cannot be replayed by an attacker. **POTENTIAL ASSESSMENT METHODS AND OBJECTS**: **Examine**: If the transaction involves the use of a cryptographic protocol responding to a challenge nonce sent by the verifier, the authenticator is considered replay resistant. **Test**: If verifying a physical authenticator that does not implement a cryptographic challenge/response protocol, attempt to authenticate more than once using the same authenticator. If a subsequent authentication succeeds, the test of replay resistance has failed.

AAL3-8	**REQUIREMENT**: All authentication and reauthentication processes at AAL3 SHALL demonstrate authentication intent from at least one authenticator. (4.3.2) **SUPPLEMENTAL GUIDANCE**: Authentication intent is a requirement to prevent passive authentication (without the subscriber's consent). This may occur, for example, as a result of malware operating on the subscriber's endpoint taking advantage of connected cryptographic devices or as a result of a proximity attack on a subscriber's wireless authenticator. Requirements to establish authentication intent are described in Section 5.2.9. **ASSESSMENT OBJECTIVE:** Determine that all acceptable authenticators and authenticator combinations include at least one with authentication intent. **POTENTIAL ASSESSMENT METHODS AND OBJECTS**: **Examine**: CSP documentation to determine the acceptable combinations of authenticators that are available to subscribers authenticating at AAL3.

AAL3-9	**REQUIREMENT**: Multi-factor authenticators used at AAL3 SHALL be hardware cryptographic modules validated at FIPS 140 Level 2 or higher overall with at least FIPS 140 Level 3 physical security. (4.3.2) **SUPPLEMENTAL GUIDANCE**: The FIPS 140 requirements generally apply to cryptographic modules (both hardware and software). While authenticators are not directly the responsibility of the CSP (particularly in the case of bring-your-own authenticators), the CSP is still responsible for ensuring that a sufficiently strong and FIPS 140 validated authenticator is being used. Binding of CSP-supplied authenticators that are known to meet validation criteria is sufficient, as is the verification of compliance for subscriber-provided

	authenticators. This verification may take place remotely using technologies such as provenance certificates provided by the manufacturer. **ASSESSMENT OBJECTIVE:** Determine if multi-factor authenticators used at AAL3 have been validated at FIPS 140 level 2 or higher overall with at least FIPS 140 level 3 physical security. **POTENTIAL ASSESSMENT METHODS AND OBJECTS**: **Examine**: the CSP or verifier's specifications for the procurement of authenticators to determine that the required FIPS 140 compliance is achieved, or that a procedure such as the verification of provenance certificates is performed to verify compliance.

AAL3-10	**REQUIREMENT**: Single-factor cryptographic devices used at AAL3 SHALL be validated at FIPS 140 Level 1 or higher overall with at least FIPS 140 Level 3 physical security. (4.3.2) **SUPPLEMENTAL GUIDANCE**: The FIPS 140 requirements generally apply to cryptographic modules (both hardware and software). The CSP is responsible for ensuring that a sufficiently strong and FIPS 140 validated authenticator is being used. Binding of CSP-supplied authenticators that are known to meet validation criteria is sufficient, as is the verification of compliance for subscriber-provided authenticators. This verification may take place remotely using technologies such as provenance certificates provided by the manufacturer. **ASSESSMENT OBJECTIVE:** Determine if single-factor cryptographic devices used at AAL3 have been validated at FIPS 140 level 1 or higher overall with at least FIPS 140 level 3 physical security. **POTENTIAL ASSESSMENT METHODS AND OBJECTS**: **Examine**: the CSP or verifier's specifications for the procurement of authenticators to determine that the required FIPS 140 compliance is achieved, or that a procedure such as the verification of provenance certificates is performed to verify compliance.

AAL3-11	**REQUIREMENT**: Verifiers at AAL3 SHALL be verifier compromise resistant with respect to at least one authentication factor. (4.3.2) **SUPPLEMENTAL GUIDANCE**: Verifier compromise resistance, described in Section 5.2.7, is the characteristic that a successful attacker that breaches the verifier is not be able to obtain information that would allow them to impersonate a subscriber. Storage of a public key corresponding to a private key with at least 112 bits of entropy is considered verifier compromise resistant. Verification using a symmetric key or memorized secret generally are not.

	ASSESSMENT OBJECTIVE: Determine if all usable combinations of authenticators include at least one that is verifier compromise resistant. **POTENTIAL ASSESSMENT METHODS AND OBJECTS**: **Examine**: CSP documentation to determine the acceptable combinations of authenticators that are available to subscribers authenticating at AAL3.

AAL3-12	**REQUIREMENT**: If a device such as a smartphone is used in the authentication process, then the unlocking of that device (typically done using a PIN or biometric) SHALL NOT be considered to satisfy one of the authentication factors. (4.3.2) **SUPPLEMENTAL GUIDANCE**: This requirement applies to multi-factor authenticators resident on a smartphone or similar device; single-factor authenticators on such devices would only provide a single (physical) authentication factor. Unlocking of a device such as a smartphone may be done for any number of reasons unrelated to authentication, and such devices are normally in an unlocked state for a period of time thereafter. Human action such as entry of a memorized secret or presentation of a biometric factor needs to be provided that is directly associated with the authentication event. Generally, it is not possible for a verifier to know that the device had been locked or if the unlock process met the requirements for the relevant authenticator type. **ASSESSMENT OBJECTIVE:** Determine if smartphones and similar devices require human action directly associated with the authentication process. **POTENTIAL ASSESSMENT METHODS AND OBJECTS**: **Test**: Attempt to authenticate using supported smartphones and similar devices and observe that presentation of an authentication factor (memorized secret or biometric factor) is required at the time of authentication.

AAL3-13	**REQUIREMENT**: If a biometric factor is used in authentication at AAL3, then the verifier SHALL make a determination that the biometric sensor and subsequent processing meet the performance requirements stated in Section 5.2.3. (4.3.2) **SUPPLEMENTAL GUIDANCE**: Detailed conformance criteria applicable to the use of biometrics are contained in section BIO-* below. Since verification of biometric factors is not deterministic due to measurement errors in collection of the biometric information, evaluation of performance, most importantly false accept rate, is important to ensure security of the authentication process. **ASSESSMENT OBJECTIVE:** Determine if sensors and processing used for biometric authentication factors meet relevant requirements.

	POTENTIAL ASSESSMENT METHODS AND OBJECTS: **Examine**: Vendor documentation, including test data, to determine that the performance of the sensor/processing combination used with biometric factors that are accepted.

AAL3-14	**REQUIREMENT**: At AAL3, authentication of the subscriber SHALL be repeated at least once per 12 hours during an extended usage session, regardless of user activity. (4.3.3) **SUPPLEMENTAL GUIDANCE**: Reauthentication is required to mitigate the risks associated with an authenticated endpoint that has been abandoned by the subscriber or has been misappropriated by an attacker while authenticated. Reauthentication is typically requested shortly before the expiration of the session, to give the opportunity to reauthenticate prior to session expiration. **ASSESSMENT OBJECTIVE:** Determine if reauthentication requirements described above are met. **POTENTIAL ASSESSMENT METHODS AND OBJECTS**: **Test**: Authenticate, then maintain an active session for at least 12 hours, and observe that reauthentication is required. **Examine**: verifier or CSP documentation to determine that required reauthentication requirements are enforced.

AAL3-15	**REQUIREMENT**: Reauthentication of the subscriber SHALL be repeated following any period of inactivity lasting 15 minutes or longer. (4.3.3) **SUPPLEMENTAL GUIDANCE**: Reauthentication is required to mitigate the risks associated with an authenticated endpoint that has been abandoned by the subscriber or has been misappropriated by an attacker while authenticated. Reauthentication is typically requested shortly before the expiration of the session, to give the opportunity to reauthenticate prior to session expiration. **ASSESSMENT OBJECTIVE:** Determine that reauthentication requirements are met. **POTENTIAL ASSESSMENT METHODS AND OBJECTS**: **Test**: Authenticate, then idle for 15 minutes and determine that reauthentication is required. Maintain a session for at least 12 hours and observe that reauthentication is required. **Examine**: verifier or CSP documentation to determine that required reauthentication requirements are enforced.

AAL3-16	**REQUIREMENT**: Reauthentication SHALL use both authentication factors. (4.3.3) **SUPPLEMENTAL GUIDANCE**: To support the added authentication assurance, AAL3 requires that both authentication factors be presented when reauthentication is required. If a multi-factor authenticator is used, presentation and activation of that authenticator (with a memorized secret or biometric factor) is sufficient. **ASSESSMENT OBJECTIVE:** Determine that reauthentication requirements for AAL3 are met by requiring both authentication factors. **POTENTIAL ASSESSMENT METHODS AND OBJECTS**: **Test**: Invoke reauthentication requirements by either an idle session or extended session and determine that both authentication factors are required in order to extend the session.

AAL3-17	**REQUIREMENT**: The session SHALL be terminated (i.e., logged out) when either the extended usage or inactivity time limit is reached. (4.3.3) **SUPPLEMENTAL GUIDANCE**: If reauthentication is not performed in accordance with requirements AAL3-14 and AAL3-152-10, the session needs to be logged out at that time. **ASSESSMENT OBJECTIVE:** Determine that active sessions are logged out if reauthentication requirements are not met. **POTENTIAL ASSESSMENT METHODS AND OBJECTS**: **Test**: Authenticate, then idle for 15 minutes and determine that the session is logged out. Maintain a session for at least 12 hours and determine that the session is logged out. **Examine**: verifier or CSP documentation to determine that active sessions are logged out at the expiration of their reauthentication time.

AAL3-18	**REQUIREMENT**: The CSP SHALL employ appropriately-tailored security controls from the *high* baseline of security controls defined in SP 800-53 or an equivalent federal (e.g., FEDRAMP) or industry standard. The CSP SHALL ensure that the minimum assurance-related controls for high-*impact* systems or equivalent are satisfied. (4.3.4) **SUPPLEMENTAL GUIDANCE**: NIST SP 800-53 provides a comprehensive catalog of controls, three security control baselines (low, moderate, and high impact), and guidance for tailoring the appropriate baseline to specific needs and

	risk environments for federal information systems. These controls are the operational, technical, and management safeguards to maintain the integrity, confidentiality, and security of federal information systems and are intended to be used in conjunction with the NIST risk management framework outlined in SP 800-37 and SP 800-63-3 section 5 Digital Identity Risk Management. NIST SP 800-53 presents security control baselines determined by the security categorization of the information system (low, moderate or high) from NIST FIPS 199 Standards for Security Categorization of Federal Information and Information Systems. For IAL3 the high baseline controls (see https://nvd.nist.gov/800-53/Rev4/impact/high) may be considered the starting point for the selection, enhancement, and tailoring of the security controls presented. Guidance on tailoring the control baselines to best meet the organization's risk environment, systems and operations is presented in SP 800-53 section 3.2, Tailoring Baseline Security Controls. While SP 800-53 and other NIST Special Publications in the SP-800-XXX series apply to federal agencies for the implementation of the Federal Information Security Modernization Act (FISMA), non-federal entities providing services for federal information services also are subject to FISMA and should similarly use SP 800-53 and associated publications for appropriate controls. Non-federal entities may be subject to and conformant with other applicable controls systems and processes for information system security (e.g., FEDRAMP, ISO/IEC 27001). SP 800-63B allows the application of equivalent controls from such standards and processes to meet conformance with this criterion. **ASSESSMENT OBJECTIVE:** Determine if the CSP employs appropriately tailored security controls to include control enhancements, from the high baseline of security controls defined in SP 800-53 or equivalent federal (e.g., FEDRAMP) or industry standard. **POTENTIAL ASSESSMENT METHODS AND OBJECTS**: **Examine**: the CSP's *documentation* to determine it employs appropriately tailored security controls to include control enhancements, from the high baseline of security controls defined in SP 800-53 or equivalent federal (e.g., FEDRAMP) or industry standard.

AAL3-19	**REQUIREMENT**: The CSP shall comply with its respective records retention policies in accordance with applicable laws, regulations, and policies, including any NARA records retention schedules that may apply. (4.3.5) **SUPPLEMENTAL GUIDANCE**: It is recommended that CSPs document any specific retention policies they are subject to, in accordance with applicable laws, regulations, or policies, including any National Archives and Records Administration (NARA) records retention schedules that may apply.

	The CSP is responsible for the proper handling, protection, and retention or disposal of any sensitive data it collects, even after it ceases to provide identity proofing and enrollment services. A CSP may document its policies and procedures for the management of the data is collects in a data handling plan or other document. **ASSESSMENT OBJECTIVE:** Determine that the CSP has documented records retention policies based on laws and regulations applicable to the CSP's jurisdiction and scope. **POTENTIAL ASSESSMENT METHODS AND OBJECTS**: **Examine**: the CSP's records retention policy and evaluate its applicability with laws and regulations. Where applicable, audit a sample of retained records to ensure that their retention is consistent with policy.

AAL3-20	**REQUIREMENT**: If the CSP opts to retain records in the absence of any mandatory requirements, then the CSP SHALL conduct a risk management process, including assessments of privacy and security risks, to determine how long records should be retained and SHALL inform the subscriber of that retention policy. (4.3.5) **SUPPLEMENTAL GUIDANCE**: This is a conditional requirement and depends on the basis for CSP records retention. Absent clear jurisdictional requirements, risk management processes, including privacy and security risk assessment, need to be performed for records retention decisions. The records retention duration is required to be derived from a risk-based decision process. **ASSESSMENT OBJECTIVE:** Determine that a risk-based decision process for records retention was used, and that privacy and security factors were included. **POTENTIAL ASSESSMENT METHODS AND OBJECTS**: **Examine**: evidence to determine risk-based decision for records retention was used, and that notice to subscribers is provided.

3 Privacy Conformance Criteria

PRIV-1	**REQUIREMENT**: The CSP shall employ appropriately tailored privacy controls from SP 800-53 or equivalent standard. (4.4) **SUPPLEMENTAL GUIDANCE**: This requirement establishes overall privacy posture of the CSP. These controls are contained in Appendix J of SP 800-53 revision 4. **ASSESSMENT OBJECTIVE:** Ensure appropriate privacy controls are in place. **POTENTIAL ASSESSMENT METHODS AND OBJECTS**: **Examine**: the CSP's operating procedure documentation and, as applicable, authority-to-operate (ATO) for consistency with SP 800-53 or equivalent standard.

PRIV-2	**REQUIREMENT**: 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 SHALL implement measures to maintain predictability and manageability commensurate with the associated privacy risk. (4.4) **SUPPLEMENTAL GUIDANCE**: Predictability and manageability measures include providing clear notice, obtaining subscriber consent, and enabling selective use or disclosure of attributes. Predictability is meant to build trust and provide accountability and requires full understanding (and disclosure) of how the attribute information will be used. Manageability also builds trust by demonstrating a CSPs ability to control attribute information throughout processing – collection, maintenance, retention. **ASSESSMENT OBJECTIVE:** Determine that the CSP employs measures to maintain predictability and manageability commensurate with the privacy risk arising from any additional processing of attributes. **POTENTIAL ASSESSMENT METHODS AND OBJECTS**: **Examine**: the CSP's *documented policies or practices* to determine which predictability and manageability measures it employs, (e.g., notice, consent, selective disclosure).

PRIV-3	**REQUIREMENT**: Federal agencies shall consult with their SAOP to determine applicability of the Privacy Act of 1974 and the E-Government Act of 2002 with

	respect to issuance or maintenance of authenticators, and publish a System of Records Notice (SORN) or Privacy Impact Assessment (PIA) accordingly. (4.4) **SUPPLEMENTAL GUIDANCE**: This requirement applies to Federal agencies whether providing authentication services directly or through a commercial provider. This requirement directs Agencies to consult with their Senior Agency Official for Privacy (SAOP) and conduct an analysis to determine whether the collection of PII to issue or maintain authenticators triggers the requirements of the *Privacy Act of 1974* or the requirements of the *E-Government Act of 2002.* Based on this consultation and analysis, the agency may need to publish a System of Records Notice (SORN) and/or a Privacy Impact Assessment (PIA) to cover such collections, as applicable. While this requirement specifically applies only to federal agencies, CSPs that provide services to federal agencies may be expected to provide information about their identity services in support of an Agency's privacy analysis and PIA. **ASSESSMENT OBJECTIVE:** Confirm that the agency offering or using the identity proofing service has: ● consulted with its SAOP to determine if the service is subject to the Privacy Act of 1974 and/or the E-Government Act of 2002 and, if applicable; ● published a SORN and/or PIA. ***POTENTIAL ASSESSMENT METHODS AND OBJECTS****:* ***For Federal Agencies Only****:* *If an agency's SAOP determines that the identity proofing services is subject to Privacy Act and/or E-Government Act of 2002 requirements:* **Examine**: the agency's *System of Records Notice (SORN)* and/or *Privacy Impact Assessment (PIA)*, as applicable.

4 Authenticator Type-Specific Conformance Criteria

The following criteria apply when the associated authenticator type is being used, regardless of assurance level.

4.1 Memorized Secret Verifiers

MS-1	**REQUIREMENT**: If chosen by the subscriber, memorized secrets SHALL be at least 8 characters in length. (5.1.1.2) **SUPPLEMENTAL GUIDANCE**: Memorized secret length is the most reliable metric determining strength against online and offline guessing attacks. The objective is primarily to defend against online attacks (with throttling of guesses) and to provide some protection against offline attacks, with the primary defense for such attacks being secure storage of the verifier. **ASSESSMENT OBJECTIVE:** Determine if the above minimum memorized secret length is enforced. **POTENTIAL ASSESSMENT METHODS AND OBJECTS**: **Examine**: code and/or documentation to determine if minimum memorized secret length is checked. **Test:** Attempt to enroll or change a memorized secret with less than the required length. The user should be re-prompted with an explanation if this occurs.

MS-2	**REQUIREMENT**: If chosen by the CSP or verifier using an approved random number generator, memorized secrets SHALL be at least 6 characters in length. (5.1.1.2) **SUPPLEMENTAL GUIDANCE**: Memorized secret length is the most reliable metric determining strength against online and offline guessing attacks. The objective is primarily to defend against online attacks (with throttling of guesses) and to provide some protection against offline attacks, with the primary defense for such attacks being secure storage of the verifier. **ASSESSMENT OBJECTIVE:** Determine if the above minimum generated memorized secret length requirement is satisfied. **POTENTIAL ASSESSMENT METHODS AND OBJECTS**: **Examine**: code and/or documentation to determine if randomly generated memorized secrets are at least six characters in length and generated with an approved random number generator.

MS-3	**REQUIREMENT**: Truncation of the secret SHALL NOT be performed. (5.1.1.2) **SUPPLEMENTAL GUIDANCE**: Memorized secrets that are longer than expected by the verifier might (but must not) be simply truncated to an acceptable length. This gives a false impression of security to the user if the verifier only checks a subset of the memorized secret. **ASSESSMENT OBJECTIVE:** Determine if memorized secrets are being truncated prior to verification. **POTENTIAL ASSESSMENT METHODS AND OBJECTS**: **Test:** Set a memorized secret that is very long (longer than the expected maximum length) then try to authenticate with that secret with the last character changed. The test fails if the authentication attempt succeeds.

