**Feedback**

**I. General Comments**

1. The NIST SP 800-63 framework focuses on US agencies and the US federal government. If NIST intends for the framework to become international then it needs to start covering use cases that reflect wider adoption of the document.
2. In current work, the Levels of Assurance (LoA) are considered to be static. In reality, each LoA can cover a range of assurance, depending on context of use and age over time. not all levels of assurance are the same in the way that they could be used. In many cases the value of a token can change based on such things as the context of use or in the order of evaluation. In many applications, the Level of Assurance has a range of trust and thus multiple tokens, even from the same category, could be combined to elevate the confidence in a transaction. NIST needs to acknowledge that LoAs can be considered to be a dynamic attribute that assumes a range and can also be aged. The range and aging function is a function of the enrolement, frequency of use and the context of use.
3. The framework looks at the traditional three categories of authentication factors: something you have, something you are, and something you know. These categories are limiting because they assume strict and static authentication tokens with limited authentication capabilities. In many cases the context around the use of an authentication factor, such as access from a known location or time of day, can change the order of challenges or responses required by a risk engine. NIST needs to enlarge the scope of authentication categories to include context and behavior to enable a wider set of acceptable tokens and devices housing these tokens. For example, a smart phone can house a soft token that is protecting a soft PKI certificate in a Key Chain. The trust level in the token can change based on the device health such as rooting or the use of anti-virus software. As such the achievable LoA from the device can vary with time and could be a function of software on the device and also a function of OS system integrity.
4. At the point of transaction, the environment needs to be evaluated, not just the credential. NIST needs to start accommodating the latest trends in using a device as part of the authentication process. In this regard, the Fast ID Online (FIDO) and OASIS Identity-Based Attestation and Open Exchange Protocol Specification (IBOPS) models of enabling the user to authenticate to a device, and then an agent to attest to this fact, changes the dynamics of determining the LoA and the verifier (or CSP). Emphasis should be given to methods that lead to a hacker resistant authentication method where hacking the verifier server will not result in massive security breaches. For example, in the FIDO and the OASIS IBOPS models, the server holds a pointer to the client and does not store any credentials locally. This changes the attack vector of hackers whereby they will need to hack the server and the associated device to obtain a credential.
5. Recommend harmonizing NIST SP 800-63 with work done in ITU-T X.1254, ISO 29115 and OASIS TRUST Elevation.
6. The use of biometrics in the document needs to be expanded. Currently the scope is very limited to enrollment and second or third factors on hard tokens. However, the trend in the industry to unlock devices using biometrics with the task of binding the access request to a user to be performed by the verifier through the use of cumulative identity attributes that binds a device, location and behavior to an authorization request.
7. Many systems are designed to support flexible authentication based on risk-based access. In many cases, these systems select many tokens from a given LoA to enhance the trust with the authentication step. NIST needs to be flexible and adapt the work from OASIS TRUST Elevation TC in order to piggy-back on the use of common LoA metadata and trust elevation protocols that could work with Oauth, OpenID Connect and SAML.
8. The advent of smart devices and the Internet of Things requires the extension of the work to include non-human entities. The assumption that the interaction is a web-based interaction between the user and the verifier is not totally true in the current trends. Given that mobile single sign technologies are still primitive, it is important to not rely on cookies or unprotected tokens for Single Sign On support.

**II. Threats to Authentication**

In clause 5.2 page 11, NIST 800-063-1 states

“Authentication systems that incorporate all three factors are stronger than systems that only incorporate one or two of the factors. The system may be implemented so that multiple factors are presented to the verifier, or some factors may be used to protect a secret that will be presented to the verifier. For example, consider a hardware device that holds a cryptographic key. The key might be activated by a password or the hardware device might include a biometric capture device and uses a biometric to activate the key. Such a device is considered to effectively provide two factor authentication, although the actual authentication protocol between the verifier and the claimant simply proves possession of the key.”

