Identity & Access Management is Key to Digitization of Government

A ROADMAP FOR SUCCESS

By Mike Wons, *Civix Government President*

It's plain to see, with more than 93% of American adults using the internet, and over half of all government transactions taking place online, that we are in an unprecedented era of connectivity. Additionally, the COVID-19 pandemic accelerated trends to embrace technology, especially the digitization of government – whereby states are leveraging technology to be more responsive to their constituents and provide services online. This digitization of government leads to a host of economic and social advantages for states. It enables frictionless experiences, heightened productivity, increased efficiency, and lower costs for all involved. Yet, a new set of challenges has emerged because information about people is more widely available online and it is much easier for bad actors to crack passwords and compromise user credentials. And once they have access, bad actors can wreak havoc. Thus, while our nation's Secretaries of State must continue digitization, it is essential that they incorporate a robust Identity and Access Management (IAM) program to prevent bad actors from accessing applications, systems, and networks.

The stakes are especially high for Secretaries of State and Lieutenant Governors, considering their leading roles in business services and elections. With the protection provided by IAM, states can reap the benefits of digitization while mitigating risks.

1. UNDERSTANDING IAM

To fully appreciate the significance of IAM, it is important to have a general understanding of what it is and how it works. IAM encompasses the identification, authentication, and authorization of individuals to have access to resources.

The initial function of an IAM, identification, relies on "Identity Assurance," which is met when it is determined that an applicant is who they claim to be. If the applicant meets this threshold, then they become a registered user with login credentials. Authentication relies on additional

data that is difficult to produce, except by that specific user, to re-enter the system with their login credentials. This additional data falls under the category of "what you know." For example, applicants could be asked to select the correct answer from multiple choice questions such as, "which of the following addresses have you been affiliated with?" or "what was the color, make, and model of your automobile in 2010?"

2. THE CASE FOR RANDOMIZED MULTIFACTOR AUTHENTICATION

Protecting personal information with "what you know" is no longer good enough because so much of that information is accessible online. Combining "what you know" (like PIN numbers) with "what you have" (like smartcards or tokens) provides another layer of protection. Still another layer is "what you are," which is provided through biometrics – an area where much government technology is headed.

Requiring a user to provide two or more verification factors (e.g., "what you know" and "what you have") to gain access to a resource is known as multifactor authentication (MFA). This is an important component of any security program because it requires users to identify themselves by more than a username and password (credentials that are easily compromised).

While most in the public sector rely on MFA, state and government officials should consider taking the extra step to incorporate randomized multifactor authentication. Through this model, the forms of identity assurance and authentication are randomized based on factors such as the applicant's location, the point in time, the level of sensitivity, and even the applicant's identity score (described below), among others. The fact that the pattern of questions cannot be predicted is the basis for its success.

3. DESIGNING AN IAM ROADMAP

To achieve IAM, federal agencies look to the Digital Identity Guidelines issued by the National Institute of Standards and Technology (NIST). While sates should aim to comply with the NIST guidelines, each is able to make its own decisions on IAM. Largely, state and government officials should weigh how easy they want processes to be for users against the levels of IAM they want to achieve. Each state must strike its own balance between these two competing priorities.

This can be facilitated through a multi-step process: (1) determine the assurance level requirement and (2) identify the authentication options that will meet the assurance level requirement determined in the first step.

Regarding the first step, different functions will necessitate different levels. For example, unlike government business services, where agencies may want to fend off attacks from the get-go, election officials must aim to make voting processes as accessible as possible.

When it comes to easy access, advances in technology and the volumes of information available work in our favor. For example, modern technology can prevent fraudulent online voter

registration by identifying suspicious voter applications and providing state officials with a real-time identity score that gives an insight into suspicious patterns. Various risk-based authentication tools calculate identity scores from the information entered by the registering voter. Election officials can use these scores to help determine whether the registering voter is who they claim to be.

Regarding step two, identifying authentication options, this has been one of the major barriers standing in the way of public sector IAM. But that has changed with access to modern technologies and definitive sources of data.

4. BRIDGING THE IAM GAP

Most people are familiar with IAM processes from routine online experiences, such as banking, shopping, or subscribing to a service. To login, individuals are required to have a username, password, and oftentimes, click a link, enter a code, upload a government ID, or answer a security question. While widely used in the private sector, IAM processes are generally lacking in the public sector when it comes to public-facing systems. That no longer must be the case because existing technology and data banks that make IAM more attainable than ever for government agencies, including secretaries of state.

We don't have to look far for an example of this. Recently, one of our Secretary of State clients detected a spate of fraudulent business filings. The IAM was validating the bad actor's name and home address, and she was able to access the state business services system. In response, the state wanted to beef up its IAM, but it did not want the processes to be overly burdensome on users. The state was firmly against requesting Social Security Numbers and asking challenge questions. To meet the state's needs, a feature was added to capture user cell phone numbers - through which one-time passcodes are provided. Once the passcode is validated, then the account can be created. This is a simple solution that was easy to integrate into the state's existing security pro-gram, quickly and affordably.

While it may seem daunting, the fact is that states can tap into existing technology and data to achieve a high level of IAM easily, quickly, and affordably and conform with NIST guidelines. Tapping into definitive sources of data, such as those provided by Equifax and Experian, allows govern-ments to rapidly authenticate the identity of applicants. And with modular technology, the solu-tions can be quickly and seamlessly integrated with virtually any existing or third-party system.

ABOUT THE AUTHOR

MIKE WONS, CIVIX GOVERNMENT PRESIDENT

Wons leads all aspects of the 200+ person Government business unit team, from strategy to execution to growth and expansion with one focus in mind: helping make the complexity of government simple, modern, and secure. This includes delivering the industry's best software and business process solutions through an aggressively expanding portfolio of advanced digital products. Mike has over 30 years of GovTech expertise serving in General Manager, President, CEO and Chief Client Officer roles in addition to serving as the first statewide CTO for the State of Illinois.

For more information, visit gocivix.com or contact solutions@gocivix.com and 888-GOC1V1X.