MS-4	**REQUIREMENT**: Memorized secret verifiers SHALL NOT permit the subscriber to store a "hint" that is accessible to an unauthenticated claimant. (5.1.1.2) **SUPPLEMENTAL GUIDANCE**: The availability of memorized secret hints greatly weakens the strength of memorized secret authenticators. **ASSESSMENT OBJECTIVE:** Determine if password hints and prompts are provided to the user. **POTENTIAL ASSESSMENT METHODS AND OBJECTS**: **Test:** Create a memorized secret authenticator and ensure that there is no provision for adding a hint.

MS-5	**REQUIREMENT**: Verifiers SHALL NOT prompt subscribers to use specific types of information (e.g., "What was the name of your first pet?") when choosing memorized secrets. (5.1.1.2) **SUPPLEMENTAL GUIDANCE**: Prompts for specific information (often called Knowledge-based Authentication or Security Questions) encourage use of the same memorized secrets at multiple sites, which causes a vulnerability to "password stuffing" attacks. This guidance applies to account recovery situations as well as normal authentication. **ASSESSMENT OBJECTIVE:** Determine that prompts are not used. **POTENTIAL ASSESSMENT METHODS AND OBJECTS**: **Test:** Attempt to authenticate (including "forgot password" situations) and determine that there is no use of knowledge-based authentication.

MS-6	**REQUIREMENT**: When processing requests to establish and change memorized secrets, verifiers SHALL compare the prospective secrets against a list that contains values known to be commonly used, expected, or compromised. (5.1.1.2) **SUPPLEMENTAL GUIDANCE**: The maintenance of a list of common memorized secrets that cannot be used by users protects provides protection against online attacks that might otherwise succeed before throttling mechanisms take effect to defend against these attacks. This is an alternative to the use of composition rules (requirements for particular character types, etc.) and can provide more customized protection against common memorized secrets. This list may include, but is not limited to: • Passwords obtained from previous breach corpuses. • Dictionary words. • Repetitive or sequential characters (e.g. 'aaaaaa', '1234abcd'). • Context-specific words, such as the name of the service, the username, and derivatives thereof. **ASSESSMENT OBJECTIVE:** Determine that a memorized secret "blocklist" exists and is used. **POTENTIAL ASSESSMENT METHODS AND OBJECTS**: **Examine**: verifier code and/or documentation to determine the existence and some typical entries in the common memorized secrets list.

MS-7	**REQUIREMENT**: If a chosen secret is found in the list, the CSP or verifier SHALL advise the subscriber that they need to select a different secret. (5.1.1.2) **SUPPLEMENTAL GUIDANCE**: The use of common memorized secrets greatly increases the vulnerability of the account to both online (guessing) and offline (cracking) attacks. This is an alternative to the use of composition rules (requirements for particular character types, etc.) and can provide more customized protection against common memorized secrets. **ASSESSMENT OBJECTIVE:** Determine that memorized secrets appearing on the "blocklist" are rejected. **POTENTIAL ASSESSMENT METHODS AND OBJECTS**: **Test:** Attempt to set an account to use a memorized secret that is on the blocklist. The attempt should fail.

MS-8	**REQUIREMENT**: If a chosen secret is found in the list, the CSP or verifier SHALL provide the reason for rejection. (5.1.1.2)

	SUPPLEMENTAL GUIDANCE: When a subscriber chooses a weak memorized secret, it is likely that they will choose another weak memorized secret that may or may not be on the blocklist. In addition to explaining to the user the reason for the rejection of their selection, it is helpful to provide coaching on better choices. Tools like password-strength meters are often useful in this situation. **ASSESSMENT OBJECTIVE:** Determine that users are appropriately notified when memorized secrets appearing on the "blocklist" are rejected. **POTENTIAL ASSESSMENT METHODS AND OBJECTS**: **Test:** Attempt to set an account to use a memorized secret that is on the blocklist. A message explaining the reason for rejection is required to be displayed.

MS-9	**REQUIREMENT**: If a chosen secret is found in the list, the CSP or verifier SHALL require the subscriber to choose a different value. (5.1.1.2) **SUPPLEMENTAL GUIDANCE**: When a subscriber chooses a weak memorized secret, the memorized secret change process is not complete until the subscriber has chosen a different value. **ASSESSMENT OBJECTIVE:** Determine that users are re-prompted when memorized secrets appearing on the "blocklist" are rejected. **POTENTIAL ASSESSMENT METHODS AND OBJECTS**: **Test:** Attempt to set an account to use a memorized secret that is on the blocklist. A prompt to repeat the memorized secret change is required.

MS-10	**REQUIREMENT**: Verifiers SHALL implement a rate-limiting mechanism that effectively limits the number of failed authentication attempts that can be made on the subscriber's account. (5.1.1.2) **SUPPLEMENTAL GUIDANCE**: Rate limiting restricts the ability of an attacker to make many online guessing attacks on the memorized secret. Other requirements (e.g., minimum length of memorized secrets) depend on the existence of rate limiting, so effective rate limiting is an essential capability. Ideally, a rate limiting mechanism should restrict the attacker as much as possible without creating an opportunity for a denial-of-service attack against the subscriber. **ASSESSMENT OBJECTIVE:** Determine that rate limiting is effectively applied. **POTENTIAL ASSESSMENT METHODS AND OBJECTS**: **Test:** Make repeated attempts to authenticate with the wrong memorized secret

	and determine that it is not possible to successfully authenticate immediately following a large number of incorrect attempts.

MS-11	**REQUIREMENT**: Verifiers SHALL force a change of memorized secret if there is evidence of compromise of the authenticator. (5.1.1.2) **SUPPLEMENTAL GUIDANCE**: Although requiring routine periodic changes to memorized secrets is not recommended, it is important that verifiers have the capability to prompt memorized secrets on an emergency basis if there is evidence of a possible successful attack. **ASSESSMENT OBJECTIVE:** Determine that the capability exists to force memorized secret changes when a compromise is suspected. **POTENTIAL ASSESSMENT METHODS AND OBJECTS**: **Examine**: Code and administrative controls to determine that the required capability is implemented.

MS-12	**REQUIREMENT**: The verifier SHALL use approved encryption when requesting memorized secrets in order to provide resistance to eavesdropping and MitM attacks. (5.1.1.2) **SUPPLEMENTAL GUIDANCE**: As defined in Appendix A of SP 800-63-3, cryptography is considered approved if it is specified or adopted in a FIPS or NIST recommendation. **ASSESSMENT OBJECTIVE:** Ensure that only secure, well-vetted cryptographic algorithms are being used. **POTENTIAL ASSESSMENT METHODS AND OBJECTS**: **Examine**: one or both of the following: ● *documented policies or practices* to determine that only approved cryptographic algorithms can be used. ● the *system's functionality* to observe the cryptographic algorithm(s) being accepted and determine whether the algorithms are approved.

MS-13	**REQUIREMENT**: The verifier SHALL use an authenticated protected channel when requesting memorized secrets in order to provide resistance to eavesdropping and MitM attacks. (5.1.1.2) **SUPPLEMENTAL GUIDANCE**: Communication between claimant and verifier is required to be via an encrypted channel that authenticates the verifier to provide confidentiality of the authenticator output and resistance to MitM

	attacks. This is typically accomplished using the Transport Level Security (TLS) protocol. **ASSESSMENT OBJECTIVE:** Determine that the communication channel meets the requirements of an authenticated protected channel as defined in SP 800-63-3 Appendix A. ● **POTENTIAL ASSESSMENT METHODS AND OBJECTS**: **Examine**: the verifier's API documentation to ensure that TLS or a similarly secure protocol is used in conjunction with an approved encryption protocol (see MS-12).

MS-14	**REQUIREMENT**: Verifiers SHALL store memorized secrets in a form that is resistant to offline attacks. (5.1.1.2) **SUPPLEMENTAL GUIDANCE**: Storage of memorized secret verifiers in a hashed form that is not readily reversed is a key protection against offline attacks. In no case should a verifier store memorized secrets in cleartext form. Criteria MS-15 through MS-17 provide more detail on how this is done. **ASSESSMENT OBJECTIVE:** Determine that storage of memorized secret verifiers is done securely. **POTENTIAL ASSESSMENT METHODS AND OBJECTS**: **Examine**: storage of memorized secret verifiers to determine that the memorized secrets are not stored in cleartext or an easily deciphered form.

MS-15	**REQUIREMENT**: Memorized secrets SHALL be salted and hashed using a suitable one-way key derivation function. (5.1.1.2) **SUPPLEMENTAL GUIDANCE**: Key derivation functions take a password, a salt, and a cost factor as inputs then generate a password hash. Their purpose is to make each password guessing trial by an attacker who has obtained a password hash file expensive and therefore the cost of a guessing attack high or prohibitive. Use of a key derivation with a salt, preferably with a time- and memory-hard key derivation function, provides the best protection against attackers that are able to obtain a copy of the verifier database. The choice of iteration count needs to take into account the workload of the verifier in handling authentication requests while making it as computationally difficult as possible for an attacker with stolen verifier values to determine the associated memorized secrets. **ASSESSMENT OBJECTIVE:** Determine that a suitable key derivation function is used prior to storage of memorized secret verifiers.

	POTENTIAL ASSESSMENT METHODS AND OBJECTS: **Examine**: code used to hash memorized secrets for storage and comparison with stored verifiers.

MS-16	**REQUIREMENT**: The salt SHALL be at least 32 bits in length and be chosen arbitrarily to minimize salt value collisions among stored hashes. (5.1.1.2) **SUPPLEMENTAL GUIDANCE**: Salt values need to be large enough to make it impractical for an attacker to precompute hashed verifier values (so called rainbow tables). While rainbow tables are typically quite large, this requirement would increase their size by a factor of about 4.3 billion. If not chosen arbitrarily, the attacker might be able to anticipate the salt values that would be used, which would eliminate much of this advantage. **ASSESSMENT OBJECTIVE:** Determine that salt values are sufficiently large and arbitrarily chosen. **POTENTIAL ASSESSMENT METHODS AND OBJECTS**: **Examine**: code used to generate salt values used in hashing memorized secrets for storage as verifiers.

MS-17	**REQUIREMENT**: Both the salt value and the resulting hash SHALL be stored for each subscriber using a memorized secret authenticator (5.1.1.2) **SUPPLEMENTAL GUIDANCE**: In order to verify a memorized secret, it needs to be salted and hashed for comparison with the stored verifier (resulting hash). To do this, the salt value needs to be available, and since it is different for each user, needs to be stored with the verifier. It is impractical to verify a memorized secret if this is not done. **ASSESSMENT OBJECTIVE:** Determine that storage of memorized secret verifiers includes the hash. **POTENTIAL ASSESSMENT METHODS AND OBJECTS**: **Examine**: stored verifiers to determine that they include both a field for the hash and the salt value used to obtain it.

MS-18	**REQUIREMENT**: 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 SHALL be generated with an approved random bit generator and of sufficient length. (5.1.1.2) **SUPPLEMENTAL GUIDANCE**: An additional keyed hashing iteration using a key value that is secret and stored separately from the verifiers provides

	excellent protection against even attackers ("password crackers") with substantial computing resources, provided the key is not also compromised. Accordingly, it is important that this salt, which is common to multiple users, be generated in a manner that is not vulnerable to compromise. **ASSESSMENT OBJECTIVE:** Determine that the additional key derivation step uses a securely generated key. **POTENTIAL ASSESSMENT METHODS AND OBJECTS**: **Examine**: procedure for generating the secret key for the additional hashing step and determine that it is done using an approved algorithm.

MS-19	**REQUIREMENT**: 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 SHALL provide at least the minimum-security strength specified in the latest revision of SP 800-131A. (5.1.1.2) **SUPPLEMENTAL GUIDANCE**: An additional keyed hashing iteration using a key value that is secret and stored separately from the verifiers provides excellent protection against even attackers ("password crackers") with substantial computing resources, provided the key is not also compromised. Accordingly, it is important that this salt, which is common to multiple users, be of sufficient size to make cryptographic and brute-force attacks impractical. Currently, the requirement is that the key be at least 112 bits in length. **ASSESSMENT OBJECTIVE:** Determine that the additional key derivation step uses a sufficiently large key. **POTENTIAL ASSESSMENT METHODS AND OBJECTS**: **Examine**: procedure for generating the secret key and for the additional hashing step and determine that the key and hashing operation are of sufficient size.

MS-20	**REQUIREMENT**: 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 SHALL be stored separately from the memorized secrets. (5.1.1.2) **SUPPLEMENTAL GUIDANCE**: An additional keyed hashing iteration using a key value that is secret and stored separately from the verifiers provides excellent protection against even attackers ("password crackers") with substantial computing resources, provided the key is not also compromised. Accordingly, it is important that this salt, which is common to multiple users, be stored separately so that it is unlikely to be compromised along with the verifier database. One way to do this is to perform this last hashing iteration on a physically separate processor, since it only requires a value to hash as input and provides the hashed value in response.

	ASSESSMENT OBJECTIVE: Determine that the additional key derivation step uses a key that is stored separately. **POTENTIAL ASSESSMENT METHODS AND OBJECTS**: **Examine**: procedure for accomplishing the additional hashing step and determine if the key used is stored separately, preferably in a separate processor.

4.2 Look-Up Secret Verifiers

LUS-1	**REQUIREMENT**: CSPs creating look-up secret authenticators SHALL use an approved random bit generator [SP 800-90Ar1] to generate the list of secrets. (5.1.2.1) **SUPPLEMENTAL GUIDANCE**: The use of a high-quality random bit generator is important to ensure that an attacker cannot guess the look-up secret. **ASSESSMENT OBJECTIVE:** Determine that the look-up secret is securely generated. **POTENTIAL ASSESSMENT METHODS AND OBJECTS**: **Examine**: code and/or documentation to determine that the generation process for look-up secrets uses an approved algorithm.

LUS-2	**REQUIREMENT**: Look-up secrets SHALL have at least 20 bits of entropy. (5.1.2.1) **SUPPLEMENTAL GUIDANCE**: Look-up secrets need to have enough entropy to ensure that brute-force guessing attacks do not succeed **ASSESSMENT OBJECTIVE:** Determine that the look-up secrets have at least the required complexity (entropy). **POTENTIAL ASSESSMENT METHODS AND OBJECTS**: **Examine**: Code and/or documentation showing the generation process for look-up secrets to determine that the effective entropy of the secrets is at least 20 bits.

LUS-3	**REQUIREMENT**: If look-up secrets are distributed online, then they SHALL be distributed over a secure channel in accordance with the post-enrollment binding requirements in Section 6.1.2. (5.1.2.1) **SUPPLEMENTAL GUIDANCE**: Look-up secrets need to be distributed in a manner that minimizes the opportunity for attackers to intercept the secrets either by eavesdropping or man-in-the-middle attacks.

	ASSESSMENT OBJECTIVE: Determine that the secrets are distributed over a suitable secure channel (in most cases an authenticated protected channel). **POTENTIAL ASSESSMENT METHODS AND OBJECTS**: **Test**: Cause the verifier to generate a set of look-up secrets and verify that they are distributed over a secure channel.

LUS-4	**REQUIREMENT**: Verifiers of look-up secrets SHALL prompt the claimant for the next secret from their authenticator or for a specific (e.g., numbered) secret. (5.1.2.2) **SUPPLEMENTAL GUIDANCE**: In most cases claimants will be prompted for the next unused memorized secret in a list but may be challenged to use a specific secret from a list. **ASSESSMENT OBJECTIVE:** Determine that the authentication transaction prompts the claimant correctly. **POTENTIAL ASSESSMENT METHODS AND OBJECTS**: **Test**: Authenticate more than once using look-up secrets and determine that the next secret, or the one specified by the verifier, is accepted, and others are rejected.

LUS-5	**REQUIREMENT**: A given secret from an authenticator SHALL be used successfully only once. (5.1.2.2) **SUPPLEMENTAL GUIDANCE**: Many threats, such as key logging, are enabled if the look-up secret can be used more than once. **ASSESSMENT OBJECTIVE:** Determine that look-up secrets can be used only once. **POTENTIAL ASSESSMENT METHODS AND OBJECTS**: **Test**: Authenticate several times and determine that each look-up secret is used only once. **Examine**: Authentication data at verifier to determine that look-up secrets that have been used are deleted or marked as invalid.

LUS-6	**REQUIREMENT**: If a look-up secret is derived from a grid card, then each cell of the grid SHALL be used only once. (5.1.2.2) **SUPPLEMENTAL GUIDANCE**: Grid cards are sometimes used to provide a rudimentary challenge-response authentication involving the claimant. However, an attacker such as a key logger that has persistent access to the endpoint can

	derive the contents of the grid, and potentially authenticate successfully, if grid entries are reused in subsequent authentication transactions. Absent the ability to reuse grid squares, grid cards will probably no longer be attractive as authenticators. **ASSESSMENT OBJECTIVE:** Determine that grid squares be used only once. **POTENTIAL ASSESSMENT METHODS AND OBJECTS**: **Test**: Authenticate several times and determine that each grid square is used at most once. **Examine**: Authentication data at verifier to determine that grid squares that have been used are deleted or marked as invalid.

LUS-7	**REQUIREMENT**: Verifiers SHALL store look-up secrets in a form that is resistant to offline attacks. (5.1.2.2) **SUPPLEMENTAL GUIDANCE**: Storage of look-up secret verifiers in a hashed form that is not readily reversed is a key protection against offline attacks. In no case should a verifier store look-up secrets in cleartext form. **ASSESSMENT OBJECTIVE:** Determine that storage of look-up secret verifiers is done securely. **POTENTIAL ASSESSMENT METHODS AND OBJECTS**: **Examine**: Verifier authentication database to determine how look-up secret verifiers are stored.

LUS-8	**REQUIREMENT**: If look-up secrets have at least 112 bits of entropy, then they SHALL be hashed with an approved one-way function (5.1.2.2) **SUPPLEMENTAL GUIDANCE**: Use of an approved one-way function effectively protects the look-up secrets from disclosure if the verifier is compromised. Salting of secrets with this amount of entropy is not required because it is not practical to mount brute-force or cryptographic attacks against secrets this large. **ASSESSMENT OBJECTIVE:** Determine that look-up secret verifiers is done in hashed form. **POTENTIAL ASSESSMENT METHODS AND OBJECTS**: **Examine**: Verifier authentication database to determine that look-up secret verifiers are stored in hashed form. If possible, compare the verifier value against a hash of a known look-up secret and determine that they match.

LUS-9	**REQUIREMENT**: If look-up secrets have less than 112 bits of entropy, then they SHALL be salted and hashed using a suitable one-way key derivation function. (5.1.2.2) **SUPPLEMENTAL GUIDANCE**: Key derivation functions take a look-up secret, a salt, and a cost factor as inputs then generate a hash. Their purpose is to make each look-up secret guessing trial by an attacker who has obtained a look-up secret hash file expensive and therefore the cost of a guessing attack high or prohibitive. Use of a key derivation with a salt, preferably with a time- and memory-hard key derivation function, provides the best protection against attackers that are able to obtain a copy of the verifier database. The choice of iteration count needs to consider the complexity of the look-up secrets (more iterations for less complex secrets) and the workload of the verifier in handling authentication requests while making it as computationally difficult as possible for an attacker with stolen verifier values to determine the associated memorized secrets. **ASSESSMENT OBJECTIVE:** Determine that a suitable key derivation function is used prior to storage of look-up secret verifiers. **POTENTIAL ASSESSMENT METHODS AND OBJECTS**: **Examine**: code used to hash look-up secrets for storage and comparison with stored verifiers.