1. It is noted that the above statement is not accurate. It is not the number of factors that matters but the reduction in threats that the combination of factors achieves. The way the combination occurs can either reduce or increase threats of context and related vulnerabilities. The OASIS TRUST Elevation TC did produce two committee drafts based on ITU-T X.1254 (ISO 29115) that include a comprehensive list of authentication methods, and a way of computing the authentication strength based on vulnerabilities and their associated control. It is recommended that NIST build on this work to ensure that authentication strength is understood by implementers.
2. It is recommended that Trust Elevation techniques should be added to the next version of the document. Trust elevation can occur in multiple places. Consider for example a scenario where a CSP can authenticate a user coming from a smart device. The CSP can have the option of using multiple capabilities in the device such as biometric, location, and soft PKI tokens or certificates to authenticate the user. The authentication strength can be consistent with the risk engine requirements. If the CSP is acting as an IDP or attribute provider to other Verifiers or relying parties, these parties can elevate the authentication strength per their own requirements and may be able to ask the CSP of doing that on their behalf or combine the CSP tokens into application specific attributes, such as behavior, that they also can do on their own.
   1. A standardized means of asking for higher assurance such as the ones being developed by OASI TRUST Elevation TC should be used.
   2. An overlay/tailoring capability similar to SP 800-53 could also be used. Each 800-63 LOA would become a baseline that could be tailored as necessary, consistent with tailoring guidance to help each community of interest better meet its mission / business needs. In the overlays authentication strength can be computed using concepts form OASIS TRUST Elevation TC.

**III. NIST 5.2 Page 12**

Biometrics are unique personal attributes that can be used to identify a person. They include facial pictures, fingerprints, DNA, iris and retina scans, voiceprints and many other things. In this document, biometrics are used in the registration process to be able to later prevent a subscriber, who in fact registered, from repudiating the registration. This will help to identify those who commit registration fraud and to unlock tokens. Biometrics are not used directly as tokens in this document.

**Appendix A**

**Below is material for consideration to be added to the text in Appendix A and B.**

-------

**5.3 Electronic Credentials Page 13**

Electronic identity credentials bind a name and perhaps other attributes to a token. This recommendation does not prescribe particular kinds of electronic credentials. There are a variety of electronic credential types in use today, and new types of credentials are constantly being created. At a minimum, credentials include identifying information that permits recovery of the records of the registration associated with the credentials and a name that is associated with the subscriber. In every case, given the issuer and the identifying information in the credential, it must be possible to recover the registration records upon which the credentials are based. Electronic credentials may be general- purpose credentials or targeted to a particular verifier. Some common types of credentials are:

* X.509 public key identity certificates that bind an identity to a public key;
* X.509 attribute certificates that bind an identity or a public key with some attribute;
* Kerberos tickets that are encrypted messages binding the holder with some attribute or privilege.

---------------------------------------------------------------

* What schemas for establishing identity assurance have proven effective in providing an appropriate amount of security, privacy, usability, and trust based on the risk level of the online service or transaction? How do they differentiate trust based on risk? How is interoperability of divergent identity solutions facilitated?
  + Derived Credentials? (Harmonizing 800-63 and 800-157)
  + How can agencies address the need for higher LoAs in order to issue credentials that allow access to personal healthcare information with the homeless population? We need a schema that addresses this population. Primary obstacle is identity proofing. When a homeless veteran comes into a VAMC, we want to be able to identify who they are in order to connect them to the correct health record. Is this in scope for 800-63 since 800-63 is specifically for electronic authentication?
  + There is a gap in our ability to issue a credential to a homeless veteran. What we want is the ability to issue some kind of credential to homeless in order to allow both physical and logical access without having to ID proof them each time they come in.
  + What do we need to provide to our homeless veterans?
    - We need to be able to provide them with healthcare services.
    - We need to be able to provide them with other VA benefits through VBA and NCA.
    - We need to be able to consistently identify them and attach their name to EHR and other personal VA records with some degree of confidence.
    - Electronic wallets
  + What can’t we do right now?
    - Identity proofing
      * Generally they don’t have government issued photo IDs in order to be ID proofed at any LoA above LoA1.
      * Are there alternative procedures and identifiers that can be put in place to allow for ID proofing at something greater than LoA1 for the homeless/disenfranchised/or otherwise undocumented population? (Concatenating multiple LoA1 credentials, trust elevation.) Action item: Diana to pull together a paragraph identifying the issue and what we would like addressed in 800-63 to help us deal with the issue.
    - Tokens
    - Token issuing

**Topic:** ID proofing above LoA1 for populations who don’t have U.S. government issued photo IDs or an address of record. This includes the homeless population and others who have not been able, for whatever reason, to get a U.S. government issued id. Another scenario is when US agencies overseas need to issue credentials to people who only have foreign government identity documents.

