

Support State Role in Identity Management and Verification Solutions

Federal, state, local, and tribal governments currently issue numerous credentials to constituents for access to facilities or services based on a variety of endorsements. Many of the endorsements provide citizens with access to federally funded programs, but the issuance of credentials remains program-specific and has become a redundant process for many agencies and departments. In an effort to reduce risk and achieve compliance of government directives, robust and interoperable trust frameworks for identity and access management are needed. By issuing a virtual or digital identity that has multi-platform credentialing options, it will result in improved efficiency and convenience for both users and issuers. To the extent such credential is honored by commercial entities, it will also improve efficiency and security of commercial transactions, including on-line transactions.

Both the state and federal government have compelling reasons to support a national ecosystem of identity management. These include:

- Identity management is a critical cross boundary activity
- A standards-based architecture to facilitate interoperability
- Need for a uniformly accepted electronic identity approach necessary to support online transactions, licensing, eligibility, benefits enrollment, registration, etc.
- Cost reduction and business efficiency - paper and outmoded processes which waste time, energy and money
- Potential for reducing improper payments, fraud, waste and abuse with an enterprise approach to digital identity
- Citizen inconvenience and frustration with managing multiple credentials

In order for states to improve program integrity, reduce costs, streamline access, prevent fraud and curtail identity theft, effective policies must enable trust across organizational, operational, physical, and network boundaries. The resulting framework will promote data security, privacy, and the high assurance authentication needed to secure information sharing and transparency in government. Guidance on the approach to identity management will encourage a shift away from stove-piped applications to an enterprise view of identity that enables use without creating redundant sources that are difficult to protect and keep current.

With more states moving services online, NASCIO supports the [National Strategy for Trusted Identities in Cyberspace \(NSTIC\)](#) that would create a voluntary identity ecosystem to make online transactions more secure, private, and more convenient. NSTIC would promote privacy-enhancing technologies. NSTIC offers a vision of the future where the private sector, civil societies, and the public sector collaborate to create the standards and policies needed for interoperable trusted credentials that would reduce identity theft and fraud.

Recommendation:

With greater need for cross-boundary collaboration and program integrity, state governments need to leverage the existing federal initiatives on digital identity management and credentialing. Federal agencies need to coordinate with states and work toward a federated type solution that is standards based and competitively sourced to ensure interoperability across governments.

NASCIO supports the vision of NSTIC and requests that states be included in the governance structure and be considered for pilot projects to explore creating interoperable credentials, streamline business process and protect personal information in our when conducting transactions online.

For more information contact:

Pamela Richardson Walker
Director of Government Affairs
NASCIO
Hall of States
444 North Capitol Street NW, Suite 642
Washington, D.C. 20001-1511
P: (202) 624-8477
F: (202) 624-7745
C: (202) 215-2015
E: pwalker@AMRms.com
W: www.nascio.org