LUS-10	**REQUIREMENT**: If look-up secrets have less than 112 bits of entropy, then the salt SHALL be at least 32 bits in length and be chosen arbitrarily to minimize salt value collisions among stored hashes. (5.1.2.2) **SUPPLEMENTAL GUIDANCE**: Salt values need to be large enough to make it impractical for an attacker to precompute hashed verifier values (so called rainbow tables). While rainbow tables are typically quite large, this requirement would increase their size by a factor of about 4.3 billion. If not chosen arbitrarily, the attacker might be able to anticipate the salt values that would be used, which would eliminate much of this advantage. **ASSESSMENT OBJECTIVE:** Determine that salt values are sufficiently large and arbitrarily chosen. **POTENTIAL ASSESSMENT METHODS AND OBJECTS**: **Examine**: code used to generate salt values used in hashing look-up secrets for storage as verifiers.

LUS-11	**REQUIREMENT**: If look-up secrets have less than 112 bits of entropy, then both the salt value and the resulting hash SHALL be stored for each look-up secret (5.1.2.2) **SUPPLEMENTAL GUIDANCE**: In order to verify a look-up secret, it needs to be salted and hashed for comparison with the stored verifier (resulting hash). To do this, the salt value needs to be available, and since it is different for each secret, needs to be stored with the verifier. It is impractical to verify a look-up secret if this is not done. **ASSESSMENT OBJECTIVE:** Determine that storage of look-up secret verifiers includes the hash. **POTENTIAL ASSESSMENT METHODS AND OBJECTS**: **Examine**: stored verifiers to determine that they include both a field for the hash and the salt value used to obtain it.

LUS-12	**REQUIREMENT**: If look-up secrets that have less than 64 bits of entropy, then the verifier SHALL implement a rate-limiting mechanism that effectively limits the number of failed authentication attempts that can be made on the subscriber's account. (5.1.2.2) **SUPPLEMENTAL GUIDANCE**: Rate limiting restricts the ability of an attacker to make many online guessing attacks on the look-up secret. Other requirements (e.g., minimum length of look-up secrets) depend on the existence of rate limiting, so effective rate limiting is an essential capability. Ideally, a rate limiting mechanism should restrict the attacker as much as possible without creating an opportunity for a denial-of-service attack against the subscriber. **ASSESSMENT OBJECTIVE:** Determine that verifiers of look-up secrets with less than 64 bits of entropy are appropriately rate limited. **POTENTIAL ASSESSMENT METHODS AND OBJECTS**: **Test:** Make repeated attempts to authenticate with invalid look-up secrets and determine that it is not possible to successfully authenticate immediately following a large number of incorrect attempts.

LUS-13	**REQUIREMENT**: The verifier SHALL use approved encryption when requesting look-up secrets in order to provide resistance to eavesdropping and MitM attacks. (5.1.2.2) **SUPPLEMENTAL GUIDANCE**: As defined in Appendix A of SP 800-63-3, cryptography is considered approved if it is specified or adopted in a FIPS or NIST recommendation.

	ASSESSMENT OBJECTIVE: Ensure that only secure, well-vetted cryptographic algorithms are being used. **POTENTIAL ASSESSMENT METHODS AND OBJECTS**: **Examine**: one or both of the following: ● *documented policies or practices* to determine that only approved cryptographic algorithms can be used. ● the *system's functionality* to observe the cryptographic algorithm(s) being accepted.

LUS-14	**REQUIREMENT**: The verifier SHALL use an authenticated protected channel when requesting look-up secrets in order to provide resistance to eavesdropping and MitM attacks. (5.1.2.2) **SUPPLEMENTAL GUIDANCE**: Communication between claimant and verifier is required to be via an encrypted channel that authenticates the verifier to provide confidentiality of the authenticator output and resistance to MitM attacks. This is typically accomplished using the Transport Level Security (TLS) protocol. **ASSESSMENT OBJECTIVE:** Determine that the communication channel meets the requirements of an authenticated protected channel as defined in SP 800-63-3 Appendix A. **POTENTIAL ASSESSMENT METHODS AND OBJECTS**: **Examine**: the verifier's API documentation to ensure that TLS or a similarly secure protocol is used in conjunction with an approved encryption protocol (see LUS-13).

4.3 Out-of-Band Verifiers

OOB-1	**REQUIREMENT**: The out-of-band authenticator SHALL establish a separate channel with the verifier in order to retrieve the out-of-band secret or authentication request. (5.1.3.1) **SUPPLEMENTAL GUIDANCE**: A channel is considered to be out-of-band with respect to the primary communication channel (even if it terminates on the same device) provided the device does not leak information from one channel to the other without the authorization of the claimant. **ASSESSMENT OBJECTIVE:** Determine the nature of the communication channel used by the out-of-band authenticator.

	POTENTIAL ASSESSMENT METHODS AND OBJECTS: **Test:** If the same device is being used for the authenticated session and the authenticator, observe traffic between the verifier and that device to determine that a separate channel is being used for authentication.

OOB-2	**REQUIREMENT**: Communication over the secondary channel SHALL be encrypted unless sent via the public switched telephone network (PSTN). (5.1.3.1) **SUPPLEMENTAL GUIDANCE**: The secondary channel requires protection to ensure that authentication secrets are not leaked to attackers. Legacy use of the PSTN as an OOB authentication medium is exempt from this requirement, although other requirements apply (see Section 5.1.3.3). **ASSESSMENT OBJECTIVE:** Determine that the secondary communication channel is suitably secure. **POTENTIAL ASSESSMENT METHODS AND OBJECTS**: **Examine**: the verifier's API documentation to determine that TLS or a similarly secure protocol is used.

OOB-3	**REQUIREMENT**: Methods that do not prove possession of a specific device, such as voice-over-IP (VOIP) or email, SHALL NOT be used for out-of-band authentication. (5.1.3.1) **SUPPLEMENTAL GUIDANCE**: Communication with VoIP phone numbers and email do not establish the possession of a specific device, so they are not suitable for use in out-of-band authentication which is used as a physical authenticator (something you have). **ASSESSMENT OBJECTIVE:** Determine that these all methods of communication with out-of-band devices prove possession and control of a specific device. **POTENTIAL ASSESSMENT METHODS AND OBJECTS**: **Examine**: Verifier documentation to determine that out-of-band communication is always done with specific devices. For example, determine whether phone numbers are checked to disqualify VoIP phone numbers if PSTN out-of-band authentication is used. Determine that authentication using email is not possible, including in account recovery situations.

OOB-4	**REQUIREMENT**: If PSTN is not being used for out-of-band communication, then the out-of-band authenticator SHALL uniquely authenticate itself by establishing an authenticated protected channel with the verifier. (5.1.3.1)

	SUPPLEMENTAL GUIDANCE: Communication between out-of-band device and verifier is required to be via an encrypted channel to provide confidentiality of the authenticator output and resistance to MitM attacks. This is typically accomplished using the Transport Level Security (TLS) protocol. **ASSESSMENT OBJECTIVE:** Determine that the communication channel meets the requirements of an authenticated protected channel as defined in SP 800-63-3 Appendix A. **POTENTIAL ASSESSMENT METHODS AND OBJECTS**: **Examine**: documentation and/or code from the authenticator application to determine how the secret is being stored and whether it is copied when the device is backed up.

OOB-5	**REQUIREMENT**: If PSTN is not being used for out-of-band communication, then the out-of-band authenticator SHALL communicate with the verifier using approved cryptography. (5.1.3.1) **SUPPLEMENTAL GUIDANCE**: As defined in Appendix A of SP 800-63-3, cryptography is considered approved if it is specified or adopted in a FIPS or NIST recommendation. **ASSESSMENT OBJECTIVE:** Determine that only secure, well-vetted cryptographic algorithms are being used. **POTENTIAL ASSESSMENT METHODS AND OBJECTS**: **Examine**: one or both of the following: ● *documented policies or practices* to determine that only approved cryptographic algorithms can be used. ● the *system's functionality* to observe the cryptographic algorithm(s) being accepted and determine whether the algorithms are approved.

OOB-6	**REQUIREMENT**: If PSTN is not being used for out-of-band communication, then the key used to authenticate the out-of-band device SHALL be stored in suitably secure storage available to the authenticator application (e.g., keychain storage, TPM, TEE, secure element). (5.1.3.1) **SUPPLEMENTAL GUIDANCE**: 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. **ASSESSMENT OBJECTIVE:** Determine how the secret key identifying the specific instance of the device or application used by the subscriber is stored.

	POTENTIAL ASSESSMENT METHODS AND OBJECTS: **Examine**: documentation and/or code from the authenticator device application to determine that the secret is being stored securely and that it is not copied when the device is backed up.

OOB-7	**REQUIREMENT**: If the PSTN is used for out-of-band authentication and a secret is sent to the out-of-band device via the PSTN, then the out-of-band authenticator SHALL uniquely authenticate itself to a mobile telephone network using a SIM card or equivalent that uniquely identifies the device. (5.1.3.1) **SUPPLEMENTAL GUIDANCE**: Since the PSTN does not support the establishment of authenticated protected channels, the alternative method of authenticating the device via the PSTN is supported. Note that there are other specific requirements for use of the PSTN that also apply (see Section 5.1.3.3). **ASSESSMENT OBJECTIVE:** Determine whether the device authenticates to the PSTN if it is used for an out-of-band authentication channel. **POTENTIAL ASSESSMENT METHODS AND OBJECTS**: **Examine**: documentation describing the method of enrolling a new out-of-band device and determine that only devices that authenticate to the network (i.e., mobile phones and not VoIP endpoints) are usable as out-of-band devices.

OOB-8	**REQUIREMENT**: If the out-of-band authenticator sends an approval message over the secondary communication channel, it SHALL either accept 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. (5.1.3.1) **SUPPLEMENTAL GUIDANCE**: Most out-of-band verifiers operate by sending a secret over the secondary channel that the subscriber transfers to the primary channel. Other methods are possible, however, specifically transferring from primary to secondary and user comparison of secrets sent to both channels (with approval being sent to the verifier over the secondary channel). It is good practice to display descriptive information relating to the authentication on the claimant's out-of-band device, to provide additional assurance that the transaction being approved by the subscriber is the correct one, and not from an attacker who exploits the subscriber's approval. **ASSESSMENT OBJECTIVE:** Determine that all out-of-band authentication flows approve the intended transaction in a secure manner. **POTENTIAL ASSESSMENT METHODS AND OBJECTS**: **Test:** Authenticate using an out-of-band device and determine that either the

	subscriber transfers a secret between devices or through comparison of secrets obtained from both devices.

OOB-9	**REQUIREMENT**: The verifier SHALL NOT store the identifying key itself, but SHALL use a verification method (e.g., an approved hash function or proof of possession of the identifying key) to uniquely identify the authenticator. (5.1.3.2) **SUPPLEMENTAL GUIDANCE**: In order for the out-of-band authenticator to be considered "something you have", it must be securely authenticated as a unique device or instance of a software-based authentication application. This is required to be done through proof of possession of a key by the authenticator, rather than presentation of the key itself. This provides verifier compromise resistance with respect to the authentication key. PSTN protocols use a proof-of-possession protocol using a secret on the SIM card of mobile devices to authenticate the device, so this requirement is met for PSTN-based authentication. **ASSESSMENT OBJECTIVE:** Determine that a proof-of-possession protocol is used to authenticate the out-of-band authenticator. **POTENTIAL ASSESSMENT METHODS AND OBJECTS**: **Examine**: documentation and/or code for the verifier to determine that the protocol used to authenticate the out-of-band authenticator uses a proof-of-possession protocol.

OOB-10	**REQUIREMENT**: Depending on the type of out-of-band authenticator, one of the following SHALL take place: transfer of a secret to the primary channel, transfer of a secret to the secondary channel, or verification of secrets by the claimant. (5.1.3.2) **SUPPLEMENTAL GUIDANCE**: Three different methods of associating the primary and secondary channel sessions are permitted. The intent of these methods is to establish approval for a specific authentication transaction, and to minimize the likelihood that an attacker with knowledge of when the subscriber authenticates can obtain approval for a rogue authentication. **ASSESSMENT OBJECTIVE:** Determine that out-of-band authentication transactions use one of the three approved flows. **POTENTIAL ASSESSMENT METHODS AND OBJECTS**: **Test**: Initiate an out-of-band authentication transaction and determine that the out-of-band secret is either transferred or displayed for comparison by the

	claimant. If the authenticator provides multiple authentication flows, determine that all flows meet this requirement.

OOB-11	**REQUIREMENT**: If the out-of-band authenticator operates by transferring the secret to the primary channel, then the verifier SHALL transmit a random secret to the out-of-band authenticator and then wait for the secret to be returned on the primary communication channel. (5.1.3.2) **SUPPLEMENTAL GUIDANCE**: This is the most common form of out-of-band authentication where an authentication secret is transmitted to the out-of-band device and entered by the user for transmission on the primary channel. **ASSESSMENT OBJECTIVE:** Determine that out-of-band authentication using a transfer of the secret from the out-of-band device to the primary channel operates as described. **POTENTIAL ASSESSMENT METHODS AND OBJECTS**: **Test**: Initiate an out-of-band authentication transaction and determine that the out-of-band secret is transferred from the out-of-band authenticator to the session being authenticated.

OOB-12	**REQUIREMENT**: If the out-of-band authenticator operates by transferring the secret to the secondary channel, then the verifier SHALL display 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. (5.1.3.2) **SUPPLEMENTAL GUIDANCE**: This is a less typical authentication flow but is also acceptable in that the secret securely associates possession and control of the out-of-band authenticator with the session being authenticated. **ASSESSMENT OBJECTIVE:** Determine that out-of-band authentication using a transfer of the secret from the primary channel to the out-of-band authenticator operates as described. **POTENTIAL ASSESSMENT METHODS AND OBJECTS**: **Test**: Initiate an out-of-band authentication transaction and determine that successful authentication depends on the out-of-band secret being transferred correctly from the out-of-band authenticator to the session being authenticated.

OOB-13	**REQUIREMENT**: If the out-of-band authenticator operates by verification of secrets by the claimant, then the verifier SHALL display 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. (5.1.3.2) **SUPPLEMENTAL GUIDANCE**: This is a somewhat more user-friendly authentication flow because it does not require the claimant to read and manually enter the authentication secret, but it carries the additional risk that the claimant will approve the authentication without actually comparing the secrets received from the independent channels. Approval is required to be obtained from the out-of-band authenticator rather than the primary channel because that at least establishes control of the authenticator. **ASSESSMENT OBJECTIVE:** Determine that out-of-band authentication using verification of secrets received from the primary channel and the out-of-band authenticator operates as described. **POTENTIAL ASSESSMENT METHODS AND OBJECTS**: **Test**: Initiate an out-of-band authentication transaction and determine that successful authentication depends a positive response by the claimant that the out-of-band secret received from the session being authenticated and the out-of-band authenticator are the same, and that a response to the contrary causes authentication to fail.

OOB-14	**REQUIREMENT**: The authentication SHALL be considered invalid if not completed within 10 minutes. (5.1.3.2) **SUPPLEMENTAL GUIDANCE**: Secrets used in out-of-band authentication are short-term secrets and need to have a definite lifetime. This requirement also relieves the verifier from the responsibility of log-term storage of the secrets. **ASSESSMENT OBJECTIVE:** Determine that out-of-band authentication secrets expire as required. **POTENTIAL ASSESSMENT METHODS AND OBJECTS**: **Test**: Initiate an out-of-band authentication transaction, but delay responding until slightly more than 10 minutes has passed. If the authentication succeeds, this requirement has not been met.

OOB-15	**REQUIREMENT**: Verifiers SHALL accept a given authentication secret only once during the validity period. (5.1.3.2) **SUPPLEMENTAL GUIDANCE**: In order to prevent an attacker who gains access to an authentication secret generated by the subscriber from using it, it is important that the secret only be valid for a single authentication. This requirement only applies when a secret is being transferred between the primary channel and the out-of-band authenticator.

	ASSESSMENT OBJECTIVE: Determine that an out-of-band secret can be used only once. **POTENTIAL ASSESSMENT METHODS AND OBJECTS**: **Test**: Initiate two out-of-band authentication transactions and attempt to use the same secret for both transactions. If both authentications succeed, this requirement has not been met.

OOB-16	**REQUIREMENT**: The verifier SHALL generate random authentication secrets with at least 20 bits of entropy. (5.1.3.2) **SUPPLEMENTAL GUIDANCE**: Consistent with other short-term authentication secrets, 20 bits of entropy are required to provide resistance against brute force attacks. 6-digit numeric secrets (19.93 bits of entropy) are sufficiently close to 20 bits to be acceptable. **ASSESSMENT OBJECTIVE:** Determine that the out-of-band secrets have at least the required complexity (entropy). **POTENTIAL ASSESSMENT METHODS AND OBJECTS**: **Test**: Obtain a representative set of out-of-band secrets to obtain an estimate for their entropy (complexity) and determine that it is at least 20 bits.

OOB-17	**REQUIREMENT**: The verifier SHALL generate random authentication secrets using an approved random bit generator [SP 800-90Ar1]. (5.1.3.2) **SUPPLEMENTAL GUIDANCE**: The use of a high-quality random bit generator is important to ensure that an attacker cannot guess the out-of-band secret. **ASSESSMENT OBJECTIVE:** Determine that out-of-band secrets are securely generated. **POTENTIAL ASSESSMENT METHODS AND OBJECTS**: **Examine**: code and/or documentation to determine that the generation process for out-of-band secrets uses an approved algorithm.

OOB-18	**REQUIREMENT**: If the authentication secret has less than 64 bits of entropy, the verifier SHALL implement 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 Section 5.2.2. (5.1.3.2) **SUPPLEMENTAL GUIDANCE**: Rate limiting limits the opportunity for attackers to mount a brute-force attack on the out-of-band verifier. Since the out-

	of-band secret has a limited lifetime, it is sufficient to limit the number of attempts allowed during the (maximum) 10-minute lifetime of the secret. **ASSESSMENT OBJECTIVE:** Ensure that the number of attempts to enter an out-of-band secret are limited. **POTENTIAL ASSESSMENT METHODS AND OBJECTS**: **Test**: Attempt to make at least 100 tries entering an incorrect out-of-band secret. If this is possible, and a subsequent attempt with the correct secret succeeds in authenticating, this requirement has not been met.