**Issue:** The VA issues credentials at LoA2 for Veterans, but we are unable to issue these credentials to homeless Veterans because we are unable to meet the LoA2 criteria for ID proofing. In general, the homeless population has neither an address of record nor a U.S. government issued ID. (Add sentence to add a foreign issued IDs. Do a separate write-up for the foreign issued IDs.)

**Suggestion for inclusion in NIST 800-63**: Include additional/alternative procedures and identifiers that can be used for identity proofing at greater than LoA1 for people without a U.S. government issued ID. Some possibilities include:

* Trust elevation techniques
* Aggregation of multiple LoA1 credentials/personal information
* Biometrics
* Could identity assurance processes and technologies be separated into distinct components? If so, what should the components be and how would this provide appropriate level of identity assurance?
  + Create building blocks that when put together in different configurations allow for the achievement of different LoAs?
    - The idea that multiple LoA1 credentials may, when aggregated, achieve LoA2.
* What innovative approaches are available to increase confidence in remote identity proofing? If possible, please share any performance metrics to corroborate increased confidence levels.
  + Diana’s white paper that references the OASIS trust elevation group?
* (Judy) What privacy considerations arising from identity assurance should be included in the revision? Are there specific privacy-enhancing technologies, requirements or architectures that should be considered?
  + Diana will reach out to the OASIS PMRM and Privacy by Design WGs and see if she can get some ideas.
  + Judy will write up something on this and try and find a privacy paper written by Ann Geyer
  + Need a privacy impact consideration for the different LoAs? Need a write up of what the privacy impact considerations would look like at the different LoAs.

Write up from Judy:  
**TOPIC: Privacy Enhancing Digital Identities**

**ISSUE**:  Existing government–centric privacy legislation and guidance are inadequate to protect individual privacy rights that are encapsulated in government and private sector systems, as witnessed by the EHR breaches and cybersecurity threats.  Government-centric legislation includes Federal Information Practice Principles (FIPP) that has become “God and apple pie,” not only for government agencies, but has been widely adopted by the U.S.  Private sector. Moreover, existing privacy legislation such as the requirement that agencies perform a Privacy Impact Assessment (PIA) is government-focused and largely ineffective in preventing cybersecurity attacks. The existing legislation and solutions are  not linked to security of personal identities.

 Even in the healthcare industry, which has sector-specific privacy legislation (HIPAA Security and Privacy rule, Accountable Care Act and Population Health), digital identifies are not sufficiently safeguarded.  Breaches are commonplace, involving the compromise of millions of EHR records, including President Obama’s, e.g., Anthem, and identity theft is rampant.

**NIST ACTION**:

NIST needs to provide policy support for the new generation of privacy protections. There is no privacy policy guidance that attempts to safeguard one’s digital identity. Government sponsored PIV, PIV-I,  and PIV-Derived Credentials and their associated Levels of Assurance (LOA) are focused on verification and validation of the token, not on the digital identity of the individual.

Privacy here is defined as reasonable assurance of secure access to a person’s Personally Identifiable Information (PII), the possession of a unique digital identity, and the relative sanctity of their Protected Health Information (PHI).  An example of a definition of unique digital identity can be found in the draft language available from the NIST/IDESG Healthcare Working Group (HC WG).

The new generation of privacy protections includes frameworks and standards developed and piloted by Health Level 7, International, such as Data Segmentation for Privacy,  Fast Healthcare Interoperability Resources (FHIR) - a draft standard for the exchange of resources which was recently piloted and demonstrated at the HIMSS15 and RSA meetings in April 2015 as “Privacy on FHIR.”

