Building Constituent Trust:
A Better Way to Implement Identity and Access Management

Virtualized services will only grow more important in the future.
Three of NASICO's 2021 State CIO Top 10 Priorities[1] were:

- ✓ **Digital Services**
- ✓ **Cloud Services**
- ✓ **Identity and Access Management (IAM)**

To protect constituent data, government organizations rely on IAM and authentication.

83% of digital constituent service applications require some form of authentication to verify user credentials[2]

When considering IAM tools, state and local government organizations traditionally faced a tough choice:
Build it yourself or buy it off the shelf from a third-party vendor?

Here's what to know with each of those options:

Build It

Why It's Smart
- Customized to meet the exact needs of your organization
- Ownership of data, product features and roadmap

What to Keep in Mind
- Will take months or years to develop in-house
- Your team must keep up with shifting cyber threats, along with emerging compliance and privacy requirements
- You assume internal risk management for waste, fraud and abuse
- Difficult to retain institutional knowledge when CIOs and other IT leaders leave or retire
- Hard to meet evolving needs on regulation and certification requirements

Buy It

Why It's Smart
- Easy to implement in a matter of days
- Fast, reliable, 24/7 support from cybersecurity experts

What to Keep in Mind
- Can be difficult to customize many off-the-shelf applications for government agencies
- Unique requirements of different public agencies can result in siloed identity engines for every application and a frustrating user experience
- Difficult to pivot in future as needs change (vendor lock-in)
- Inadequate feature set or roadmap to meet current and future requirements

Fortunately, modern government organizations don't have to choose whether to build or buy. They can do both.

Partnering with a vendor for an identity-as-a-service (IDaaS) solution combines the benefits of building in-house with the strengths of buying off the shelf.
IDaaS offers:

- **Rapid speed-to-service:** Implement IAM within weeks instead of months or years.
- **Custom-built application:** Meet the needs of multiple agencies, ensuring a single sign-on experience for constituents.
- **Flexible deployment:** Choose to deploy in a fully managed public or private cloud to eliminate costly maintenance.
- **Extensibility:** Further customize and scale as your future requirements change.
- **Best-in-class security features:** Protect against data breaches and comply with standards such as OIDC, SAML, OAuth2.0, and WS-Federation and certifications like OpenID Connect, SOC 2 and HIPAA.

Government organizations should look for an IDaaS solution that is:

- Highly customizable and agile
- Simple enough for your developers to adapt
- Extensible and flexible for future needs
- Backed by a customer support team, including security experts, ready to help with any problem 24/7

[1] https://www.nascio.org/resource-center/resources/state-cio-top-ten-policy-and-technology-priorities-for-2021/
[2] https://papers.govtech.com/Enhancing-Digital-Citizen-Services-through-Identity-and-Access-Management-139544.html