OOB-19	**REQUIREMENT**: If out-of-band verification is to be made using the PSTN, then the verifier SHALL verify that the pre-registered telephone number being used is associated with a specific physical device. (5.1.3.3) **SUPPLEMENTAL GUIDANCE**: Some telephone numbers, such as those that are associated with VoIP services, are not associated with a specific device and can receive calls and text messages without establishing possession and control of a specific device. Such telephone numbers are not suitable for OOB authentication. Services exist to distinguish telephone numbers that are associated with a device from those that aren't. **ASSESSMENT OBJECTIVE:** Determine if the verifier blocks use of unsuitable phone numbers as required. **POTENTIAL ASSESSMENT METHODS AND OBJECTS**: **Test**: Attempt to register a VoIP phone number for out-of-band authentication. If the registration succeeds, this requirement has not been met.

OOB-20	**REQUIREMENT**: 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 SHALL only occur as described in Section 6.1.2. (5.1.3.3) **SUPPLEMENTAL GUIDANCE**: The binding of a new authenticator requires that the subscriber authenticate at the same or a higher AAL than that at which the authenticator will be used, and that a notification be sent to the subscriber. This is required to prevent attackers from changing the phone number of a PSTN-based out-of-band authenticator to one they control. **ASSESSMENT OBJECTIVE:** Confirm that changes in out-of-band authentication are performed securely. **POTENTIAL ASSESSMENT METHODS AND OBJECTS**: **Test**: Determine that a change in the out-of-band authentication telephone

	number cannot be made without first completing authentication at AAL2. Determine that a notification of the change is sent to the subscriber.

OOB-21	**REQUIREMENT**: If PSTN is used for out-of-band authentication, then the CSP SHALL offer subscribers at least one alternate authenticator that is not RESTRICTED and can be used to authenticate at the required AAL. (5.2.10) **SUPPLEMENTAL GUIDANCE**: Use of the PSTN for out-of-band authentication involves additional risk, resulting in its being designated as a restricted authenticator. CSPs are required to provide subscribers with a meaningful alternative. **ASSESSMENT OBJECTIVE:** Determine that alternative authenticators are available. **POTENTIAL ASSESSMENT METHODS AND OBJECTS**: **Test**: When provisioning a PSTN-based out-of-band authenticator, determine that alternative physical authenticators are available for all platforms (desktop, mobile, app) that the subscriber might use.

OOB-22	**REQUIREMENT**: If PSTN is used for out-of-band authentication, then the CSP SHALL Provide meaningful notice to subscribers regarding the security risks of the RESTRICTED authenticator and availability of alternative(s) that are not RESTRICTED. (5.2.10) **SUPPLEMENTAL GUIDANCE**: Use of the PSTN for out-of-band authentication involves additional risk, resulting in its being designated as a restricted authenticator. CSPs are required to explain these risks to subscribers and offer more secure alternatives. **ASSESSMENT OBJECTIVE:** Determine that notice regarding security risks is provided. **POTENTIAL ASSESSMENT METHODS AND OBJECTS**: **Test**: When provisioning a PSTN-based out-of-band authenticator, determine that notice is provided regarding security risks of PSTN authentication and the availability of alternative physical authenticators.

OOB-23	**REQUIREMENT**: If PSTN is used for out-of-band authentication, then the CSP SHALL address any additional risk to subscribers in its risk assessment. (5.2.10)

	SUPPLEMENTAL GUIDANCE: Use of the PSTN for out-of-band authentication involves additional risk, resulting in its being designated as a restricted authenticator. These risks need to be documented. **ASSESSMENT OBJECTIVE:** Determine that the necessary risk assessment has taken place. **POTENTIAL ASSESSMENT METHODS AND OBJECTS**: **Examine**: the risk assessment to determine that the risks of using a restricted authenticator in the relevant application are properly documented.

OOB-24	**REQUIREMENT**: If PSTN is used for out-of-band authentication, then the CSP SHALL develop 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. (5.2.10) **SUPPLEMENTAL GUIDANCE**: Use of the PSTN for out-of-band authentication involves additional risk, resulting in its being designated as a restricted authenticator. A plan for eliminating them in the future needs to be documented. **ASSESSMENT OBJECTIVE:** Determine that the necessary planning has taken place. **POTENTIAL ASSESSMENT METHODS AND OBJECTS**: **Examine**: the digital identity acceptance statement to determine that a plan for migration away from the use of PSTN out-of-band authentication is properly documented.

4.4 OTP Verifiers

OTP-1	**REQUIREMENT**: The secret key and its algorithm SHALL provide at least the minimum security strength specified in the latest revision of SP 800-131A (112 bits as of the date of this publication). (5.1.4.1, 5.1.5.1) **SUPPLEMENTAL GUIDANCE**: The secret key used by an OTP authenticator needs to be sufficiently complex to resist online and offline attacks. An attacker may have the ability to observe the authenticator output at some point during its operation; it needs to be impractical for the secret key to be derived from a set of these observations. **ASSESSMENT OBJECTIVE:** Determine that the secret key is sufficiently complex, taking into consideration the algorithm being used.

	POTENTIAL ASSESSMENT METHODS AND OBJECTS: **Examine**: the code and/or documentation for the verifier to determine that the complexity (entropy) associated with the secret key is sufficient.

OTP-2	**REQUIREMENT**: The nonce SHALL be of sufficient length to ensure that it is unique for each operation of the device over its lifetime. (5.1.4.1, 5.1.5.1) **SUPPLEMENTAL GUIDANCE**: If the nonce isn't long enough, the output of the authenticator will repeat, which represents an easily avoided vulnerability. **ASSESSMENT OBJECTIVE:** Determine that the nonce is sufficiently long that the same nonce will not be reused. **POTENTIAL ASSESSMENT METHODS AND OBJECTS**: **Examine**: documentation describing the manner in which the nonce is updated following each generation of an authenticator output. Calculate the number of authentications or period of time before the nonce repeats and determine that it is greater than the lifetime of any authenticator.

OTP-3	**REQUIREMENT**: OTP authenticators — particularly software-based OTP generators —SHALL NOT facilitate the cloning of the secret key onto multiple devices. (5.1.4.1, 5.1.5.1) **SUPPLEMENTAL GUIDANCE**: Like other physical authenticators, the use of OTP authenticators is premised upon the authenticator secret being present in a single authenticator so that it proves possession of a specific device. Mechanisms that would facilitate cloning the secret onto multiple devices include the ability to enroll more than one device producing the same OTP output and backup mechanisms, especially when software-based authenticators are used. Verifiers are expected to make their best effort at determining that bring-your-own authenticators not issued by them meet this requirement and to have policies not allowing the use of non-compliant authenticators. **ASSESSMENT OBJECTIVE:** Determine that the management of authenticator secrets is sufficiently secure to ensure that authenticators have unique secrets. **POTENTIAL ASSESSMENT METHODS AND OBJECTS**: **Examine**: process for provisioning secrets on authenticators when they are associated with a subscriber account. For software-based authenticators, examine the process for backing up the authenticator secret to determine that there is not a mechanism to allow more than one authenticator to share the same secret.

OTP-4	**REQUIREMENT**: The authenticator output SHALL have at least 6 decimal digits (approximately 20 bits) of entropy. (5.1.4.1, 5.1.5.1) **SUPPLEMENTAL GUIDANCE**: Consistent with other short-term authentication secrets, 20 bits of entropy are required to provide resistance against brute force attacks. 6-digit numeric secrets (19.93 bits of entropy) are sufficiently close to 20 bits to be acceptable. **ASSESSMENT OBJECTIVE:** Determine that the authenticator output has at least the required complexity (entropy). **POTENTIAL ASSESSMENT METHODS AND OBJECTS**: **Test**: Obtain a representative set of authenticator outputs to obtain an estimate for their entropy (complexity) and determine that it is at least 20 bits.

OTP-5	**REQUIREMENT**: If the nonce used to generate the authenticator output is based on a real-time clock, then the nonce SHALL be changed at least once every 2 minutes. (5.1.4.1, 5.1.5.1) **SUPPLEMENTAL GUIDANCE**: The authenticator output needs to be changed often enough that there is reasonable assurance that it is in the possession of the claimant and that it is not susceptible to OTP-guessing attacks. **ASSESSMENT OBJECTIVE:** Determine that the output of time-based OTP authenticators changes often enough. **POTENTIAL ASSESSMENT METHODS AND OBJECTS**: **Examine**: authenticator and/or verifier code to determine that the rate at which new authenticator outputs are generated is sufficient. **Test:** Observe the rate at which authenticator outputs are generated to determine that their rate is sufficient.

OTP-6	**REQUIREMENT**: The OTP value associated with a given nonce SHALL be accepted only once. (5.1.4.1, 5.1.5.1) **SUPPLEMENTAL GUIDANCE**: A fundamental premise of a “one-time” authenticator is that it can be used successfully only once during its validity period. **ASSESSMENT OBJECTIVE:** Determine that the authenticator output can be used only once while it is valid. **POTENTIAL ASSESSMENT METHODS AND OBJECTS**: **Test**: Determine that it is not possible to successfully authenticate more than

	once using the same authenticator output (during the validity period, if time-based).

OTP-7	**REQUIREMENT**: The symmetric keys used by authenticators are also present in the verifier, and SHALL be strongly protected against compromise. (5.1.4.2, 5.1.5.2) **SUPPLEMENTAL GUIDANCE**: Verifiers typically contain symmetric keys for all subscribers using OTP authenticators. This makes them a particularly rich target for attackers. While the protection of these keys is implementation-dependent and there is therefore no specific requirement for how the keys are protected, measures to prevent the exfiltration of the keys are needed. An example of such a measure is the storage of keys and generation of authenticator outputs in a separate device accessible only by the verifier. **ASSESSMENT OBJECTIVE:** Determine that the verifier stores OTP authenticator keys securely. **POTENTIAL ASSESSMENT METHODS AND OBJECTS**: **Examine**: method in which the authenticator keys are stored and determine whether the keys are well protected against compromise.

OTP-8	**REQUIREMENT**: If a single-factor OTP authenticator is being associated with a subscriber account, then the verifier or associated CSP SHALL use approved cryptography to either generate and exchange or to obtain the secrets required to duplicate the authenticator output. (5.1.4.2, 5.1.5.2) **SUPPLEMENTAL GUIDANCE**: It is critical that authentication secrets be generated and transferred or negotiated securely. This includes the use of secure random number generators and protocols for transferring or negotiating (e.g., Diffie-Hellman) secret values. As defined in Appendix A of SP 800-63-3, cryptography is considered approved if it is specified or adopted in a FIPS or NIST recommendation. **ASSESSMENT OBJECTIVE:** Determine that approved cryptographic algorithms are used. **POTENTIAL ASSESSMENT METHODS AND OBJECTS**: **Examine**: one or both of the following: ● *documented policies or practices* to determine that only approved cryptographic algorithms can be used. ● the *system's functionality* to observe the cryptographic algorithm(s) being used and determine whether the algorithms are approved.

OTP-9	**REQUIREMENT**: The verifier SHALL use approved encryption when collecting the OTP. (5.1.4.2, 5.1.5.2) **SUPPLEMENTAL GUIDANCE**: As defined in Appendix A of SP 800-63-3, cryptography is considered approved if it is specified or adopted in a FIPS or NIST recommendation. **ASSESSMENT OBJECTIVE:** Ensure that only secure, well-vetted cryptographic algorithms are being used. **POTENTIAL ASSESSMENT METHODS AND OBJECTS**: **Examine**: one or both of the following: • *documented policies or practices* to determine that only approved cryptographic algorithms can be used. the *system's functionality* to observe the cryptographic algorithm(s) being accepted and determine that the algorithms are approved.

OTP-10	**REQUIREMENT**: The verifier SHALL use an authenticated protected channel when collecting the OTP. (5.1.4.2, 5.1.5.2) **SUPPLEMENTAL GUIDANCE**: Communication between claimant and verifier is required to be via an encrypted channel that authenticates the verifier to provide confidentiality of the authenticator output and resistance to MitM attacks. This is typically accomplished using the Transport Level Security (TLS) protocol. **ASSESSMENT OBJECTIVE:** Determine that the communication channel meets the requirements of an authenticated protected channel as defined in SP 800-63-3 Appendix A. **POTENTIAL ASSESSMENT METHODS AND OBJECTS**: **Examine**: the verifier's API documentation to ensure that TLS or a similarly secure protocol is used in conjunction with an approved encryption protocol. **Test:** Authenticate using an OTP authenticator and verify that the authenticator output is collected in a protected session such as TLS. Observe the cryptographic algorithms used in the connection.

OTP-11	**REQUIREMENT**: If a time-based OTPs [RFC 6238] is used, it SHALL have a defined lifetime 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. (5.1.4.2, 5.1.5.2) **SUPPLEMENTAL GUIDANCE**: The clocks on time-based authenticators are subject to drift because of cost and environmental factors such as temperature.

	Accordingly, verifiers need to accept authenticator outputs before and particularly after the intended validity period to allow use by authenticators that are not in synchronization. **ASSESSMENT OBJECTIVE:** Determine that verifiers provide an appropriate "grace period" around the expected validity window. **POTENTIAL ASSESSMENT METHODS AND OBJECTS**: **Examine**: documentation, code, and specifications for the OTP device hardware as appropriate to determine that the verifier will accept an authenticator output submitted an appropriate amount of time before or after the actual authentication time window.

OTP-12	**REQUIREMENT**: Verifiers SHALL accept a given time-based OTP only once during the validity period. (5.1.4.2, 5.1.5.2) **SUPPLEMENTAL GUIDANCE**: In order to prevent an attacker who gains access to an OTP authenticator output from using it, it is important that the secret only be valid for a single authentication. **ASSESSMENT OBJECTIVE:** Determine that the authenticator output can be used only once while it is valid. **POTENTIAL ASSESSMENT METHODS AND OBJECTS**: **Test**: Determine that it is not possible to successfully authenticate more than once using the same authenticator output (during the validity period, if time-based).

OTP-13	**REQUIREMENT**: If the authenticator output has less than 64 bits of entropy, the verifier SHALL implement 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 Section 5.2.2. (5.1.4.2, 5.1.5.2) **SUPPLEMENTAL GUIDANCE**: OTPs whose output has less entropy are more vulnerable to online guessing attacks. To mitigate these attacks, rate limiting is required. Online guessing attacks are less of a concern for time-based OTP authenticators because of the limited validity window, but a limit on the number of guesses during a given validity period is effective in resisting automated attacks. **ASSESSMENT OBJECTIVE:** Ensure that rate-limiting is used for less complex OTP outputs. **POTENTIAL ASSESSMENT METHODS AND OBJECTS**: **Test**: Attempt to authenticate (using automated tools if necessary) many times

	using the wrong authenticator output, followed by an attempt with the correct value. The test fails if the authentication attempt succeeds.

OTP-14	**REQUIREMENT**: If the authenticator is multi-factor, then each use of the authenticator SHALL require the input of the additional factor. (5.1.5.1) **SUPPLEMENTAL GUIDANCE**: To ensure that a multi-factor authenticator cannot be stolen and used repeatedly following activation, a separate activation is required for each use of the authenticator. It is preferable for a multi-factor authenticator not to indicate that the wrong memorized secret or biometric were presented, but rather to produce an authenticator output that is invalid, although this is not required. This provides protection against guessing or presentation attacks on the authenticator itself. **ASSESSMENT OBJECTIVE:** Ensure that multi-factor authenticators require entry of an additional factor each time they are used. **POTENTIAL ASSESSMENT METHODS AND OBJECTS**: **Test**: Determine that presentation of a valid memorized secret or biometric is required to obtain each valid authenticator output.

OTP-15	**REQUIREMENT**: If the authenticator is multi-factor and a memorized secret is used by the authenticator for activation, then that memorized secret SHALL be a randomly-chosen numeric secret at least 6 decimal digits in length or other memorized secret meeting the requirements of Section 5.1.1.2. (5.1.5.1) **SUPPLEMENTAL GUIDANCE**: The requirement for memorized secrets used as activation factors is the same as that for memorized secrets used as distinct authenticators (see MS-*). **ASSESSMENT OBJECTIVE:** Determine if minimum memorized secret complexity is enforced. **POTENTIAL ASSESSMENT METHODS AND OBJECTS**: **Examine**: documentation to determine the requirements placed on memorized secrets used as activation factors. **Test:** Attempt to set a memorized secret that does not meet MS-* requirements and determine that it is not accepted.

OTP-16	**REQUIREMENT**: If the authenticator is multi-factor, then use of a memorized secret for activation SHALL be rate limited as specified in Section 5.2.2. (5.1.5.1)

	SUPPLEMENTAL GUIDANCE: Rate limiting is required to provide protection against brute-force guessing attacks, particularly if the authenticator gives an indication when an incorrect secret is entered. **ASSESSMENT OBJECTIVE:** Determine that the authenticator applies rate limiting to a memorized secret authentication factor. **POTENTIAL ASSESSMENT METHODS AND OBJECTS**: **Test**: Make repeated attempts to authenticate with the wrong memorized secret and determine that it is not possible to successfully authenticate immediately following a large number of incorrect attempts.

OTP-17	**REQUIREMENT**: If the authenticator is multi-factor and is activated by a biometric factor, then that factor SHALL meet the requirements of Section 5.2.3, including limits on the number of consecutive authentication failures. (5.1.5.1) **SUPPLEMENTAL GUIDANCE**: General requirements for biometric activation factors include false accept rate criteria and the number of consecutive authentication failures that are allowed. **ASSESSMENT OBJECTIVE:** Ensure that the biometric sensor and algorithms meet performance requirements. **POTENTIAL ASSESSMENT METHODS AND OBJECTS**: **Evaluate**: Determine that criteria BIO-* are met.

OTP-18	**REQUIREMENT**: 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 — SHALL be zeroized immediately after an OTP has been generated. (5.1.5.1) **SUPPLEMENTAL GUIDANCE**: It is important that the unencrypted key and associated data be zeroized to minimize the likelihood that it can be misappropriated by an attacker following a successful authentication. Each authentication requires a re-presentation of the activation factor (see OTP-14). Verifiers are expected to make their best effort at determining that bring-your-own authenticators not issued by them meet this requirement and to have policies not allowing the use of non-compliant authenticators. **ASSESSMENT OBJECTIVE:** Ensure that the activation factor and unencrypted key are securely discarded following each activation. **POTENTIAL ASSESSMENT METHODS AND OBJECTS**: **Examine**: Documentation and/or design documents for the authenticator to determine that it zeroes out the activation factor following each authentication.

OTP-19	**REQUIREMENT**: If the authenticator is multi-factor, the verifier or CSP SHALL establish, via the authenticator source, that the authenticator is a multi-factor device. (5.1.5.2) **SUPPLEMENTAL GUIDANCE**: From the standpoint of a verifier, a multi-factor OTP authenticator appears the same as a single-factor OTP authenticator. In order to establish that the authenticator meets the multi-factor requirements, the verifier or CSP can issue the authenticator, examine it in some way, or rely on an assertion from the manufacturer. **ASSESSMENT OBJECTIVE:** Determine that only multi-factor authenticators meeting these requirements are used as multi-factor. **POTENTIAL ASSESSMENT METHODS AND OBJECTS**: **Examine**: Procurement specifications for authenticators issued by the CSP or verifier or procedures for establishing that other multi-factor authenticators meet these requirements.