* What requirements, processes, standards, or technologies are currently excluded from 800-63-2 that should be considered for future inclusion?
  + Solutions for portability of authentication credentials between agencies and organizations (Identity federation through the use of things like Connect.gov and FIDO compliant tokens/web sites)
  + Derived credentials
    - Derived PIVi?
  + Biometrics
  + Trust-elevation (OASIS Trust Elevation workgroup)
  + OpenID Connect
  + FIDO standard
  + Fair Information Practice Principles (FIPP)
    - Consent as part of authentication.
  + NIST Computer Security Division Released NISTIR 7817, A Credential Reliability and Revocation Model for Federated Identities (Alicia to send a summary)
    - "This document seeks to investigate credential and attribute revocation with a particular focus on identifying missing requirements. This document first introduces and analyzes the different types of digital credentials and identifies missing revocation-related requirements for each model in a federated environment. As a second goal, and as a by-product of the analysis and recommendations, this paper suggests a credential reliability and revocation service that serves to address the missing requirements."
    - Look in section 3.6. Supplementary URRS Feature: Credential Media (Token) Revocations
    - Look in section 3.7. Supplementary URRS Feature: Derived Credential Revocation
  + Guidance on Single Sign-On (SSO)?
  + Mobile device authentication solutions
  + Authentication in the cloud
  + user-centric solutions
  + Guidance around security token services (Dave)
  + Identity as a service (Dave)
    - (blurb from Dave) To improve customer experience, enhance convenience, and increase the number of customers accessing VHA web sites,  VHA is interested in mobile authentication, cloud-based proofing and authentication, and security token services.  We suggest expanding 800-63 as necessary to provide guidance/insights in each of these specific areas.
  + Non-person authentication
    - Currently, 800-63 focuses only on remote authentication of a human to a federal IT system. The VHA has significant need for authentication in various other contexts including non-person entity (e.g., device) authentication, system to system authentication in a service oriented architecture model, and data origin authentication.  We suggest expanding the scope of 800-63 to provide guidance/insights on all logical access authentication contexts.
  + Anonymous/pseudonymous authentication
    - In addition, VHA has significant need for authentication of anonymous or pseudonymous claimants. 800-63 does speak to those briefly, but we suggest adding any additional guidance/insights in those areas.
    - (Dave to provide use case scenario)
* Should a representation of the confidence level in attributes be standardized in order to assist in making authorization decisions? What form should that representation take?
* What methods can be used to increase the trust or assurance level (sometimes referred to as “trust elevation”) of an authenticated identity during a transaction? If possible, please share any performance metrics to corroborate the efficacy of the proposed methods.
  + Refer them to the OASIS trust elevation group for additional (Diana will bring this to their attention.)
  + We suggest implementing an overlay/tailoring capability similar to SP 800-53. Each 800-63 LOA would become a baseline that could be tailored as necessary, consistent with tailoring guidance to help each community of interest better meet its mission / business needs. We understand that an overlay can be dangerous in that it could dilute an LOA if inappropriate substitutions are made. But if changes are made that are comparable to LOA requirements, that would likely be a great benefit to communities that have different needs. It would also likely provide greater flexibility during the lifespan of a specific 800-63 version (i.e., communities won't need to wait for a new 800-63 version to implement an alternative approach that would be deemed satisfactory/acceptable at that point in time).

Other topics:

* The need for additional LoAs
  + How can agencies address the need for higher LoAs in order to access things like healthcare services with the homeless population?
  + Use of mobile devices?
  + Sector specific LOAs. (Diana: I’m not sure that this is in scope for 800-63 but it would be appropriate to propose additional LOAs along with scenarios describing possible application.)

Write-up from Judy:  
**TOPIC: Enriching LOAs**

**The Problem:**

1)      The private sector is trying to use the 800-63-2 LOA structure and it’s not working. The NIST Guideline is too rigid and government-centric for public sector adoption and is not user-friendly in its current configuration.  The consumer-centric market is rapidly being transformed into a relational digital enterprise of the Internet of Things. The NIST Guideline needs to re-purpose its focus on end user identity [and privacy control]. Note: This has a direct influence on controlling privacy (as defined by access control, who has what privileges? When? Under what conditions or event?).

2)      LOA 1 is quickly being eroded as social media private sector institutions and governments at all levels abandon the  'user-name and password' as an access function due to escalating cybersecurity and identity threats and breaches.

3)      The healthcare community is chipping away at LOA 2, as seen by the fact that the HIMSS Identity Management task Force recently endorsed LOA 3 for access to healthcare portals. See<http://www.himss.org/files/HIMSS_IDMTF_IAPP_Recommendation_Final.pdf>.

**NIST Action**

1) NIST needs to enrich LOA's 2, 3, 4   by adding functionality layers to their core components, e.g., via an attribute ecosystem. LOA 2, 2.1, 2.2 … 3.5, 4.5, etc., each with supporting trust marks.

For LOA 3, everybody has to adhere to core components, and then to each desired level of add-ons. NIST has to define what these should be.

2) NIST should convene groups to decide on a set of pre-approved devices for biometric devices, iris scans, etc., that would represent functionality levels for the three LOA classes and unique to Level 4, the acceptance of e-notarization where several states are in play with more to follow. NIST would determine the device mix.

