4 Priorities for Effective Identity Management

The term "critical infrastructure" evokes images of power lines and water treatment facilities, but it also applies to the identity management platforms that protect networks from cyber intrusion.

At a recent GovLoop virtual event, "**Access Denied: How to Improve Your Agency's Identity Management**," Steve Caimi, Director of US Public Sector Solutions Marketing with Okta — a firm that provides identity management solutions — and Joey Barkley, Okta Federal's Senior Solutions Engineer, spoke about four priorities that public sector organizations should consider when managing identities across their networks.

Here are takeaways from their discussion.

Priority 1 – Modernize...

1

IT and adopt the cloud

IT modernization is on the to-do list of almost every government organization. In terms of identity management, that means moving away from identity siloes and embracing the cloud to ensure secure, seamless experiences across apps and portals, said Caimi and Barkley.

There should be a **single frictionless login, centralized administration, and low/no-code options** that allow for fast, simple integrations. And, among other modernization concerns, legacy systems need on-premises and other support — since most agencies will keep their legacy tech, at least for a while.

"For the time that we implemented [legacy] solutions, they were absolutely valid and served a need," said Barkley. "But then we started to adopt newer technologies that were cloud-based... Now the identity solutions that we implemented years and years ago don't mesh well with the new, modern way we're doing things. We've got to keep pushing the envelope."

Priority 2 – Strengthen...

Cyber posture and maintain compliance

In May 2021, the White House issued a cybersecurity executive order that charged federal agencies with modernizing their IT, moving toward a zero-trust architecture, and adopting secure cloud services. Within a few months, the Cybersecurity and Infrastructure Security Agency released its Zero Trust Maturity Model to give organizations specific zero-trust guidance, Caimi noted.

And the first of the maturity model's five pillars, he said, is Identity — specifically, ensuring and enforcing that "**the right users and entities have the right access to the right resources at the right time**." Rather than building firewalls and assuming that "all the bad stuff is on the outside," zero trust assumes that every network, whether internal or external, cannot be trusted, he said.

Barkley agreed. "The reality," he explained, "is that if we stay in the past with our identity solutions, they're going to become less and less secure over time, and we need, as practitioners, to be able to ... adopt the newer, [more] secure technologies available to us."

Priority 3 – Achieve...
Digital service excellence

Organizations are improving their abilities to provide digital services, but Barkley and Caimi said there's a long way to go. A December 2021 executive order ("Transforming Federal Customer Experience and Service Delivery to Rebuild Trust in Government") made that clear, they said.

Caimi explained: Officials "are basically saying, 'Federal agencies, as you interact with the American people, you need to redesign your applications so they're **not only simple to use, but they're accessible to everybody, no matter their skill level.**'" The services also should be equitable, protective, transparent, responsive, efficient and effective, he said.

Login.gov — a secure sign-in portal that people can use to access participating agency systems, such as the Social Security Administration's — is one example in which Okta can help, Caimi and Barkley noted. That is, Okta's identity platform can help agencies integrate login.gov with their own systems and ensure a better digital experience for their employees, contractors and constituents.

Priority 4 – Prevent...
Identity theft and fraud

There are many reasons for identity theft and fraud, but whenever there are significant pools of money, especially for public benefits, there is bound to be identity theft, said Caimi.

He highlighted recent targets of public-sector identity fraud, including Pandemic Unemployment Assistance and the pandemic-era Paycheck Protection Program, as well as Medicaid, the Supplemental Nutrition Assistance Program and the Temporary Assistance for Needy Families, among other entities.

To combat this cybercrime, Barkley and Caimi stressed the importance of **phishing-resistant, multi-factor authentication requirements**, so people need more than a username and password to log in.

"The message here is you have to establish identity and then you have to be able to authenticate that user, once the identity has been established," Barkley said. You need to tie those functions in, and "that's where the rubber really meets the road."

For more information on Okta's identity management solutions, visit okta.com.