OTP-20	**REQUIREMENT**: In the absence of a trusted statement that it is a multi-factor device, the verifier SHALL treat the authenticator as single-factor, in accordance with Section 5.1.4. (5.1.5.2) **SUPPLEMENTAL GUIDANCE**: Authenticators of unknown provenance or that are not known by the CSP or verifier to meet all of the requirements for multi-factor OTP authenticators can be used, but only as single-factor authenticators. **ASSESSMENT OBJECTIVE:** Determine that unknown multi-factor authenticators and those not meeting these requirements are usable only as single-factor authenticators. **POTENTIAL ASSESSMENT METHODS AND OBJECTS**: **Examine**: Procedures for binding OTP authenticators to subscriber accounts to determine that only authenticators meeting relevant requirements are treated as multi-factor.

4.5 Cryptographic Verifiers

CRYP-1	**REQUIREMENT**: If the cryptographic authenticator is software based, the key SHALL be stored in suitably secure storage available to the authenticator application. (5.1.6.1, 5.1.8.1) **SUPPLEMENTAL GUIDANCE**: Although dependent on the computing device on which the authenticator is operating, authenticator software needs to avail itself of the most secure storage available, considering issues like ability to

	extract the secret from the device and its potential to be included in backup data. Verifiers are expected to make their best effort at determining that bring-your-own authenticators not issued by them meet this requirement and to have policies not allowing the use of non-compliant authenticators. **ASSESSMENT OBJECTIVE:** Ensure that the authenticator is storing secret keys appropriately. **POTENTIAL ASSESSMENT METHODS AND OBJECTS**: **Examine**: Documentation describing how secret keys are stored and their inclusion in backup data.

CRYP-2	**REQUIREMENT**: If the cryptographic authenticator is software based, the key SHALL be 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. (5.1.6.1, 5.1.8.1) **SUPPLEMENTAL GUIDANCE**: Although dependent on the computing device on which the authenticator is operating, authenticator software needs to store secret keys in a manner that limits access to keys to the maximum extent possible so that they cannot be accessed by other (possibly rogue) applications and/or users. Verifiers are expected to make their best effort at determining that bring-your-own authenticators not issued by them meet this requirement and to have policies not allowing the use of non-compliant authenticators. **ASSESSMENT OBJECTIVE:** Ensure that the authenticator is storing secret keys appropriately. **POTENTIAL ASSESSMENT METHODS AND OBJECTS**: **Examine**: Documentation describing how secret keys are stored access controls on the keys.

CRYP-3	**REQUIREMENT**: If the cryptographic authenticator is software based, it SHALL NOT facilitate the cloning of the secret key onto multiple devices. (5.1.6.1, 5.1.8.1) **SUPPLEMENTAL GUIDANCE**: Like other physical authenticators, the use of cryptographic authenticators is premised upon the authenticator secret being present in a single authenticator so that it proves possession of a specific device. Mechanisms that would facilitate cloning the secret onto multiple devices include the ability to enroll more than one device with the same key and backup mechanisms, especially when software-based authenticators are used. Verifiers are expected to make their best effort at determining that bring-your-own

	authenticators not issued by them meet this requirement and to have policies not allowing the use of non-compliant authenticators. **ASSESSMENT OBJECTIVE:** Determine that the management of authenticator secrets is sufficiently secure to ensure that authenticators have unique secrets. **POTENTIAL ASSESSMENT METHODS AND OBJECTS**: **Examine**: process for provisioning secrets on authenticators when they are associated with a subscriber account to determine that unnecessary copies of the secret are not made. Examine the process for backing up the platform containing the authenticator secret to determine that there is not a mechanism to allow more than one authenticator to share the same secret.

CRYP-4	**REQUIREMENT**: If the authenticator is single-factor and hardware-based, secret keys unique to the device SHALL NOT be exportable (i.e., cannot be removed from the device). (5.1.7.1) **SUPPLEMENTAL GUIDANCE**: Cryptographic device authenticators are constructed so as not to allow the secret key to be obtained from the device. These devices are enrolled for authentication using the public cryptographic key, but the private key is never shared. This requirement addresses primarily functionality allowing the key to be exported; FIPS 140 requirements cover the resistance of the device to various forms of attack. **ASSESSMENT OBJECTIVE:** Ensure that there is no mechanism permitting the private key to be extracted from the device. **POTENTIAL ASSESSMENT METHODS AND OBJECTS**: **Examine**: sample devices and documentation to determine that there is not a mechanism allowing the private key to be extracted.

CRYP-5	**REQUIREMENT**: If the authenticator is hardware-based, the secret key and its algorithm SHALL provide at least the minimum security length specified in the latest revision of SP 800-131A (112 bits as of the date of this publication). (5.1.7.1, 5.1.9.1) **SUPPLEMENTAL GUIDANCE**: The secret key used by a cryptographic authenticator needs to be sufficiently complex to resist online and offline attacks. An attacker may have the ability to observe the authenticator output at some point during its operation; it needs to be impractical for the secret key to be derived from a set of these observations. Since verifiers and cryptographic authenticators must use the same algorithms to successfully authenticate, assessment of the verifier also assesses the authenticators that may be used.

	ASSESSMENT OBJECTIVE: Determine that the secret key is sufficiently complex. **POTENTIAL ASSESSMENT METHODS AND OBJECTS**: **Examine**: the code and/or documentation for the verifier to determine that the complexity (entropy) associated with the secret key meets the minimum requirement.

CRYP-6	**REQUIREMENT**: If the authenticator is hardware-based, the challenge nonce SHALL be at least 64 bits in length. (5.1.7.1, 5.1.9.1) **SUPPLEMENTAL GUIDANCE**: This requirement applies to hardware-based cryptographic authenticators. The challenge nonce is required to be large enough that it will not be reused during the lifetime of the authenticator in order to provide replay protection. Since verifiers and cryptographic authenticators must use the same algorithms to successfully authenticate, assessment of the nonce generated by the verifier also assesses the authenticators that may be used. **ASSESSMENT OBJECTIVE:** Determine that the nonce is sufficiently complex. **POTENTIAL ASSESSMENT METHODS AND OBJECTS**: **Examine**: the code and/or documentation for the verifier to determine that the size of the nonce meets the minimum requirement.

CRYP-7	**REQUIREMENT**: If the authenticator is hardware-based, approved cryptography SHALL be used. (5.1.7.1, 5.1.9.1) **SUPPLEMENTAL GUIDANCE**: As defined in Appendix A of SP 800-63-3, cryptography is considered approved if it is specified or adopted in a FIPS or NIST recommendation. Since verifiers and cryptographic authenticators must use the same algorithms to successfully authenticate, assessment of the verifier also assesses the authenticators that may be used. **ASSESSMENT OBJECTIVE:** Determine that only secure, well-vetted cryptographic algorithms are being used. **POTENTIAL ASSESSMENT METHODS AND OBJECTS**: **Examine**: one or both of the following: ● *documented policies or practices* to determine that only approved cryptographic algorithms can be used. ● The *system's functionality* to observe the cryptographic algorithm(s) being accepted and determine whether the algorithms are approved.

CRYP-8	**REQUIREMENT**: Cryptographic keys stored by the verifier SHALL be protected against modification. (5.1.7.2) **SUPPLEMENTAL GUIDANCE**: Protection against modification is required for all keys to ensure that an attacker can't substitute keys they control, which would permit them to authenticate successfully. This protection could be provided by operating system access controls, or through integrity checks of the stored keys with separately stored hashes. **ASSESSMENT OBJECTIVE:** Determine if keys stored in the verifier have appropriate protection against modification. **POTENTIAL ASSESSMENT METHODS AND OBJECTS**: **Examine**: code and/or documentation for the verifier to determine if protection against modification that is afforded to stored keys.

CRYP-9	**REQUIREMENT**: If symmetric keys are used, cryptographic keys stored by the verifier SHALL be protected against disclosure. (5.1.7.2) **SUPPLEMENTAL GUIDANCE**: Protection against disclosure is required for symmetric keys because their disclosure also would permit an attacker to authenticate successfully. This protection could be provided through operating system access controls. **ASSESSMENT OBJECTIVE:** Determine if symmetric keys stored in the verifier have appropriate protection against disclosure. **POTENTIAL ASSESSMENT METHODS AND OBJECTS**: **Examine**: code and/or documentation for the verifier to determine if protection against disclosure that is afforded to stored symmetric keys.

CRYP-10	**REQUIREMENT**: The challenge nonce SHALL be at least 64 bits in length (5.1.7.2) **SUPPLEMENTAL GUIDANCE**: This requirement applies to verifiers of cryptographic authentication. The challenge nonce is generated by the verifier and used by a cryptographic authenticator to compute the authenticator output. The challenge needs to be sufficiently long that it will not need to repeat during the lifetime of the authenticator, so the authenticator output, if available to an attacker, cannot be replayed. **ASSESSMENT OBJECTIVE:** Determine that a sufficiently large nonce is generated by the verifier.

	POTENTIAL ASSESSMENT METHODS AND OBJECTS: **Examine**: code and/or documentation describing the nonce used in order to determine that it is 64 bits or longer.

CRYP-11	**REQUIREMENT**: The challenge nonce SHALL either be unique over the authenticator's lifetime or statistically unique (i.e., generated using an approved random bit generator). (5.1.7.2) **SUPPLEMENTAL GUIDANCE**: The challenge nonce is generated by the verifier used by a cryptographic authenticator to compute the authenticator output. The nonce cannot repeat during the lifetime of the authenticator, so the authenticator output, if available to an attacker, cannot be replayed. This can be accomplished by either deterministic means (e.g., an algorithm choosing values guaranteed not to repeat) or statistically (random values chosen from a range giving a very low probability that the same nonce will ever be seen twice). **ASSESSMENT OBJECTIVE:** Determine that a unique nonce is generated by the verifier. **POTENTIAL ASSESSMENT METHODS AND OBJECTS**: **Examine**: code and/or documentation describing the nonce used in order to determine that it generates unique or statistically unique challenges.

CRYP-12	**REQUIREMENT**: The verification operation SHALL use approved cryptography. (5.1.7.2) **SUPPLEMENTAL GUIDANCE**: As defined in Appendix A of SP 800-63-3, cryptography is considered approved if it is specified or adopted in a FIPS or NIST recommendation. Since verifiers and cryptographic authenticators must use the same algorithms to successfully authenticate, assessment of the verifier also assesses the authenticators that may be used. **ASSESSMENT OBJECTIVE:** Determine that the verifier uses only secure, well-vetted cryptographic algorithms are being used. **POTENTIAL ASSESSMENT METHODS AND OBJECTS**: **Examine**: one or both of the following: ● *documented policies or practices* to determine that only approved cryptographic algorithms can be used. ● The *system's functionality* to observe the cryptographic algorithm(s) being accepted and determine whether the algorithms are approved.

CRYP-13	**REQUIREMENT**: If a multi-factor cryptographic software authenticator is being used, then each authentication requires the presentation of the activation factor. (5.1.8.1) **SUPPLEMENTAL GUIDANCE**: The activation factor, either a memorized secret or a biometric, is required to be presented each time an authentication operation is requested by the authenticator to ensure that an activated authenticator cannot be used by an attacker. **ASSESSMENT OBJECTIVE:** Determine that the activation factor is required for each authentication. **POTENTIAL ASSESSMENT METHODS AND OBJECTS**: **Examine**: documentation describing the process of authenticating using the cryptographic authenticator. **Test:** Perform multiple authentications and verify that the activation factor is required each time.

CRYP-14	**REQUIREMENT**: If the authenticator is multi-factor, then any memorized secret used by the authenticator for activation SHALL be a randomly-chosen numeric secret at least 6 decimal digits in length or other memorized secret meeting the requirements of Section 5.1.1.2. (5.1.8.1, 5.1.9.1) **SUPPLEMENTAL GUIDANCE**: The requirement for memorized secrets used as activation factors is the same as that for memorized secrets used as distinct authenticators (see MS-*). **ASSESSMENT OBJECTIVE:** Determine if minimum memorized secret complexity is enforced. **POTENTIAL ASSESSMENT METHODS AND OBJECTS**: **Examine**: documentation to determine the requirements placed on memorized secrets used as activation factors. **Test:** Attempt to set a memorized secret that does not meet MS-* requirements and determine that it is not accepted.

CRYP-15	**REQUIREMENT**: If the authenticator is multi-factor, then use of a memorized secret for activation SHALL be rate limited as specified in Section 5.2.2. (5.1.8.1, 5.1.9.1) **SUPPLEMENTAL GUIDANCE**: Rate limiting is required to provide protection against brute-force guessing attacks, particularly if the authenticator gives an indication when an incorrect secret is entered.

	ASSESSMENT OBJECTIVE: Determine that the authenticator applies rate limiting to a memorized secret authentication factor. **POTENTIAL ASSESSMENT METHODS AND OBJECTS**: **Test**: Make repeated attempts to authenticate with the wrong memorized secret and determine that it is not possible to successfully authenticate immediately following a large number of incorrect attempts.

CRYP-16	**REQUIREMENT**: If the authenticator is multi-factor and is activated by a biometric factor, then that factor SHALL meet the requirements of Section 5.2.3, including limits on the number of consecutive authentication failures. (5.1.8.1, 5.1.9.1) **SUPPLEMENTAL GUIDANCE**: General requirements for biometric activation factors include false accept rate criteria and the number of consecutive authentication failures that are allowed. **ASSESSMENT OBJECTIVE:** Ensure that the biometric sensor and algorithms meet performance requirements. **POTENTIAL ASSESSMENT METHODS AND OBJECTS**: **Evaluate**: Determine that criteria BIO-* are met.

CRYP-17	**REQUIREMENT**: 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 — SHALL be zeroized immediately after an authentication transaction has taken place. (5.1.8.1, 5.1.9.1) **SUPPLEMENTAL GUIDANCE**: It is important that the unencrypted key and associated data be zeroized to minimize the likelihood that it can be misappropriated by an attacker following a successful authentication. Verifiers are expected to make their best effort at determining that bring-your-own authenticators not issued by them meet this requirement and to have policies not allowing the use of non-compliant authenticators. **ASSESSMENT OBJECTIVE:** Ensure that the activation factor and unencrypted key are securely discarded following each activation. **POTENTIAL ASSESSMENT METHODS AND OBJECTS**: **Examine**: Documentation and/or design documents for the authenticator to determine that it zeroes out the activation factor following each authentication.

5 General Authentication Criteria

5.1 General requirements applicable to AAL2 and AAL3 authentication processes

GEN-1	**REQUIREMENT**: CSPs SHALL provide subscriber instructions on how to appropriately protect a physical authenticator against theft or loss. (5.2.1) **SUPPLEMENTAL GUIDANCE**: Instruction should address aspects of protecting the specific type of authenticator being used. **ASSESSMENT OBJECTIVE:** Determine that instruction was provided. **POTENTIAL ASSESSMENT METHODS AND OBJECTS**: **Examine**: briefing handouts or procedures for issuing physical authenticators to determine that the subscriber was briefed on the importance of protecting the authenticator and strategies for doing so.

GEN-2	**REQUIREMENT**: The CSP SHALL provide a mechanism to revoke or suspend the authenticator immediately upon notification from subscriber that loss or theft of the authenticator is suspected. (5.2.1) **SUPPLEMENTAL GUIDANCE**: The CSP needs to have a documented procedure to allow subscribers to report lost or stolen physical authenticators, and to revoke or suspend such authenticators promptly when reported. Subscribers need to be instructed (see GEN-1) the procedure for reporting loss or theft. **ASSESSMENT OBJECTIVE:** Determine that a reporting procedure exists. **POTENTIAL ASSESSMENT METHODS AND OBJECTS**: **Examine**: procedures for accepting and processing reports of lost or stolen physical authenticators to determine that effective procedures exist.

GEN-3	**REQUIREMENT**: If required by the authenticator type descriptions in Section 5.1, then the verifier SHALL implement controls to protect against online guessing attacks. (5.2.2) **SUPPLEMENTAL GUIDANCE**: Throttling or rate limiting is key to resistance against online guessing attacks. This is generally required for memorized secrets or when the authenticator output of a look-up secret, OOB, or OTP authenticator may have less than 64 bits of entropy. **ASSESSMENT OBJECTIVE:** Determine that rate limiting is applied when required.

	POTENTIAL ASSESSMENT METHODS AND OBJECTS: **Examine**: code or documentation to determine the existence of rate limiting applied. **Test:** Attempt to authenticate repeatedly unsuccessfully and observe that authentications are impeded when this occurs.

GEN-4	**REQUIREMENT**: If required by the authenticator type descriptions in Section 5.1 and the description of a given authenticator does not specify otherwise, then the verifier SHALL limit consecutive failed authentication attempts on a single account to no more than 100. (5.2.2) **SUPPLEMENTAL GUIDANCE**: Throttling or rate limiting is key to resistance against online guessing attacks. It is important that it be implemented in a non-abrupt manner as described in the specification so that it is not usable as a denial-of-service mechanism by an attacker. Additional techniques MAY be used to reduce the likelihood that an attacker will lock the legitimate claimant out as a result of rate limiting. These include: • Requiring the claimant to complete a CAPTCHA before attempting authentication. • Requiring the claimant to wait following a failed attempt for a period of time that increases as the account approaches its maximum allowance for consecutive failed attempts (e.g., 30 seconds up to an hour). • Accepting only authentication requests that come from a white list of IP addresses from which the subscriber has been successfully authenticated before. • Leveraging other risk-based or adaptive authentication techniques to identify user behavior that falls within, or out of, typical norms. These might, for example, include use of IP address, geolocation, timing of request patterns, or browser metadata. **ASSESSMENT OBJECTIVE:** Determine that appropriate rate limiting is applied when required **POTENTIAL ASSESSMENT METHODS AND OBJECTS**: **Examine**: code or documentation to determine the nature of rate limiting applied. **Test:** Attempt to authenticate repeatedly unsuccessfully and determine that authentications are impeded when this occurs and that it is not possible to authenticate successfully after 100 consecutive unsuccessful tries.

GEN-5	**REQUIREMENT**: If signed attestations are used, then they SHALL be signed using a digital signature that provides at least the minimum security strength

	specified in the latest revision of SP 800-131A (112 bits as of the date of this publication). (5.2.4) **SUPPLEMENTAL GUIDANCE**: Attestations are sometimes provided by cryptographic authenticators to securely indicate their capabilities, e.g., that they are hardware-based or that they have characteristics such as two-factor capability. For the attestations to be useful, these signatures need to use algorithms and keys that are sufficiently strong. **ASSESSMENT OBJECTIVE:** Determine if only attestations of sufficient strength are trusted. **POTENTIAL ASSESSMENT METHODS AND OBJECTS**: **Examine**: documentation and/or code for the verifier to determine that, if it relies upon signed attestations, the verifier only accepts attestations that are sufficiently strongly signed.