3) NIST needs to enrich the existing government LOA platform and process, by enriching digital identities and associated attributes. This would establish a digital marketplace for authenticated identities.

The private sector could then adopt this enriched infrastructure for a quasi-seamless interface between government and the private sector, and within the private sector.

* Looking at LoAs from different viewpoints:
  + The same credential can have different LoAs depending on the viewpoint.
  + E.g.: from the viewpoint of VA, something like Google credentials are only LoA1; however from the viewpoint of the consumer using Google credentials with 2-factor authentication enabled is at least LoA2 or higher. Increased trust in the credential from the viewpoint of the consumer that the consumer is the only one who can authenticate to anything using that credential.

Identified Gaps in the existing document that need to be addressed:

* Foreign issued credentials when ID proofing overseas: how do agencies deal with them at the different LoAs? Diana to pull from her risk assessment paper.
  + Add guidance on how to gain confidence? What are acceptable/comparable ID proofing documentation/processes? Could this be similar to the homeless population solution?
* Look closely at the LOA descriptions and ensure that “valid credential,” “validate,” “verified credential” and “verification” are well defined as well as the processes involved.
* Define “control” and “possession” and harmonize these definitions across NIST standards.

**Appendix B**

**DAON Input**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Line number**  (e.g. 17) | **Clause/ Subclause**  (e.g. 3.1) | **Paragraph/ Figure/ Table/**  (e.g. Table 1) | **Type of comment1** | **Comments** | **Proposed change** |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | 2 | 3rd full para on pg. 3 | te | Biometrics is not considered authentication tokens because they are not secrets; however, they may be used to activate other secret-based tokens. Therefore, they may be used in Multi-factor Tokens (as defined in 6.1.1) but not in Multi-token authentication (as defined in 6.1.2).  This addresses their use in “serial” verification, through local activation, but not “parallel” verification where the second factor is verified at the verifier.  This document should allow for the use of biometrics in the second case where:   1. The biometric is used as a 2nd (or 3rd) factor only, and 2. The biometric is protected during transmission to the verifier.   For example, a Single-factor crypto token uses a locally stored key within a cryptographic protocol (e.g., TLS), achieving LoA2. When a biometric is added to activate that key, it becomes a Multi-factor crypto token, achieving LoA3.  However, if the Single-factor crypto token is both verified and used to create a secure channel to the verifier, the biometric may be transmitted over that secure channel and verified at the verifier rather than locally. This is not currently supported. | Add to the end of this paragraph:  “However, biometrics are included in the list of defined token types for use as a second or third authentication factor only.”  NOTE: Other changes below relate to this same comment. |
|  | 2 | 1st para on pg. 4 | te | Rather than disallow biometrics as a token type, restrict them to use as a 2nd or 3rd factor given the conditions cited above. | Change 1st sentence to read:  “Biometric characteristics do not constitute secrets suitable for use as a single authentication factor.”  Change 3rd sentence to read:  This document supports the use of biometrics to “unlock” conventional authentication tokens, as a 2nd or 3rd factor in multi-token authentication, to prevent repudiation of registration, and to verify that the same individual participates in all phases of the registration process.  OR  Delete entire paragraph. |
|  | 3 | Biometrics entry, 2nd para | te | Same as above. | Change 2nd sentence to read:  “In this document, biometrics may be used to unlock authentication tokens, as a 2nd or 3rd factor in multi-token authentication, and prevent repudiation of registration. |
|  | 4.3 | 4th para on pg. 21 | te | Same as above. | Add to last sentence:  “except when used as a 2nd or 3rd factor in multi-token authentication.” |
|  | 4.3 | 5th para on pg 21 | te | Same as above. | Replace last 2 sentence with:  “If a single factor is presented to the Verifier, it must contain a secret. Additional factors used to protect (activate) the secret token do not themselves need to be secrets. If multiple factors are presented to the Verifier, at least one must contain a secret and others must be adequately protected.” |
