Below, but not limited to, is a sampling of content extrapolated from the ANSI/NASPO IDPV_Standard_v6.2 Jan. 7 2015 and offers approaches in relation to the KBA Evaluation Performance for Remote Identity Proofing solicitation which proposes the following:

"In order to help establish a common understanding of KBA and remote identity proofing services, it is proposed that standardized approaches are developed to:

1) determine the accuracy and efficacy of KBA and remote proofing techniques. This may include requirements for the currency and validity of the information used in the proofing or the development of the KBA questions; and

2) report failure rates of KBA systems. In addition to standardizing validity criteria for data and processes used in the proofing process or KBA question development, this standard will establish reporting requirements for false acceptance, false rejections, and failure to enroll."

Scope of the IDPV Standard

This Standard provides requirements and guidance for an Identity Proofing and verification methodology, and associated privacy requirements, for identity management systems. However in deference for observations to the relevance of the IDPV standard to the KBA solicitation, out of scope exclusions are included.

Excluded from the scope are:

a) any attributes of a person or criteria that determine suitability of a person to fulfill a role, qualify for a benefit, satisfy a responsibility, or perform any kind of job or task;

b) any operational aspects associated with the acquisition or custody of evidence, personal information, admission, processing or handling of persons applying for issuance, enrollment or onboarding;

c) measurement of biometric characteristics, except as contra-indicators (additional handling of measurement of biometric characteristics is expected to be included in a future version of this standard).

d) handling of exceptions such as **failure** or inability of a person to satisfy the minimum evidence requirements. Handling of exceptions is expected to be included in a future version of this standard;

e) linking a verified identity to an Identity Credential;

f) collection, storage, and use of personally identifiable information (PII) for purposes other than proofing identity; and

g) requirements for security of remote proofing.

"Calls for Contribution" mentioned on line 379 of the Introduction, **line 954 of Section 7.6** and line 1045 of Section 8.6. The drafting committee believes these sections will benefit from additional contribution. Comments and contributions received on or before March 9, 2015 will be acknowledged by NASPO and considered by the IDPV drafting committee.

Line 954 of Section 7.6 may be an opportunity for collaborative contribution to address the KBA Solicitation purpose

"7.6 Accountability and Auditing 954

Identity proofers shall have in place appropriate methods and metrics for auditing and individual redress as well as the measurements and contra-indications that would allow entities to determine the accuracy and effectiveness of the identity proofing process developed under this standard. An assessment of accuracy and effectiveness would take into account aspects such as required audit log data, data integrity, data retention periods, transaction retention periods, and frequency and methods of redress."

7.1 Provision of Evidence

In the event that Verification Checks using evidence other than an Identity Credential (such as Knowledge Based Authentication) are selected for in-person proofing, information in the form of answers to questions may also be disclosed by the individual undergoing Identity Proofing.

Page 45

Table 9 – PII Required for Performance of Verification Checks

Personally Identifiable Information (PII) Required to be Disclosed		**Purpose of Requesting Disclosure of PII is to Enable:**
A	**Check Ref No.**	**B**
Identity and contact information of a corroborator.	V10	Cross Reference with Corroborator (Affidavit, interview, testimony, etc.).
Identity and contact information of a TRUSTED corroborator.	V11	Cross Reference with Trusted Corroborator (Affidavit, interview, testimony, etc.).
Answers to superficial questions.	V12	Interviewing of Subject (Superficial).
Answers to investigating questions.	V13	Interviewing of Subject (Investigating).
Answers to knowledge based questions.	V14	Interviewing of Subject (Using Knowledge Based Authentication).

Page 51

FRAUD Use of a fictitious or another person's identity.	where the other person is a stranger.	evidence often provided by the use of Identity Credentials stolen or obtained from the stranger. Those Identity Credentials may be altered to suit the fraudster in accordance with technique F2. above or the fraudster may alter his or her appearance or behavior to match the stereotype or known (if any) attributes of the stranger. Use of this type of imposter fraud is high risk because the fraudster is aware of an inability to answer detailed questions about the life history of the stranger. Unlike the use of a fictitious identity, the risk of getting caught posing as a stranger does not diminish with time unless the original person is dead.

Page 76

Symptoms of fraud to be detected	Any mismatch, including spelling, between previously recorded data, photographs, signatures and possible answers to challenge questions, etc., and the data, photographs, signatures, answers, etc., currently disclosed and tendered as evidence.

Page 88

Check V12	**Interviewing of Subject (Superficial)**
Definition	**Interviewing of subject** - means the process of acquiring personal data or information that is required to assert or corroborate an identity or correct an assertion or corroboration of identity. **Superficial** - means that the questions are standardized, normally not interactive and intended only to acquire missing data or evidence (specific Identity Credentials) or correct data or evidence. Not interactive means that the answer to one question will not be used to formulate a series of new previously undetermined questions aimed at assessing the veracity of the data and evidence. *Note A: Questions posed during the process of screening the eligibility of a person for issuance of an Identity Credential or enrollment into an identity management system are an example of superficial interviewing.*