GEN-6	**REQUIREMENT**: If the verifier and CSP are separate entities (as shown by the dotted line in SP 800-63-3 Figure 4-1), then communications between the verifier and CSP SHALL occur through a mutually-authenticated secure channel (such as a client-authenticated TLS connection). (5.2.6) **SUPPLEMENTAL GUIDANCE**: In cases where the verifier and CSP are separate, it is important that this not create additional security vulnerabilities as compared with an integrated verifier/CSP combination. This requirement ensures that there is not an opportunity to perform eavesdropping or active attacks on the channel between them. **ASSESSMENT OBJECTIVE:** Determine if communication between verifier and CSP is sufficiently secure. **POTENTIAL ASSESSMENT METHODS AND OBJECTS**: **Examine**: the verifier's API documentation to determine that TLS or a similarly secure protocol is used requiring authentication of both the client and server.

GEN-7	**REQUIREMENT**: 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 SHALL be either a memorized secret or a physical authenticator. (6.2) **SUPPLEMENTAL GUIDANCE**: It is important that the loss of control of an authenticator be quickly reported to the CSP. To balance between the need to easily and promptly report this and the risk of a fraudulent report, a backup authenticator, either a memorized secret or physical authenticator, should be

	usable by the subscriber to make this report. Only a single, single-factor authenticator is required. **ASSESSMENT OBJECTIVE:** Determine if CSPs supporting backup authenticators for loss reports use appropriate authenticators for this purpose. **POTENTIAL ASSESSMENT METHODS AND OBJECTS**: **Test**: Using a test account and the backup authenticator for that account, make a lost authenticator report to the CSP and determine that the authenticator is suspended properly.

GEN-8	**REQUIREMENT**: *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 SHALL be 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. (6.2) **SUPPLEMENTAL GUIDANCE**: Reversibility of suspension is intended to minimize the impact of inadvertent loss reports from the subscriber and in some cases from an attacker who may be attempting to deny service to the subscriber. **ASSESSMENT OBJECTIVE:** Determine if suspension can be reversed by the subscriber. **POTENTIAL ASSESSMENT METHODS AND OBJECTS**: **Test**: Using a test account and an associated authenticator other than that which was reported lost, revert a loss report previously made to the CSP and determine that it the suspended authenticator is reinstated.

GEN-9	**REQUIREMENT**: If and when an authenticator expires, it SHALL NOT be usable for authentication. (6.3) **SUPPLEMENTAL GUIDANCE**: Expiration is used by some CSPs to limit the security exposure from an authenticator that is lost but the loss has not been detected/reported and revoked. **ASSESSMENT OBJECTIVE:** Determine if expired authenticators cannot be used for authentication. **POTENTIAL ASSESSMENT METHODS AND OBJECTS**: **Test**: Using an authenticator that has expired, attempt to authenticate and determine that this cannot be done successfully.

GEN-10	**REQUIREMENT**: The CSP SHALL require subscribers to surrender or prove destruction of any physical authenticator containing attribute certificates signed by the CSP as soon as practical after expiration or receipt of a renewed authenticator. (6.3) **SUPPLEMENTAL GUIDANCE**: The requirement for surrender or destruction of expired authenticators minimizes the possibility that authentication with an expired authenticator will be attempted. PKI-based authenticators that are collected or known to be destroyed also do not need to be included in certificate revocation lists. **ASSESSMENT OBJECTIVE:** Determine if expired authenticators are collected or provably destroyed. **POTENTIAL ASSESSMENT METHODS AND OBJECTS**: **Examine**: CSP procedures for handling of authenticators that expire to determine that collection and/or destruction are performed.

GEN-11	**REQUIREMENT**: CSPs SHALL revoke the binding of authenticators promptly 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. (6.4) **SUPPLEMENTAL GUIDANCE**: Prompt revocation ensures that unauthorized parties are not able to use the authenticator to make unauthorized access to the subscriber account. Revocation at subscriber request can affect only a single authenticator; the other classes of revocation generally affect all authenticators associated with the subscriber's account. **ASSESSMENT OBJECTIVE:** Determine if procedures exist to properly revoke authenticators upon request from the subscriber, when an account ceases to exist, or when the subscriber is no longer eligible **POTENTIAL ASSESSMENT METHODS AND OBJECTS**: **Examine**: CSP procedures for revocation of authenticators to ensure that it is properly completed for all reasons for revocation.

GEN-12	**REQUIREMENT**: The CSP SHALL require subscribers to surrender or certify destruction of any physical authenticator containing certified attributes signed by the CSP as soon as practical after revocation or termination takes place. (6.4) **SUPPLEMENTAL GUIDANCE**: This requirement blocks the use of the authenticator's certified attributes in offline situations between revocation/termination and expiration of the certification. Prompt revocation ensures that unauthorized parties are not able to use the authenticator to make

	unauthorized access to the subscriber account. Collection or destruction also minimizes the dependence on (and growth of) certificate revocation lists, which are not always 100% effective in accomplishing revocation, particularly in offline situations. **ASSESSMENT OBJECTIVE:** Determine if revoked authenticators containing certified attributes is collected or destroyed promptly. **POTENTIAL ASSESSMENT METHODS AND OBJECTS**: **Examine**: CSP procedures for handling of revoked authenticators to determine that authenticators containing certified attributes are collected or their destruction is conformed.

5.2 Use of Biometrics

BIO-1	**REQUIREMENT**: Biometrics SHALL be used only as part of multi-factor authentication with a physical authenticator (*something you have*). (5.2.3) **SUPPLEMENTAL GUIDANCE**: For a variety of reasons outlined in Section 5.2.3, a biometric factor is not considered to be an authenticator by itself. The risks associated with biometric factors are largely mitigated by binding the biometric with a specific physical authenticator. **ASSESSMENT OBJECTIVE:** Determine if all use of biometrics for authentication is in conjunction with a physical authenticator. **POTENTIAL ASSESSMENT METHODS AND OBJECTS**: **Examine**: Documentation describing all authentication flows supported by the verifier and determine that all use of a biometric factor is in conjunction with a physical authenticator.

BIO-2	**REQUIREMENT**: An authenticated protected channel between sensor (or an endpoint containing a sensor that resists sensor replacement) and verifier SHALL be established. (5.2.3) **SUPPLEMENTAL GUIDANCE**: This requirement ensures that biometric data that flows across the network to the verifier is protected from disclosure and that an attacker cannot substitute a "skimmer" or other fraudulent replacement for the biometric sensor. If the biometric factor is verified directly on a multi-factor authenticator and the sensor is tightly integrated with it, that local connection does not require an authenticated protected channel. **ASSESSMENT OBJECTIVE:** Determine that appropriate sensor security measures are in place.

	POTENTIAL ASSESSMENT METHODS AND OBJECTS: **Examine**: Documentation describing the communication protocol used between sensors and verifiers.

BIO-3	**REQUIREMENT**: The sensor or endpoint SHALL be authenticated prior to capturing the biometric sample from the claimant. (5.2.3) **SUPPLEMENTAL GUIDANCE**: This requirement ensures that the biometric data being verified is obtained from the expected sensor rather than from a device that may be spoofing biometric information. This is generally not required when the biometric factor is verified in an endpoint that is tightly integrated with the sensor in a manner that resists sensor replacement. **ASSESSMENT OBJECTIVE:** Determine that the intended sensor is used to collect the biometric factor. **POTENTIAL ASSESSMENT METHODS AND OBJECTS**: **Examine**: Documentation describing integration of the sensor and endpoint or the method of authenticating the sensor.

BIO-4	**REQUIREMENT**: The biometric system SHALL operate with an FMR [ISO/IEC 2382-37] of 1 in 1000 or better. This FMR SHALL be achieved under conditions of a conformant attack (i.e., zero-effort impostor attempt) as defined in [ISO/IEC 30107-1]. (5.2.3) **SUPPLEMENTAL GUIDANCE**: Since biometric comparison is an approximate match, an operating point threshold is chosen by the verifier that balances false matches and false non-matches. To operate adequately as a verifier, a 1 in 1000 or better false match rate is required. **ASSESSMENT OBJECTIVE:** Determine if the false match rate criterion is met by the biometric system. **POTENTIAL ASSESSMENT METHODS AND OBJECTS**: **Examine**: Testing results to determine that a better than 1 in 1000 false match rate Is achieved by the biometric system.

BIO-5	**REQUIREMENT**: The biometric system SHALL allow no more than 5 consecutive failed authentication attempts or 10 consecutive failed attempts if PAD demonstrating at least 90% resistance to presentation attacks is implemented. (5.2.3) **SUPPLEMENTAL GUIDANCE**: With a false accept rate of as much as 1 in 1000 zero-effort attempts, the ability to make a large number of biometric

	authentication attempts would result in an unacceptably high probability of mis-authentication. This limit is comparable to that provided by several commercial products (mobile devices) currently on the market. **ASSESSMENT OBJECTIVE:** Determine if the limit on consecutive failed attempts is enforced. **POTENTIAL ASSESSMENT METHODS AND OBJECTS**: **Test**: Attempt to authenticate several times with an invalid biometric (e.g., wrong fingerprint) and determine that that an alternate factor is requested or delays are imposed after the appropriate number of consecutive failures.

BIO-6	**REQUIREMENT**: Once the limit on authentication failures has been reached, the biometric authenticator SHALL either: (1) Impose a delay of at least 30 seconds before the next attempt, increasing exponentially with each successive attempt, or (2) disable the biometric user authentication and offer another factor (e.g., a different biometric modality or a PIN/Passcode if it is not already a required factor) if such an alternative method is already available. (5.2.3) **SUPPLEMENTAL GUIDANCE**: Following a number of consecutive biometric match failures that exceeds the limit in BIO-5, subsequent attempts need to be either aggressively delayed (e.g., 1 minute before the following failed attempt, 2 minutes before the second following attempt) or another authentication or biometric modality associated with the same physical authenticator needs to be used. **ASSESSMENT OBJECTIVE:** Determine if the response to excessive consecutive failed attempts is performed correctly. **POTENTIAL ASSESSMENT METHODS AND OBJECTS**: **Test**: Attempt to authenticate several times with an invalid biometric (e.g., wrong fingerprint) and determine that that an alternate factor is requested or delays are imposed after the appropriate number of consecutive failures.

BIO-7	**REQUIREMENT**: The verifier SHALL make a determination of sensor and endpoint performance, integrity, and authenticity. (5.2.3) **SUPPLEMENTAL GUIDANCE**: The verifier needs to have a basis for determining that biometric verification meets the necessary performance requirements. This may be accomplished by authenticating the sensor or endpoint, by a certification by an approved accreditation authority, or by runtime interrogation of a signed attestation. **ASSESSMENT OBJECTIVE:** Determine if the verifier allows only properly vetted sensors and endpoints.

	POTENTIAL ASSESSMENT METHODS AND OBJECTS: **Examine**: documentation to establish that the verifier determines that the sensor and endpoint are required to meet the necessary performance requirements.

BIO-8	**REQUIREMENT**: If biometric comparison is performed centrally, then use of the biometric as an authentication factor SHALL be limited to one or more specific devices that are identified using approved cryptography. (5.2.3) **SUPPLEMENTAL GUIDANCE**: The ability to use a biometric factor on an arbitrary device greatly increases the value of breached biometric data. For this reason, the use of the biometric factor is limited to specific devices for each subscriber. A separate key is required since the main authentication key is only unlocked upon successful comparison of the biometric factor. **ASSESSMENT OBJECTIVE:** Determine if the biometric factor can only be used from specific devices. **POTENTIAL ASSESSMENT METHODS AND OBJECTS**: **Examine**: design documentation and user interface flows to determine how the endpoint is authenticated in conjunction with the use of the biometric, the manner in which the biometric factor is individually associated with each device to be used, and that the necessary authentication is accomplished using approved cryptography as defined in Appendix A of SP 800-63-3..

BIO-9	**REQUIREMENT**: If biometric comparison is performed centrally, then a separate key SHALL be used for identifying the device. (5.2.3) **SUPPLEMENTAL GUIDANCE**: Since the main authentication key has not yet been unlocked, a separate key is required for identifying the specific device(s) that the biometric may be used with. **ASSESSMENT OBJECTIVE:** Determine if a separate key is used for authenticating the device for use of the biometric factor. **POTENTIAL ASSESSMENT METHODS AND OBJECTS**: **Examine**: design documentation to determine whether a separate key exists and is used for purposes of authorizing the use of the biometric.

BIO-10	**REQUIREMENT**: If biometric comparison is performed centrally, then biometric revocation, referred to as biometric template protection in ISO/IEC 24745, SHALL be implemented. (5.2.3)

	SUPPLEMENTAL GUIDANCE: Central databases of biometric templates are an attractive target for attackers. The ability to securely revoke biometric factors is required in response to that threat. **ASSESSMENT OBJECTIVE:** Determine if biometric revocation is implemented. **POTENTIAL ASSESSMENT METHODS AND OBJECTS**: **Examine**: operating procedures to determine that a procedure exists for revoking a biometric factor that has been breached.

BIO-11	**REQUIREMENT**: If biometric comparison is performed centrally, all transmission of biometrics SHALL be over the authenticated protected channel. (5.2.3) **SUPPLEMENTAL GUIDANCE**: Because of the replay potential of biometric data, biometric information needs to be distributed in a manner that minimizes the opportunity for attackers to intercept the data either by eavesdropping on man-in-the-middle attacks. **ASSESSMENT OBJECTIVE:** Determine if an authenticated protected channel is used for transmitting biometric data. **POTENTIAL ASSESSMENT METHODS AND OBJECTS**: **Examine**: documentation and code to determine that an authenticated protected channel is used. **Test:** Observe communication traffic to see that an authenticated protected channel is established for this purpose.

BIO-12	**REQUIREMENT**: Biometric samples and any biometric data derived from the biometric sample such as a probe produced through signal processing SHALL be zeroized immediately after any training or research data has been derived (5.2.3) **SUPPLEMENTAL GUIDANCE**: If the biometric factor is used for any supplemental purpose, it is important that it not be a mechanism for breach of subscribers' biometric data. **ASSESSMENT OBJECTIVE:** Determine if data is zeroized as required. **POTENTIAL ASSESSMENT METHODS AND OBJECTS**: **Examine**: procedures for research and training use of biometric data and determine that the biometric data is securely cleared at the earliest possible opportunity.

5.3 Verifier Impersonation Resistance

VIR-1	**REQUIREMENT**: A verifier impersonation-resistant authentication protocol SHALL establish an authenticated protected channel with the verifier. (5.2.5) **SUPPLEMENTAL GUIDANCE**: The establishment of an authenticated protected channel is particularly important when implementing verifier impersonation resistance because it will be necessary to bind information about the channel together with the authenticator output (see VIR-2 below). **ASSESSMENT OBJECTIVE:** Determine if an authenticated protected channel is used for verifier impersonation resistant authentication. **POTENTIAL ASSESSMENT METHODS AND OBJECTS**: **Examine**: documentation and code to determine that an authenticated protected channel is used for verifier impersonation resistant authentication protocols. **Test:** Observe communication traffic to determine that an authenticated protected channel is established for this purpose.

VIR-2	**REQUIREMENT**: A verifier impersonation resistant protocol SHALL strongly and irreversibly bind a channel identifier that was negotiated in establishing the authenticated protected channel to the authenticator output. (5.2.5) **SUPPLEMENTAL GUIDANCE**: The binding of a channel identifier negotiated in the establishment of an authenticated protected channel to the authenticator output has the effect of providing strong man-in-the-middle protection, even against attackers that possess a trusted certificate for the verifier. One way to establish this binding is by signing the channel identifier using a private key controlled by the claimant for which the public key is known to the verifier. Client-authenticated TLS is an example of a cryptographic authentication protocol that meets this requirement. **ASSESSMENT OBJECTIVE:** Determine if the authentication meets requirements for verifying binding of the channel to the authentication transaction. **POTENTIAL ASSESSMENT METHODS AND OBJECTS**: **Examine**: communication protocols to determine the manner which the channel identifier is used in the calculation and verification of the authenticator output.

VIR-3	**REQUIREMENT**: The verifier SHALL validate the signature or other information used to prove verifier impersonation resistance. (5.2.5) **SUPPLEMENTAL GUIDANCE**: In order to prove verifier impersonation resistance, it is necessary for the verifier to validate the binding established in VIR-2 to determine that the channel identifier, as seen by the verifier, is the same as that bound to the authentication transaction by the claimant. **ASSESSMENT OBJECTIVE:** Determine if the verifier impersonation resistance requirement has been satisfied. **POTENTIAL ASSESSMENT METHODS AND OBJECTS**: **Examine**: documentation or code to determine that the authentication only succeeds if verifier impersonation resistance is satisfied (i.e., that the same channel identifier is seen by both parties).

VIR-4	**REQUIREMENT**: Approved cryptographic algorithms SHALL be used to establish verifier impersonation resistance where it is required. (5.2.5) **SUPPLEMENTAL GUIDANCE**: As defined in Appendix A of SP 800-63-3, cryptography is considered approved if it is specified or adopted in a FIPS or NIST recommendation. **ASSESSMENT OBJECTIVE:** Determine if only secure, well-vetted cryptographic algorithms are being used. **POTENTIAL ASSESSMENT METHODS AND OBJECTS**: **Examine**: one or both of the following: ● *documented policies or practices* to determine that only approved cryptographic algorithms can be used. ● the *system's functionality* to observe the cryptographic algorithm(s) being accepted.

VIR-5	**REQUIREMENT**: Keys used for this purpose SHALL provide at least the minimum security strength specified in the latest revision of SP 800-131A (112 bits as of the date of this publication. (5.2.5) **SUPPLEMENTAL GUIDANCE**: The key used to establish verifier impersonation resistance needs to be sufficiently complex to resist online and offline attacks. **ASSESSMENT OBJECTIVE:** Determine if the key used to bind the channel identifier is sufficiently complex.

	POTENTIAL ASSESSMENT METHODS AND OBJECTS: **Examine**: the code and/or documentation for the verifier to determine the complexity (entropy) associated with the secret key.

VIR-6	**REQUIREMENT**: Authenticators that involve the manual entry of an authenticator output, such as out-of-band and OTP authenticators, SHALL NOT be considered verifier impersonation-resistant because the manual entry does not bind the authenticator output to the specific session being authenticated. (5.2.5) **SUPPLEMENTAL GUIDANCE**: Authenticators that do not have an opportunity to create a binding with the communication channel cannot be verifier impersonation resistant. Verifier impersonation resistance is required for at least one authenticator used for AAL3 authentication; verifier impersonation resistance is recommended but not required for AAL2. **ASSESSMENT OBJECTIVE:** Determine if only cryptographic authenticators are considered verifier impersonation resistant. **POTENTIAL ASSESSMENT METHODS AND OBJECTS**: **Examine**: Types of authenticators accepted by the verifier to determine that only cryptographic authenticators are considered verifier impersonation resistant (see requirement AAL3-6).

6 Authenticator Lifecycle Management Criteria

6.1 Authenticator Binding

BIND-1	**REQUIREMENT**: Authenticators SHALL be bound to subscriber accounts by either issuance by the CSP as part of enrollment or associating a subscriber-provided authenticator that is acceptable to the CSP. (6.1) **SUPPLEMENTAL GUIDANCE**: In the past, many physical authenticators were provided by the CSP. More recently, there has been a trend toward *BYO authenticators*, which can be both cost-effective for CSPs and convenient for the subscriber. This requirement ensures that such BYO authenticators are subject to approval by the CSP, primarily to ensure that they meet security requirements. **ASSESSMENT OBJECTIVE:** Determine if the CSP has approval authority for BYO authenticators. **POTENTIAL ASSESSMENT METHODS AND OBJECTS**: **Examine**: authenticators accepted by the verifier to determine that the CSP can determine the characteristics of authenticators they accept and can reject those not meeting their security requirements.