|  | 4.3 | 2nd para on pg 22 | te | Same as above. | Add 3rd paragraph (between current 2nd & 3rd) reading:  “In addition, biometrics may be used as a 2nd or 3rd factor in a multi-token authentication. For example, consider again the piece of hardware (a token) which contains a cryptographic key (the token secret). The cryptographic key produces an output (the token authenticator) which is used in the authentication process to authenticate the Claimant and to establish a secure channel to the piece of hardware. The biometric may then be captured on this hardware, transmitted over the secure channel, and authenticated at the Verifier. In this case, an impostor must steal the encrypted key (by stealing the hardware) and replicate the fingerprint to be successfully authenticated, just as above. This specification considers such a device to effectively provide two factor authentication, since both the secret and the biometric are required to complete the authentication. |
|  | 6.1 | 1st para | te | Same as above. | Change 1st sentence to read:  “In the e-authentication context, a primary token contains a secret to be used in authentication processes.”  Add before last sentence:  “Secondary tokens (those used as a 2nd or 3rd factor) may not be secrets (i.e., may be *something you are*). |
|  | 6.1.2 |  | te | Same as above. | Add 10th bullet:   * *Biometric Token*. A sample of a biometric characteristic captured from the claimant. A reference sample is collected during registration and stored within the CSP. During authentication, the claimant presents their biometric characteristic to a biometric reader which captures a fresh biometric sample which is securely transmitted to the verifier where it is matched to the reference sample to determine if the two samples originate from the same human being. Biometric tokens may only be used as a 2nd or 3rd factor in multi-token authentication; they may not be used alone as a single-token. Biometrics is *something you are.* |
|  | 6.2 | Table 4 | te | Add biometric threat examples. | Under Duplication, add the following example:  A biometric sample is copied to create an artefact. |
|  | 6.2.1 | Table 5 | te | Add biometric threat mitigation. | Under Duplication, add the following mitigation:   * Use biometrics which are more difficult to discover (e.g., those not publicly exposed) and/or incorporate biometric aliveness detection mechanisms, including challenge/response. |
|  | 6.3.1.1 | Para 1 | te | Add note regarding biometrics. | After 1st para, add 2nd para to read:  “Although biometric tokens may not be used in single-token authentication, the associated token and verifier requirements are included in Table 6 in order to specify their requirements when used in multi-token authentication.” |
|  | 6.3.1.1 | Table 6 | te | Add biometric token requirements.  NOTE: Accuracy proposed is taken from NIST SP800-76-2. | Add row at end of table with the following entries:  Token Type: Biometric Token  Level: N/A (used only as 2nd or 3rd factor)  Token Requirements: Biometric tokens shall be encrypted during storage and transmission.  Verifier Requirements: The verifier shall implement a biometric matcher capable of achieving an FNMR less than or equal to 0.01 at an FMR of 0.01 (with one or more samples). |
|  | 6.3.1.2 | Table 7 | te | Add biometrics to Table 7 to indicate their use in multi-token authentication. | Add last row as shown below:    Add last column as shown below:    Where the row/column headers are unchanged other than the addition of rows/columns for Biometric Token. |
|  | 6.3.1.2 | 1st para on pg 56 | te | Rather than disallow biometrics as a token type, restrict them to use as a 2nd or 3rd factor given the conditions cited in Daon-1. | Change to read:  The principles used in generating Table 7 are as follows. Level 3 can be achieved using two tokens rated at Level 2 that represent two different factors of authentication. Since this specification does not address the use of biometrics as a stand-alone token for remote authentication, achieving Level 3 can occur by either adding a Biometric Token (*something you are*) to a separate Level 2 token (either *something you have* or *something you know*) or by combining two separate Level 2 tokens from the *something you have* and *something you know* categories.  Token (Level 2, *something you have*) + Token (Level 2, *something you know*) → Token (Level 3)  or  Token (Level 2, *something you have or something you know*) + Biometric Token (*something you are*) → Token (Level 3) |
|  | 6.3.1.2 | 3rd para on pg 56 | te | Same as above. | Add new paragraph between existing 3rd & 4th paragraphs:  “Likewise, a Biometric Token may be combined with a Memorized Secret Token (*something you know*) or a Single-Factor Cryptographic Device (*something you have*) to elevate the trust of the Level 2 single-factor token to a Level 3 multi-token (and multi-factor) authentication.” |
|  | 7.3.1.3 | First bullet | te | Biometrics should be protected to the same level as shared secrets. | Change first paragraph to read:  *Credential storage* – Files of long-term shared secrets or biometrics used by CSPs or Verifiers at Level 3 shall be protected by access controls that limit access to administrators and only to those applications that require access. Such ~~shared secret~~ files shall be encrypted so that: |
|  |  |  | ge | Document should be updated to accommodate mobile devices, particularly with respect to browser references. | None – leave this for another day. |