Comments of the World Privacy Forum

To the IDPV National Standard Project

Regarding Requirements and Implementation Guidelines for Assertion, Resolution, Evidence, and Verification of Personal Identity, version 5.3.1

Sent via email to idpv_project @naspo.info and IDPV@naspo.info

North American Security Products Organization (NASPO)
204 E Street NE,
Washington, DC 20002

September 5, 2014

Re: Document No. NASPO-IDPV-066, dated June 26, 2014

Dear Members of the IDPV National Standard Project,

Thank you for the opportunity to comment on Requirements and Implementation Guidelines for Assertion, Resolution, Evidence, and Verification of Personal Identity, version 5.3.1, published on June 26 at <http://www.naspo.info/naspo-idpv-project>. We appreciate the opportunity to comment on this proposed national standard. The World Privacy Forum is a 501(c)(3) non-partisan, non-profit public interest research and consumer education group. We focus our activities on privacy issues, and much of our work focuses on technology and identity-related privacy issues. We have testified before Congress and have published significant privacy studies. You can see our publications and more information at www.worldprivacyforum.org.

We understand the impetus to create a national standard for identity verification and proofing. We have read the proposed standard carefully, and we see the need for several changes to the standard. In our comments, our intent is to help create a standard that increases security, trustworthiness of identities and identity credentials while protecting individual privacy. We do not seek to constrain the ability of Identity Proofers and Relying Parties to innovate in the creation of more reliable and trustworthy identities.

Identity thieves and fraudsters are creative and will continue to be, and those who detect fraud and protect against it should be as well. That being said, we recognize that a national standard for identity verification and proofing is important, but it must strike a better balance between the need for fraud detection and privacy protection for individuals

who have done nothing to merit suspicion and scrutiny. The impact of an imbalance in the standard would have deleterious consequences for consumers by permitting or encouraging extensive collection of personal information that can, in itself, act as attractive targets for fraudsters. In the end, if the standard does not strike a fair balance, one risk is that it will be tagged as anti-privacy and anti-consumer, and the entire effort could fail.

Following are our recommendations based on our analysis of version 5.3.1 of the standard. We have written our comments in narrative format, below, and request these be considered. We have also submitted a summary of the comments on the IDPV form.

I. Identity Assurance Levels need to be better defined

The proposed standard does not provide any linkage between Identity Assurance Levels (hereafter IAL), how the identity might be used, and what evidence would provide appropriate assurance for the intended use. Instead, the proposed standard uses vague terms such as "little or no confidence," "some confidence," "high confidence" and "very high confidence."[1] These terms are not appropriate for use in a precise standard.

Other national efforts addressed this issue with more precision. For example, the UK Good Practice Guidelines for identity proofing individuals state that identities verified to Level 2 may be used in civil proceedings; identities verified to Level 3 may be used in criminal proceedings.[2]

New Zealand defined three components for establishing an identity, as follows:

- *"Evidence that the claimed identity is valid* – i.e. that the person was born and, if so, that the owner of that identity is still alive

- *Evidence that the presenter links to the claimed identity* – i.e. that the person claiming the identity is who they say they are and that they are the only claimant of the identity

- *Evidence that the presenter uses the claimed identity* – i.e. that the claimant is operating under this identity within the community".[3]

Though differing in their approaches, both the UK and New Zealand clearly define and thereby carefully limit the purposes of collecting and verifying evidence of identity.

---

[1] NASPO-IDPV-066, June 26, 2014, p3, p. 17.

[2] CESG National Technical Authority for Information Assurance and Cabinet Office, Government Digital Service, "Identity Proofing and Verification of an Individual," Good Practice Guide No. 45, Issue Number 2.2, December 2013, p. 11.

[3] Department of Internal Affairs, "Evidence of Identity Standard," Section 5.2, Core Concepts for Establishing Identity, available at http://www.dia.govt.nz/EOI/EOIv2Part3-Sections5-6.html.

In contrast, the NASPO proposed standard leaves the determinations of identity-related risks and decisions about highest-priority types of identity fraud entirely up to the Relying Parties. Even though Appendix D1 provides guidance for selecting IALs based on a risk analysis, it provides no guidance on how Relying Parties should trade off risks to different parties in the identity verification transaction, including individuals being identity proofed.

We agree that it makes sense to allow Relying Parties to determine which identities they will accept, including the determination of the types of identity fraud that they most commonly encounter and need to prevent. Nevertheless, some issues remain to be addressed in the standard.

Foremost among these issues is that leaving the IAL levels vague could drive Relying Parties to higher-level credentials than they really need. Additionally, vague definitions of IALs could provide incentives to Identity Proofers to collect as much information about individuals as possible in order to be able to serve as many different Relying Parties as possible with as many different IAL definitions and verification enhancements as possible. As currently written, the Data Minimization requirement, Section 8.4, does not address this issue.[4]

Footnote 16 of the IDP/V Standard v. 5.3 notes that "Identity Proofers or other entities should perform and document a risk analysis before selecting proofing enhancements that lead to additional collection of personal information or evidence." An elegant solution to the weakness in the standard as currently written would be to move the section on performance and documentation of a risk analysis for verification checks out of the footnote and add it to Section 8.4, Data Minimization, as a mandatory requirement for compliance with the standard.