BIND-2	**REQUIREMENT**: Throughout the digital identity lifecycle, CSPs SHALL maintain a record of all authenticators that are or have been associated with each identity. (6.1) **SUPPLEMENTAL GUIDANCE**: In order to authenticate subscribers successfully, the CSP needs to maintain a record of authenticators bound to each subscriber's account. In addition, a record of authenticators formerly bound to each account needs to be kept for forensic purposes. **ASSESSMENT OBJECTIVE:** Determine if the CSP maintains the necessary records. **POTENTIAL ASSESSMENT METHODS AND OBJECTS**: **Examine**: records maintained by the CSP to determine that the necessary information is included.

BIND-3	**REQUIREMENT**: The CSP or verifier SHALL maintain the information required for throttling authentication attempts when required. (6.1) **SUPPLEMENTAL GUIDANCE**: In order to successfully support the throttling of authentication attempts (see section 5.2.2 and requirement GEN-3), the CSP needs to maintain information on the number of consecutive failed authentication attempts.

	ASSESSMENT OBJECTIVE: Determine if the CSP maintains the necessary records. **POTENTIAL ASSESSMENT METHODS AND OBJECTS**: **Examine**: records maintained by the CSP to determine that the necessary information is included.

BIND-4	**REQUIREMENT**: The CSP SHALL also verify the type of user-provided authenticator so verifiers can determine compliance with requirements at each AAL. (6.1) **SUPPLEMENTAL GUIDANCE**: In order to determine compliance with AAL-specific requirements, the CSP needs to reliably determine some authenticator characteristics, such as whether the authenticator is hardware-based, whether it is a single-factor or multi-factor authenticator, and performance characteristics of associated biometric sensors. Mechanisms to do this include attestation certificates from the manufacturer and examination of the authenticator (particularly at account issuance). In the absence of this information, the CSP needs to assume that the authenticator is the weakest type that is consistent with the authentication protocol being used. **ASSESSMENT OBJECTIVE:** Determine if the CSP verifies authenticator types and uses that information when determining the AAL. **POTENTIAL ASSESSMENT METHODS AND OBJECTS**: **Examine**: procedures used and records maintained by the CSP to determine that the authenticator characteristics are determined, recorded, and used in AAL decisions.

BIND-5	**REQUIREMENT**: The record created by the CSP SHALL contain the date and time the authenticator was bound to the account. (6.1) **SUPPLEMENTAL GUIDANCE**: For forensic purposes it is useful to have a record of the period of time each authenticator is bound to the subscriber's account. **ASSESSMENT OBJECTIVE:** Determine if the CSP maintains the necessary records. **POTENTIAL ASSESSMENT METHODS AND OBJECTS**: **Examine**: records maintained by the CSP to determine that the necessary information is included.

BIND-6	**REQUIREMENT**: When any new authenticator is bound to a subscriber account, the CSP SHALL ensure that the binding protocol and the protocol for

	provisioning the associated key(s) are done at a level of security commensurate with the AAL at which the authenticator will be used. (6.1) **SUPPLEMENTAL GUIDANCE**: If the process of binding an authenticator is not strong enough, an authenticator that is fraudulently bound to the account could be used by an attacker to gain access to a subscriber's account. The authentication factor being bound to the account needs to be included in the authentication process for the session in which the authenticator is bound. **ASSESSMENT OBJECTIVE:** Determine if the CSP uses protocols and procedures that are sufficiently strong. **POTENTIAL ASSESSMENT METHODS AND OBJECTS**: **Examine**: procedures used by the CSP to determine that they are of comparable strength to the authentication processes themselves. See also BIND-8.

BIND-7	**REQUIREMENT**: Protocols for key provisioning SHALL use authenticated protected channels or be performed in person to protect against man-in-the-middle attacks. (6.1) **SUPPLEMENTAL GUIDANCE**: For the same reasons that man-in-the-middle attacks are of concern during authentication, they could occur during provisioning, which could result in the binding of an attacker's key to the account rather than the subscriber's key. **ASSESSMENT OBJECTIVE:** Determine if the CSP uses protocols that are resistant to man-in-the-middle attacks. **POTENTIAL ASSESSMENT METHODS AND OBJECTS**: **Examine**: documentation describing the protocols used in provisioning keys and other binding operations to ensure that an authenticated protected channel using a protocol such as TLS is used, or that the operation is performed in person.

BIND-8	**REQUIREMENT**: Binding of multi-factor authenticators SHALL require multi-factor authentication (or equivalent at identity proofing). (6.1) **SUPPLEMENTAL GUIDANCE**: In order to prevent a subscriber with only single-factor authentication from up-leveling to multi-factor, binding of a multi-factor authenticator requires that the subscriber be multi-factor authenticated at the time the new authenticator is bound **ASSESSMENT OBJECTIVE:** Determine that the CSP requires appropriate authentication prior to multi-factor authenticator binding. **POTENTIAL ASSESSMENT METHODS AND OBJECTS**: **Examine**: documentation describing the process for binding a new multi-factor

	authenticator to determine that multi-factor authentication or equivalent is required. **Test**: Attempt to bind a multi-factor authenticator while authenticated with only one factor; the assessment fails if this is possible.

BIND-9	**REQUIREMENT**: At enrollment, the CSP SHALL bind 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. (6.1.1) **SUPPLEMENTAL GUIDANCE**: Executive order 13681 requires the use of multi-factor authentication for the release of personal data. Therefore, it is important that the CSP associate sufficient authentication factors at enrollment to make this possible. **ASSESSMENT OBJECTIVE:** Determine if the CSP associates sufficient authentication factors at enrollment. **POTENTIAL ASSESSMENT METHODS AND OBJECTS**: **Examine**: documentation describing the binding of authenticators at enrollment by the CSP to determine that the procedures require sufficient authenticators to be bound to new subscriber accounts.

BIND-10	**REQUIREMENT**: At enrollment, authenticators at the same AAL as the desired IAL SHALL be bound to the account. (6.1.1) **SUPPLEMENTAL GUIDANCE**: In order to support higher identity assurance, correspondingly high authenticator assurance levels are required to ensure the proper use of the identity. **ASSESSMENT OBJECTIVE:** Determine if at enrollment the CSP associates authenticators sufficient to support the effective use of the desired identity assurance level. **POTENTIAL ASSESSMENT METHODS AND OBJECTS**: **Examine**: documentation describing the binding of authenticators at enrollment by the CSP to determine that authenticators appropriate to the IAL are bound to the account.

BIND-11	**REQUIREMENT**: If the subscriber is authenticated at AAL1, then the CSP SHALL NOT expose personal information, even if self-asserted, to the subscriber. (6.1.1)

	SUPPLEMENTAL GUIDANCE: Executive Order 13681 requires the use of multi-factor authentication for the release of personal information. It does not limit this to personal information coming from an official source. **ASSESSMENT OBJECTIVE:** Determine if the CSP does not support authentication at AAL1 or provides very limited capability to subscribers authenticated at that AAL. **POTENTIAL ASSESSMENT METHODS AND OBJECTS**: **Test**: Authenticate at AAL1 and determine that personal information is not released to either the subscriber or to a relying party.

BIND-12	**REQUIREMENT**: If enrollment and binding are being done remotely and cannot be completed in a single electronic transaction, then the applicant SHALL identify 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. (6.1.1) **SUPPLEMENTAL GUIDANCE**: The issuance or binding of authenticators may occur well after the enrollment process, following adjudication and eligibility determinations. It is necessary to securely associate the applicant that appears for identity proofing with the person appearing for authenticator issuance/binding in order to avoid mis-issuance of authenticators. At this point it is not possible to fully authenticate the applicant, but the use of a temporary secret provides the necessary protection for this one-time transaction. **ASSESSMENT OBJECTIVE:** Determine if the CSP has procedures in place to securely associate authenticator binding with enrollment. **POTENTIAL ASSESSMENT METHODS AND OBJECTS**: **Observe**: If binding and enrollment take place in separate sessions, determine that CSP procedures include the issuance of a unique temporary secret that the applicant presents in order to perform authenticator binding.

BIND-13	**REQUIREMENT**: 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. (6.1.1) **SUPPLEMENTAL GUIDANCE**: Long-term secrets need to be protected against disclosure while they are sent to the applicant. This applies primarily to symmetric keys, such as for OTP authenticators, that are sent to the applicant by the CSP. "Protected session" in this context refers to an authenticated protected channel as defined in SP 800-63-3 Appendix A,

	ASSESSMENT OBJECTIVE: Determine if the CSP adequately protects the secrets being exchanged while performing remote binding of authenticators. **POTENTIAL ASSESSMENT METHODS AND OBJECTS**: **Examine**: the verifier's API documentation to ensure that TLS or a similarly secure protocol is used.

BIND-14	**REQUIREMENT**: If enrollment and binding are being done in person and cannot be completed in a single physical encounter, the applicant SHALL identify themselves in person by either using a secret as described in BIND-12 above, or through use of a biometric that was recorded during a prior encounter. (6.1.1) **SUPPLEMENTAL GUIDANCE**: The issuance or binding of authenticators may occur well after the enrollment process, following adjudication and eligibility determinations. It is necessary to securely associate the applicant that appears for identity proofing with the person appearing for authenticator issuance/binding in order to avoid mis-issuance of authenticators. At this point it is not possible to fully authenticate the applicant, but the use of a temporary secret provides the necessary protection for this one-time transaction. **ASSESSMENT OBJECTIVE:** Determine if the CSP has procedures in place to securely associate authenticator binding with enrollment. **POTENTIAL ASSESSMENT METHODS AND OBJECTS**: **Examine**: If binding and enrollment take place in separate sessions, determine that CSP procedures include the issuance of a unique temporary secret that the applicant presents in order to perform authenticator binding, or by biometric comparison with a biometric recorded during a previous encounter.

BIND-15	**REQUIREMENT**: If enrollment and binding are being done in person and cannot be completed in a single physical encounter, temporary secrets SHALL NOT be reused. (6.1.1) **SUPPLEMENTAL GUIDANCE**: The issuance or binding of authenticators may occur well after the enrollment process, following adjudication and eligibility determinations. It is necessary to securely associate the applicant that appears for identity proofing with the person appearing for authenticator issuance/binding in order to avoid mis-issuance of authenticators. A new secret for this purpose is required for each subsequent encounter. **ASSESSMENT OBJECTIVE:** Determine if the CSP issues new temporary secrets for each subsequent encounter. **POTENTIAL ASSESSMENT METHODS AND OBJECTS**: **Examine**: If binding and enrollment take place in separate in-person sessions,

	determine that CSP procedures include the issuance of a new unique temporary secret for each subsequent interaction.

BIND-16	**REQUIREMENT**: 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 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. (6.1.1) **SUPPLEMENTAL GUIDANCE**: To avoid misappropriation of long-term authenticator secrets at enrollment, the CSP is required to load the secrets onto authenticators directly, or deliver them to the new subscriber in a manner that confirms the address of record, typically by sending a short-term secret to that address that the new subscriber uses to obtain the long-term secret **ASSESSMENT OBJECTIVE:** Determine if the CSP has procedures in place to securely deliver long-term authenticator secrets to new subscribers. **POTENTIAL ASSESSMENT METHODS AND OBJECTS**: **Examine**: If binding and enrollment take place in separate in-person sessions, determine that CSP procedures call for the loading of authenticator secrets locally onto a physical device that is issued in person to the applicant, or by sending a short-term secret to the applicant (new subscriber).

BIND-17	**REQUIREMENT**: Before adding a new authenticator to a subscriber's account, the CSP SHALL first require the subscriber to authenticate at the AAL (or a higher AAL) at which the new authenticator will be used. (6.1.2.1) **SUPPLEMENTAL GUIDANCE**: In order to maintain the significance of AALs and prevent attackers from leveraging lower AAL authentication to gain access to higher AAL resources, subscribers binding additional authenticators need to do so at the maximum AAL at which they will be used. **ASSESSMENT OBJECTIVE:** Determine if the CSP observes proper procedures for binding additional authenticators. **POTENTIAL ASSESSMENT METHODS AND OBJECTS**: **Observe**: Determine that the binding process for additional authenticators requires the subscriber to authenticate at the maximum AAL at which the new authenticator will be used.

BIND-18	**REQUIREMENT**: If the subscriber's account has only one authentication factor bound to it, the CSP SHALL require the subscriber to authenticate at

	AAL1 in order to bind an additional authenticator of a different authentication factor. (6.1.2.2) **SUPPLEMENTAL GUIDANCE**: This is a special-case, one-time only exception to BIND-17 to allow a single-factor account not subject to identity proofing (IAL1) to be upgraded to a multi-factor account. This provides a mechanism for such accounts to increase their authentication security. **ASSESSMENT OBJECTIVE:** Determine if the CSP, when upgrading single-factor accounts, does so in the most secure manner available. **POTENTIAL ASSESSMENT METHODS AND OBJECTS**: **Test**: Establish a single-factor account and attempt to add an additional authenticator of a different factor to it and determine that it requires user authentication.

BIND-19	**REQUIREMENT**: If a subscriber loses all authenticators of a factor necessary to complete multi-factor authentication and has been identity proofed at IAL2 or IAL3, that subscriber SHALL repeat the identity proofing process described in SP 800-63A. (6.1.2.3) **SUPPLEMENTAL GUIDANCE**: Repeating the identity proofing process is an onerous requirement when a subscriber is no longer able to complete multi-factor authentication, but it is necessary to avoid the security problems typically present in "account recovery" situations. This is the primary reason that the binding of multiple authenticators is recommended, particularly in the case of physical authenticators. The entire identity proofing process need not be repeated if the CSP has maintained enough records of the evidence presented to repeat the verification phase of identity proofing. **ASSESSMENT OBJECTIVE:** Determine if the CSP, when replacing a lost authentication factor, repeats the relevant portions of the identity proofing process. **POTENTIAL ASSESSMENT METHODS AND OBJECTS**: **Test**: Establish a multi-factor account and simulate the loss of an authentication factor (either a physical authenticator or a memorized secret). Observe the account-recovery procedures to determine that identity proofing evidence is used to reestablish the lost authentication factor.

BIND-20	**REQUIREMENT**: 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 SHALL require the claimant to authenticate using an authenticator of the remaining factor, if any, to confirm binding to the existing identity. (6.1.2.3)

	SUPPLEMENTAL GUIDANCE: While use of an authenticator at a different factor is only a single authentication factor (and therefore only AAL1), authentication in conjunction with the repeated identity proofing process provides assurance that the claimant is who they claim to be. **ASSESSMENT OBJECTIVE:** Determine if the CSP, when replacing a lost authentication factor, authenticates the subscriber. **POTENTIAL ASSESSMENT METHODS AND OBJECTS**: **Test**: Establish a multi-factor account and simulate the loss of an authentication factor (either a physical authenticator or a memorized secret). Observe the account-recovery procedures to determine that the subscriber is authenticated using any available authentication factor.

BIND-21	**REQUIREMENT**: Subscribers who have been identity proofed at IAL3 and lose all authenticators of a factor necessary for multi-factor authentication SHALL reestablish authentication factors in person, or through a supervised remote process as described in SP 800-63A Section 5.3.3.2. (6.1.2.3) **SUPPLEMENTAL GUIDANCE**: This is a supplemental requirement to BIND-19 to ensure that the process used for IAL3 proofed subscribers has the additional strength necessary to support that level of identity assurance. **ASSESSMENT OBJECTIVE:** Determine if the CSP applies additional diligence to replacement of a lost authentication factor for a subscriber identity proofed at IAL3. **POTENTIAL ASSESSMENT METHODS AND OBJECTS**: **Test**: Establish an account that has been identity proofed at IAL3 and simulate the loss of an authentication factor (either a physical authenticator or a memorized secret). Observe the account-recovery procedures to determine that the repeated identity proofing process is also done either in person or via supervised remote identity proofing.

BIND-22	**REQUIREMENT**: Subscribers who have been identity proofed at IAL3 and lose all authenticators of a factor necessary for multi-factor authentication SHALL verify the biometric collected during the original proofing process (6.1.2.3) **SUPPLEMENTAL GUIDANCE**: This is a supplemental requirement to BIND-19 to ensure that the process used for IAL3 proofed subscribers has the additional strength necessary to support that level of identity assurance, since identity proofing at IAL3 requires the collection of a biometric characteristic.

	ASSESSMENT OBJECTIVE: Determine if the CSP applies additional diligence to replacement of a lost authentication factor for a subscriber identity proofed at IAL3. **POTENTIAL ASSESSMENT METHODS AND OBJECTS**: **Test**: Establish an account that has been identity proofed at IAL3 and simulate the loss of an authentication factor (either a physical authenticator or a memorized secret). Observe the account-recovery procedures to determine that the repeated identity proofing process requires a match against the biometric collected during the original proofing process.

BIND-23	**REQUIREMENT**: 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. (6.1.2.3) **SUPPLEMENTAL GUIDANCE**: Loss of a memorized secret is different from the loss of a physical authenticator because it is not mitigated by the binding of multiple authenticators. This alternate method of associating a new memorized secret may be used by CSPs to avoid the need for repeating identity proofing. **ASSESSMENT OBJECTIVE:** Determine if the CSP, when replacing a lost memorized secret, does so as securely as possible. **POTENTIAL ASSESSMENT METHODS AND OBJECTS**: **Test**: Establish an account that has two-factor authentication and has at least two physical authenticators bound to it. Simulate the loss of the memorized secret and determine if the CSP requires use of two physical authenticators plus a confirmation code sent to an address of record in order to establish a new memorized secret.

BIND-24	**REQUIREMENT**: If the CSP opts to allow binding of a new memorized secret with the use of two physical authenticators, then the confirmation code SHALL consist of at least 6 random alphanumeric characters generated by an approved random bit generator [SP 800-90Ar1]. (6.1.2.3) **SUPPLEMENTAL GUIDANCE**: The confirmation code is required to have sufficient entropy and to be generated in a manner that cannot be predicted by an attacker. **ASSESSMENT OBJECTIVE:** Determine if the CSP, when replacing a lost memorized secret, uses a securely generated confirmation code. **POTENTIAL ASSESSMENT METHODS AND OBJECTS**: **Examine**: code and/or documentation for generating the confirmation code to

	determine that it has the required complexity and is generated using an approved random bit generator.

BIND-25	**REQUIREMENT**: If the CSP opts to allow binding of a new memorized secret with the use of two physical authenticators, then the confirmation code SHALL be 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 Service. Confirmation codes sent by means other than physical mail SHALL be valid for a maximum of 10 minutes. (6.1.2.3) **SUPPLEMENTAL GUIDANCE**: The confirmation code has a limited lifetime to mitigate the risk of loss or misappropriation in transit. **ASSESSMENT OBJECTIVE:** Determine if the CSP, when replacing a lost memorized secret, limits the validity duration of the confirmation code. **POTENTIAL ASSESSMENT METHODS AND OBJECTS**: **Examine**: code and/or documentation for generating the conformation code to determine that it will not be accepted beyond the specified time after it is sent.