Check V13	**Interviewing of Subject (Investigating)**
Definition	**Investigating** - means that the interviewing is a process of "examination for discovery" (EFD) aimed at assessing the veracity of the asserted identity and evidence provided by the subject. ***Note:*** *EFD is a highly skilled process that requires the use of trained professionals. It does not need to violate privacy principles, but can be perceived as an intrusive process. EFD questions are interactive, meaning that the answer to one question is used to formulate the next question. All questions are aimed at building or destroying the credibility of an asserted identity. The person performing EFD (unlike the person using dynamic knowledge based authentication) does not have the benefit of being in possession of life-print questions for which the correct answers are known in advance. Hence, the questions posed by the skilled EFD practitioner should enable the practitioner to be convinced that the knowledge of the subject is or is not in accordance with the life history of the asserted identity*.
General instructions	1. to perform in-person investigative interaction engage the service of persons who are skilled in the conduct of this type of interaction. 2. provide a private setting (both visual and audible) for the conduct of this check. 2. use knowledge of birth place, current address and disclosed Biographical Attributes to prepare questions that a person with these attributes should reasonably be expected to answer correctly. 3. record the existence of any mismatches between observed personal characteristics and age and appearance shown on tendered Identity Credentials. 6. record the existence of errors made in answers to questions. 7. if the results of comparison reveal mismatches in more than one Identity Credential or Biographical Attribute record that a critical combination has been detected. 8. when performing this check follow, in addition, the special instructions given below for higher IAL and remote proofing.

Check V14	**Interviewing of Subject (Using Knowledge Based Authentication)**
Definition	**Knowledge based authentication (KBA)** - uses secrets provided by a person or publicly available information about events and transactions in the life of a person to pose questions for which the answers are known in advance. ***Note:*** *There are two forms of KBA, static and dynamic. Static KBA (also known as shared secrets) poses a restricted set of questions for which the subject has already confided the answers. The challenge questions posed by financial institutions are an example of the use of static KBA. Dynamic KBA (DKBA) does not use answers supplied by the subject. DKBA typically uses factual information about important events, transactions and situations that have occurred or existed in the life of a person to pose questions (often in multiple choice format) the answers to which should be known to the person. Failure to answer all or a high proportion of those questions leads one to suspect that the person may be an imposter.*
Purpose	To verify, using dynamic knowledge based authentication (KBA) techniques, that a person is who he or she claims to be and no symptoms of imposter fraud exist) by correctly answering the required number of questions based on the IAL of the transaction.
Symptoms of fraud to be detected	Inability to answer the needed amount of questions based on risk tolerance could indicate a need to do further enhanced due diligence on the subject
General instructions	1. to perform KBA engage the service of a KBA provider or build an engine that will support dynamic question generation. 2. work with the KBA provider or internal solution to configure the setup to meet the risk level of the transaction. 3. KBA solutions can be offered via web services integrated into a user interface (website, mobile, kiosk, IVR) or provided in a hosted web application to a call center agent or other type of customer service

	representative to perform the quiz in-person or over the telephone. 4. follow a data minimization strategy and only use Biographical Attributes needed to resolve to a single identity in order to generate a KBA quiz. 5. implement the solution within your business workflow and have the subject take the quiz. 6. score the quiz to see if the questions answered result in a pass or fail based on the configuration setup of the quiz. 7. when performing the quiz, follow the special instructions given below for each IAL and remote proofing.
Special instructions for remote proofing	Limit the number of attempts in taking the quiz in a certain time period. Limit the amount of time the subject receives to take the quiz within a reasonable time period.
Detection criteria	In the event that the subject does not pass the required amount of questions, record the possible existence of a contra-indication and if possible, use other enhanced due diligence techniques such as V13, Question Subject – Investigating

Check V14	**Interviewing of Subject (Using Knowledge Based Authentication)**
Definition	**Knowledge based authentication (KBA)** - uses secrets provided by a person or publicly available information about events and transactions in the life of a person to pose questions for which the answers are known in advance. ***Note:*** *There are two forms of KBA, static and dynamic. Static KBA (also known as shared secrets) poses a restricted set of questions for which the subject has already confided the answers. The challenge questions posed by financial institutions are an example of the use of static KBA. Dynamic KBA (DKBA) does not use answers supplied by the subject. DKBA typically uses factual information about important events, transactions and situations that have occurred or existed in the life of a person to pose questions (often in multiple choice format) the answers to which should be known to the person. Failure to answer all or a high proportion of those questions leads one to suspect that the person may be an imposter.*
Purpose	To verify, using dynamic knowledge based authentication (KBA) techniques, that a person is who he or she claims to be and no symptoms of imposter fraud exist) by correctly answering the required number of questions based on the IAL of the transaction.
Symptoms of fraud to be detected	Inability to answer the needed amount of questions based on risk tolerance could indicate a need to do further enhanced due diligence on the subject
General instructions	1. to perform KBA engage the service of a KBA provider or build an engine that will support dynamic question generation. 2. work with the KBA provider or internal solution to configure the setup to meet the risk level of the transaction.

	3. KBA solutions can be offered via web services integrated into a user interface (website, mobile, kiosk, IVR) or provided in a hosted web application to a call center agent or other type of customer service representative to perform the quiz in-person or over the telephone. 4. follow a data minimization strategy and only use Biographical Attributes needed to resolve to a single identity in order to generate a KBA quiz. 5. implement the solution within your business workflow and have the subject take the quiz. 6. score the quiz to see if the questions answered result in a pass or fail based on the configuration setup of the quiz. 7. when performing the quiz, follow the special instructions given below for each IAL and remote proofing.
Special instructions for remote proofing	
	Limit the number of attempts in taking the quiz in a certain time period. Limit the amount of time the subject receives to take the quiz within a reasonable time period.
Detection criteria	In the event that the subject does not pass the required amount of questions, record the possible existence of a contra-indication and if possible, use other enhanced due diligence techniques such as V13, Question Subject – Investigating