* 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 have become “God and apple pie,” not only for government agencies, but have 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.
	+ Eg: 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.