

Prepared by:
Lisa Kimball, Chairperson, Virginia Identity Management Standards Advisory Council (IMSAC)
January 25, 2018
Amended February 1, 2018

TALKING POINTS: HOUSE BILL NO. 1269

General Background

- Identity can generally be thought of as a collection of attributes (identifying information) that describe a subject (e.g., an individual, device, or other legal entity)
 - 'Subject' applies to both human and non-person entities
 - Examples of attributes include height, age, date of birth, IP address, industry, business state, etc.
- Identity is the foundation of various transactions – that is, a subject must have certain attributes in order to participate in a transaction (e.g., an individual must provide proof of residency in a particular district in order to register to vote in that district)
- Digital identity is merely the online persona or unique representation of a subject engaged in an online transaction

Digital Identity Management Standards

- Identity management generally refers to the process for proofing, authenticating, and verifying a subject's identity
- Various entities are involved in identity management, including attribute providers, identity providers, and identity proofers
- The Identity Management Standards Advisory Council (IMSAC) recommends technical and data standards regarding verification and authentication of identity in digital and online transactions – that is, digital identity management standards
- IMSAC has developed digital identity management standards to address topics such as enrollment in digital identity systems, identity proofing, the issuance of digital identity credentials, assertions of digital identity credentials in online transactions, authentication of digital identity credentials, and verification of asserted identities
- Much like other areas, issues of liability arise in identity transactions when someone suffers a loss
 - In the absence of identity-specific rules governing liability, if someone suffered a loss and sued, a court would likely find some basis under general laws (e.g., contract, tort, privacy, warranty) to allocate liability
 - This uncertainty regarding liability is a barrier to entry for many potential identity providers
 - In that regard, the Electronic Identity Management Act (Act) adopts a standards-based identity specific rule on liability – that is, an identity provider that complies with applicable standards (including the standards developed by IMSAC) would have a safe harbor from liability, while identity providers do not comply with such standards would bear the liability risk
 - The Act was presumably intended to encourage identity providers to establish operations in the Commonwealth

HB1269

- In its present form, the Act only anticipates non-federated systems – that is, a digital identity system where a user may only use its digital identity credential to verify its identity with the entity that issued the credential
 - For example, a user goes to their bank's website, verifies their identity, and receives a digital identity credential (e.g., a user name and password) – in the future, the user may present that credential to their bank to prove their identity – but the user could not

- successfully present that credential to a different digital identity system (e.g., a different bank or a credit card company) to prove their identity
- HB1269 amends the Act to accommodate federated digital identity systems – that is, a process whereby a user can present a digital identity credential issued by one digital identity system to a second digital identity system to prove the user’s identity
 - The importance of federation is illustrated by the following example:
 - Amazon offers two payment cards: (1) the Amazon Prime Store Card that can be used exclusively at Amazon.com (“Store Card”), and (2) the Amazon Prime Rewards Visa Card that can be used at any retailer who is part of the Visa network (“Credit Card”).
 - By analogy, an identity credential (“IdC”) in a non-federated digital identity system is like the Store Card (i.e., can only be used to prove identity to the issuer), but an IdC in a federated digital identity system is like the Credit Card (i.e., can be used to prove identity to both issuer and other in-network entities).
 - If passed, HB1269 would allow IMSAC to pass digital identity management standards to govern the passing of authentication and verification information between discrete digital identity systems

Additional Information (1 February 2018):

- The Electronic Identity Management Act (Act), specifically § 59.1-552, currently both establishes and limits an identity provider’s liability for the issuance of an identity credential – compliance with IMSAC standards is one of several considerations
- The initial purpose of the Act is to foster the growth of the Commonwealth’s digital economy by providing incentives for various entities involved in the identity ecosystem to establish operations in the Commonwealth; the Act does not mandate compliance with any particular standards (IMSAC, NIST, or otherwise)
- IMSAC is currently considering a requirement that a third-party certification authority must certify that a digital identity system complies with IMSAC standards — the goal of this requirement is merely to establish/encourage public trust in the digital identity system
- The guidance documents recommended by IMSAC and adopted by the Secretary of Technology (for now) are not regulations adopted pursuant to the Administrative Process Act or Commonwealth of Virginia Information Technology Resource Management Policies, Standards, and Guidelines adopted pursuant to § 2.2-2007.
 - **A court will ultimately decide whether an identity provider is eligible for the limitation of liability under the Act**
 - That is, even where a third-party certification authority certifies that a digital identity system complies with IMSAC standards, a court could find an identity provider liable if the court finds non-compliance with IMSAC standards