It is essential to the underlying wholeness of the standard that the IAL levels should be well defined, and that compliance with Fair Information Practice Principles (FIPPs) be mandatory in all aspects of the proofing process. Over the long term, imprecision in this area could lead to substantial over collection and widen the door for potential abuse of consumer information.

II. The Standard needs to offer evidence that different options offer equivalent levels of assurance and fraud protection

The standard as currently proposed contains several sections where multiple options are made available. We are concerned about the significant lack of evidence for using this approach. A standard must be based on objectively reliable evidence. What specific and relevant evidence demonstrates that exercising different options, alone or in combination, produces an equivalent level of assurance and fraud detection?

According to the Foreword and Note 7 at line 866, the equivalences were based on

[4] NASPO-IDPV-066, June 26, 2014, Section 8.4 Data Minimization.

"expert opinions of a small group of experts." What are the qualifications of the experts? Was a scientifically validated method, such as the Delphi method, used to collect and aggregate their opinions?

We will walk you through one exemplar of the problems with the standard as currently proposed.

Example for IAL 3

For IAL 3, the current proposal reads:

Option B
either V2 or V3; and
either V6, V7, V8, V13 or V14; and
either V15, V16, V17 or V18.

What is the evidence-based support for the contention that a combination of V2+V6+V15 is equivalent in providing assurance and fraud detection to V2+V7+V15 or any other possible combination of the verification checks on this list?

This issue affects several parts of the standard.

- Multiple options for evidence that can be presented to support a claim of identity. Do different combinations of evidence items produce an equivalent level of support for claimed identity at the stated IAL?

- Multiple sets of verification checks available at each IAL, with some verification checks applicable only if a specific type of evidence is presented. Does the use of different combinations of verification checks produce the same level of confidence in the identity and the same level of fraud detection?

- Different strength weightings are attached to different contraindications. What is the evidence for the weightings and for the "critical combinations"?

There should be a methodologically valid study to determine equivalence of different options whenever multiple options exist. The study needs to be public and methodologically transparent. NASPO should issue a call for the research community to suggest appropriate methodologies for conducting such a study. There should also be a schedule for repeating the study, e.g., every three years, to account for the evolution of technology and experience with the use of the standard.

III. The Data Minimization principle needs to apply not only to the initial set of attributes used to identify individuals, but to all parts of the proofing process

As written, the standard claims to adhere to the Data Minimization principle while permitting a great deal of data, including a full "biographical footprint," to be collected, retained, accessed and analyzed.

The standard needs to put greater and more carefully thought-through and managed restrictions on data collection in order for Identity Proofers to comply with the Data Minimization principle. The authoring committee performed a study to minimize data required to uniquely identify individuals.[5] However, much additional data is collected as evidence and as part of verification checks. Such additional collection is either tacitly assumed or actively encouraged throughout the standard, and there is no evidence that any effort was made to minimize or even restrict such collection.

The fact is that documents collected as part of evidence of identity contain more than just the attributes being verified, but the standard places no limitation on collection and retention of **all** the information in the evidence by the Identity Proofer. In fact, the standard goes even further by encouraging identity proofers to *look beyond* the evidence collected under the standard.

Line 710 states that:

> "[t]he elements required to uniquely resolve an identity can be used to examine the individual's "biographical footprint," which would indicate whether the identity is real, synthetic, or requires additional scrutiny. Additional data would also provide a means by which contra-indications can be identified."

We acknowledge that some additional data collection and retention may be necessary in some situations. For example, driver's license number, date and state of issuance form a part of documentation for using the driver's license to verify asserted name and date of birth. There are also cases where comprehensive data collection is helpful, e.g., to identify synthetic or fraudulent identities that spring full-blown from nowhere.

However, as written, the Standard claims to adhere to the Data Minimization principle while it in reality does not, because it in no way limits collection and retention of data after the individual has been identified.

We have some suggestions to resolve this issue. One possible approach is for the Identity Proofer to collect data only to the extent that it is necessary to verify asserted attribute(s) and to retain only the data necessary to record the transaction, i.e., the asserted attribute(s), the evidence used to verify it, and the outcome of the evidence check.

---

[5] "Establishment of Core Identity Attribute Sets & Supplemental Identity Attributes," Report of the IDPV Identity Resolution Project, NASPO-IDPV-060, February 14, 2014 available for download at http://www.naspo.info/naspo-idpv-project.

Collection or retention of any additional data, including "biographical footprint" should take place only when there are clear indications of fraud, and these indications should be recorded together with an analysis of how the additional data or evidence requested or collected would resolve the questions raised by the initial verification, and the outcome of the additional verification. The additional data should not be retained longer than the next cycle of identity verification.

Thank you for the opportunity to comment on this important proposal. If you have any questions regarding our comments and suggestions, or would like to discuss this further with us, please contact us at 760-712-4281.

Respectfully submitted,

Pam Dixon
Executive Director, World Privacy Forum