7 Session Management Criteria

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.

7.1 Session Bindings

SESS-1	**REQUIREMENT**: A session is maintained by a session secret which SHALL be shared between the subscriber's software and the service being accessed. (7.1) **SUPPLEMENTAL GUIDANCE**: This secret binds the two ends of the session, allowing the subscriber to continue using the service over time. **ASSESSMENT OBJECTIVE:** Determine if session management is based on a secret that is shared by the session endpoints. **POTENTIAL ASSESSMENT METHODS AND OBJECTS**: **Examine**: CSP/RP procedures and/or code for associating incoming transactions with an existing session and determine that a shared secret is used.

SESS-2	**REQUIREMENT**: The secret SHALL be presented directly by the subscriber's software or possession of the secret SHALL be proven using a cryptographic mechanism. (7.1) **SUPPLEMENTAL GUIDANCE**: The session secret is considered a short-term secret, so direct presentation of a shared secret is permitted, even at AAL2 or AAL3. **ASSESSMENT OBJECTIVE:** Determine if session management is based on a shared secret. **POTENTIAL ASSESSMENT METHODS AND OBJECTS**: **Examine**: CSP/RP procedures and/or code for associating incoming transactions with an existing session and determine that a shared secret is used either directly or via proof of possession.

SESS-3	**REQUIREMENT**: The secret used for session binding SHALL be generated by the session host in direct response to an authentication event. (7.1) **SUPPLEMENTAL GUIDANCE**: The session secret needs to be directly associated with authentication so that it isn't inadvertently provided to the wrong session.

	ASSESSMENT OBJECTIVE: Determine if the session management secret is generated properly and associated with a maximum AAL at which it is valid. **POTENTIAL ASSESSMENT METHODS AND OBJECTS**: **Examine**: CSP/RP procedures and/or code for generating and managing session secrets, to determine that they are generated at the appropriate time and associated with the correct AAL.

SESS-4	**REQUIREMENT**: A session SHALL NOT be considered at a higher AAL than the authentication event. (7.1) **SUPPLEMENTAL GUIDANCE**: Each session has an associated maximum AAL at which it can be used that is derived from the authentication AAL; this is associated with the session and its secret by the CSP/RP. **ASSESSMENT OBJECTIVE:** Determine if the session associated with a maximum AAL at which it can be used. **POTENTIAL ASSESSMENT METHODS AND OBJECTS**: **Examine**: CSP/RP procedures and/or code for managing sessions to determine that that they are associated with the correct AAL.

SESS-5	**REQUIREMENT**: Secrets used for session binding SHALL be generated by the session host during an interaction, typically immediately following authentication. (7.1#1) **SUPPLEMENTAL GUIDANCE**: It is the responsibility of the host (RP/CSP/Verifier) to generate session secrets, not the subscriber. **ASSESSMENT OBJECTIVE:** Determine if the proper party generates session secrets. **POTENTIAL ASSESSMENT METHODS AND OBJECTS**: **Examine**: CSP/RP procedures and/or code for managing sessions to determine that that they are associated with the correct AAL.

SESS-6	**REQUIREMENT**: Secrets used for session binding SHALL be generated by an approved random bit generator [SP 800-90Ar1]. (7.1#2) **SUPPLEMENTAL GUIDANCE**: The use of a high-quality random bit generator is important to ensure that an attacker cannot guess the session secret. **ASSESSMENT OBJECTIVE:** Determine if the session management secret is securely generated.

	POTENTIAL ASSESSMENT METHODS AND OBJECTS: **Examine** code and/or documentation to determine that the generation process for session secrets uses an approved algorithm.

SESS-7	**REQUIREMENT**: Secrets used for session binding SHALL contain at least 64 bits of entropy. (7.1#2) **SUPPLEMENTAL GUIDANCE**: The use of a high-quality random bit generator is important to ensure that an attacker cannot guess the session secret. **ASSESSMENT OBJECTIVE:** Determine if the session management secret is securely generated. **POTENTIAL ASSESSMENT METHODS AND OBJECTS**: **Examine** code and/or documentation to determine that the generation process for session secrets uses an approved algorithm.

SESS-8	**REQUIREMENT**: Secrets used for session binding SHALL be erased or invalidated by the session subject when the subscriber logs out. (7.1#3) **SUPPLEMENTAL GUIDANCE**: At a minimum, the CSP/RP needs to ensure that the session secret can no longer to be used following logout. If possible, the secret should be erased on the subscriber endpoint as well. **ASSESSMENT OBJECTIVE:** Determine if the session management secret is invalidated properly following logout. **POTENTIAL ASSESSMENT METHODS AND OBJECTS**: **Examine**: CSP/RP procedures and/or code to determine that invalidating or erasing session secrets when logout occurs. **Test**: Make a copy of a session secret at the user endpoint, log out, and try to present the secret again as if logout had not occurred, and determine that it is no longer accepted.

SESS-9	**REQUIREMENT**: Secrets used for session binding SHALL be sent to and received from the device using an authenticated protected channel. (7.1#6) **SUPPLEMENTAL GUIDANCE**: Session secrets, particularly when directly presented, need to be protected against eavesdropping and man-in-the-middle attacks. This is typically accomplished using the Transport Level Security (TLS) protocol.

	ASSESSMENT OBJECTIVE: Determine if the session management secret is protected properly in transit throughout the session lifetime. **POTENTIAL ASSESSMENT METHODS AND OBJECTS**: **Examine**: the RP's documentation or code to determine that TLS or a similarly secure protocol is used in conjunction with an approved encryption protocol when transmitting session management secrets. **Test**: Attempt to manually downgrade an active session (e.g., from https to http) and determine that the downgraded packets are not associated with the session.

SESS-10	**REQUIREMENT**: Secrets used for session binding SHALL time out and not be accepted after the times specified in Sections 4.1.4, 4.2.4, and 4.3.4, as appropriate for the AAL. (7.1#7) **SUPPLEMENTAL GUIDANCE**: This requirement is in support of the reauthentication requirements in AAL2-*, AAL3-*, and REAUTH-*. The proper way to ensure that a session is logged out is to invalidate the session secrets associated with that session. A new session secret will need to be generated and associated with any session that is about to be established from the same endpoint. **ASSESSMENT OBJECTIVE:** Determine if the session management secret is invalidated properly when the session times out and has not been reauthenticated. **POTENTIAL ASSESSMENT METHODS AND OBJECTS**: **Examine**: the RP's documentation or code to determine that session secrets are invalidated properly when a session times out.

SESS-11	**REQUIREMENT**: Secrets used for session binding SHALL NOT be available to insecure communications between the host and subscriber's endpoint. (7.1#8) **SUPPLEMENTAL GUIDANCE**: User endpoints such as browsers that support both secure and insecure communications typically have mechanisms to flag information (e.g., cookies) that are only available to secure sessions. These mechanisms are required to be used for session management secrets. See also SESS-7. **ASSESSMENT OBJECTIVE:** Determine if the session management secret is tagged to be available only to secure sessions. **POTENTIAL ASSESSMENT METHODS AND OBJECTS**: **Examine**: the RP's documentation or code to determine that session secret management only allows their availability to secure sessions.

	Test: Attempt to manually downgrade an active session (e.g., from https to http) and determine that the downgraded packets are not associated with the session.

SESS-12	**REQUIREMENT**: Authenticated sessions SHALL NOT fall back to an insecure transport, such as from https to http, following authentication. (7.1#8) **SUPPLEMENTAL GUIDANCE**: In some cases, endpoints supporting https provide, primary for legacy purposes, the ability to connect via http as well. If not done properly, this can make the site vulnerable to a "downgrade attack" where a session switches from https to http. This must not happen for authenticated sessions. If session secrets are managed properly, this downgrade interferes with the continuity of the session. **ASSESSMENT OBJECTIVE:** Determine if it is possible to downgrade a session in progress from https to http or analogous downgrade. **POTENTIAL ASSESSMENT METHODS AND OBJECTS**: **Examine**: the RP's documentation or code to determine that either insecure transport is not accepted or that a session using secure transport cannot continue under insecure transport. **Test**: Attempt to manually downgrade an active session (e.g., from https to http) and determine that the downgraded packets are not associated with the session.

SESS-13	**REQUIREMENT**: URLs or POST content SHALL contain a session identifier that SHALL be verified by the RP to ensure that actions taken outside the session do not affect the protected session. (7.1) **SUPPLEMENTAL GUIDANCE**: Unique session identifiers in the URL or POST content are used to ensure that sessions are not vulnerable to cross-site request forgery (CSRF). Note that the session identifier is separate and different from the session secret; under no circumstances should the session secret be included in a URL. **ASSESSMENT OBJECTIVE:** Determine if session management protects against cross-site request forgery. **POTENTIAL ASSESSMENT METHODS AND OBJECTS**: **Examine**: URLs and/or POST content to determine that session identifiers are present as required, and RP code/documentation to ensure that transactions with the wrong session identifier are not honored. **Test**: Attempt to perform a transaction with an incorrect session identifier and verify that transactions with the wrong session identifier are not honored.

SESS-14	**REQUIREMENT**: Browser cookies SHALL be tagged to be accessible only on secure (HTTPS) sessions. (7.1.1#1) **SUPPLEMENTAL GUIDANCE**: Browser cookies have an optional "secure" flag to ensure that they are not accidentally transmitted over a non-secure channel. This flag must be set for session secrets. **ASSESSMENT OBJECTIVE:** Determine if session secrets are protected from access by insecure sessions. **POTENTIAL ASSESSMENT METHODS AND OBJECTS**: **Test**: Observe the browser cookies at a user endpoint during an active session and ensure that cookies containing session secrets have the secure flag set.

SESS-15	**REQUIREMENT**: Browser cookies SHALL be accessible to the minimum practical set of hostnames and paths. (7.1.1#2) **SUPPLEMENTAL GUIDANCE**: Browser cookies have a scope parameter that limits the sites from to which the cookie can be sent; this should be specified as specifically as possible to limit access to the session secret as narrowly as practical. **ASSESSMENT OBJECTIVE:** Determine if session secrets are protected from access by unauthorized sites. **POTENTIAL ASSESSMENT METHODS AND OBJECTS**: **Test**: Observe the browser cookies at a user endpoint during an active session and ensure that cookies containing session secrets are scoped as specifically as can be supported by the service.

SESS-16	**REQUIREMENT**: Expiration of browser cookies SHALL NOT be depended upon to enforce session timeouts. (7.1.1#4) **SUPPLEMENTAL GUIDANCE**: While browser cookies have an expiration time, enforcement of session timeouts must occur at the RP/CSP and not at the user endpoint. Cookie expiration may, however, be used to limit accumulation of cookies in the browser. **ASSESSMENT OBJECTIVE:** Determine if cookie expiration is used for session timeout. **POTENTIAL ASSESSMENT METHODS AND OBJECTS**: **Test**: Extend the lifetime of a session secret cookie in the browser to exceed the

	session timeout and verify that it is not possible to maintain the session for longer than the permitted reauthentication time.

SESS-17	**REQUIREMENT**: The presence of an OAuth access token SHALL NOT be interpreted by the RP as presence of the subscriber, in the absence of other signals. (7.1.2) **SUPPLEMENTAL GUIDANCE**: Access tokens, used in federated identity systems, may be valid after the authentication session has ended and the subscriber has left. **ASSESSMENT OBJECTIVE:** Determine if access tokens are used inappropriately to establish presence. **POTENTIAL ASSESSMENT METHODS AND OBJECTS**: **Examine**: If access tokens are used, determine that an independent means is used to verify the continuity of the session.

7.2 Reauthentication

REAUTH-1	**REQUIREMENT**: Continuity of authenticated sessions SHALL be based upon the possession of a session secret issued by the verifier at the time of authentication and optionally refreshed during the session. (7.2) **SUPPLEMENTAL GUIDANCE**: This is a reiteration of requirement SESS-1. **ASSESSMENT OBJECTIVE:** Determine if session management is based on a secret that is shared by the session endpoints. **POTENTIAL ASSESSMENT METHODS AND OBJECTS**: **Examine**: CSP/RP procedures and/or code for associating incoming transactions with an existing session and determine that a shared secret is used.

REAUTH-2	**REQUIREMENT**: Session secrets SHALL be non-persistent, i.e., they SHALL NOT be retained across a restart of the associated application or a reboot of the host device. (7.2) **SUPPLEMENTAL GUIDANCE**: Session secrets are not to be maintained across a restart of the associated application or a reboot of the host device in order to minimize the likelihood that a misappropriated logged in device can be exploited.

	ASSESSMENT OBJECTIVE: Determine if session management secrets are maintained in non-persistent storage or flagged as non-persistent (e.g., for browser cookies) **POTENTIAL ASSESSMENT METHODS AND OBJECTS**: **Examine**: CSP/RP procedures and/or code for managing session secrets at the user endpoint to determine that available mechanisms to erase secrets on restart/reboot are used.

REAUTH-3	**REQUIREMENT**: Periodic reauthentication of sessions SHALL be performed to confirm the continued presence of the subscriber at an authenticated session. (7.2) **SUPPLEMENTAL GUIDANCE**: In order to protect against a subscriber leaving a logged-in endpoint, timeouts are defined for session inactivity and overall session length. The timer for these timeouts is reset by a reauthentication transaction. Higher AALs have more stringent (shorter) reauthentication timeouts. Following expiration of the session timer, the subscriber is required to start a new session by authenticating. **ASSESSMENT OBJECTIVE:** Determine if session timeouts are honored. **POTENTIAL ASSESSMENT METHODS AND OBJECTS**: **Examine**: CSP/RP procedures and/or code for managing session timers and determine that sessions are logged out when the timers expire. **Test**: Begin a session (authenticate) and allow the session to expire. Determine that the session is terminated at the end of the session timeout period. This test should be performed for both inactivity and total session timers.

REAUTH-4	**REQUIREMENT**: A session SHALL NOT be extended past the guidelines in Sections 4.1.3, 4.2.3, and 4.3.3 (depending on AAL) based on presentation of the session secret alone. (7.2) **SUPPLEMENTAL GUIDANCE**: The existence and possession of a session secret does not consider whether the subscriber continued to be in control of the session endpoint. To mitigate this risk, the session secret is only valid for a limited period of time. While the session secret is "something you have", it is not an authenticator. **ASSESSMENT OBJECTIVE:** Determine if the appropriate session timeouts for the session AAL are honored. **POTENTIAL ASSESSMENT METHODS AND OBJECTS**: **Examine**: CSP/RP procedures and/or code for managing session timers and

	determine that sessions are logged out at the appropriate expiration times for the session AAL. **Test**: Begin a session (authenticate) and allow the session to expire. Determine that the session is terminated at the end of the session timeout period. This test should be performed for both inactivity and total session timers.

REAUTH-5	**REQUIREMENT**: Prior to session expiration, the reauthentication time limit SHALL be extended by prompting the subscriber for the authentication factor(s) specified in Table 7-1 (any one factor at AAL1, a memorized secret or biometric at AAL2, and full reauthentication at AAL3). (7.2) **SUPPLEMENTAL GUIDANCE**: Before the session times out, the subscriber should be given an opportunity to reauthenticate to extend the session. The subscriber may be prompted when an idle timeout is about to expire, to allow them to cause activity and thereby avoid the need to reauthenticate. **ASSESSMENT OBJECTIVE:** Determine if proper reauthentication methods are used. **POTENTIAL ASSESSMENT METHODS AND OBJECTS**: **Examine**: CSP/RP procedures and/or code to determine that subscribers whose sessions are about to expire are required to reauthenticate with the required factors for the AAL.

REAUTH-6	**REQUIREMENT**: When a session has been terminated, due to a time-out or other action, the user SHALL be required to establish a new session by authenticating again. (7.2) **SUPPLEMENTAL GUIDANCE**: After the session time-out, the session is terminated. A new session needs to be established, and full authentication requirements for the session AAL need to be satisfied. **ASSESSMENT OBJECTIVE:** Determine sessions are fully logged out at the expiration of the reauthentication time. **POTENTIAL ASSESSMENT METHODS AND OBJECTS**: **Examine**: CSP/RP procedures and/or code to determine that subscribers whose sessions have expired are required to establish a new session, including full authentication for the AAL.

REAUTH-7	**REQUIREMENT**: If federated authentication is being used, then since the CSP and RP often employ separate session management technologies, there SHALL NOT be any assumption of correlation between these sessions. (7.2.1)

	SUPPLEMENTAL GUIDANCE: When an RP session expires and the RP requires reauthentication, it is entirely possible that the session at the CSP has not expired and that a new assertion could be generated from this session at the CSP without reauthenticating the user. **ASSESSMENT OBJECTIVE:** Determine if session management by the RP makes any use of CSP session times in federated applications. **POTENTIAL ASSESSMENT METHODS AND OBJECTS**: **Examine**: CSP and RP procedures and/or code for federated applications to determine that CSP authentication times are not used to establish the length of RP sessions.

REAUTH-8	**REQUIREMENT**: An RP requiring reauthentication through a federation protocol SHALL — if possible within the protocol — specify the maximum acceptable authentication age to the CSP. (7.2.1) **SUPPLEMENTAL GUIDANCE**: In some applications, RPs may require a "fresh" authentication to meet its authentication risk requirements. By specifying maximum age, the RP can proactively request the CSP to obtain a new authentication to meet that requirement. **ASSESSMENT OBJECTIVE:** Determine if federated session management supports authentication freshness specification. **POTENTIAL ASSESSMENT METHODS AND OBJECTS**: **Examine**: CSP and RP procedures and/or code for authenticating subscribers where the RP has specific authentication freshness requirements to determine that requirement is communicated to the CSP when supported by the federation protocol.

REAUTH-9	**REQUIREMENT**: If federated authentication if being used and an RP has specific authentication age requirements that it has communicated to the CSP, then the CSP SHALL reauthenticate the subscriber if they have not been authenticated within that time period. (7.2.1) **SUPPLEMENTAL GUIDANCE**: When the RP communicates its authentication freshness requirements to the CSP, the CSP is expected to reauthenticate the subscriber to support a session that meets those requirements. **ASSESSMENT OBJECTIVE:** Ensure that federated session management supports authentication freshness specification. **POTENTIAL ASSESSMENT METHODS AND OBJECTS**: **Examine**: CSP and RP procedures and/or code to determine that the CSP

	reauthenticates the subscriber reauthenticates the subscriber when the RP has specific authentication freshness requirements that are expiring.

REAUTH-10	**REQUIREMENT**: If federated authentication if being used, the CSP SHALL communicate 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. (7.2.1) **SUPPLEMENTAL GUIDANCE**: When federation authentication is being used, the authentication assertion from the CSP needs to contain the authentication event time to allow the RP to request reauthentication at an appropriate interval if it has specific authentication age requirements. **ASSESSMENT OBJECTIVE:** Determine if federated authentication assertions specify the authentication time. **POTENTIAL ASSESSMENT METHODS AND OBJECTS**: **Examine**: CSP and RP procedures and/or code to determine that the CSP includes authentication time in its authentication assertions.