

Cloud, Mobility and Security

Identity, access management are critical to securing the enterprise

As agencies move to the cloud in support of mobile workforces, access management and identity are moving to the forefront of efforts to secure their enterprise.

New mobile, cloud and “as-a-service” offerings have made it more difficult for agencies to protect their data. Shoring up perimeter security doesn’t protect global enterprises.

Agencies must be smarter in their approach to identity, credential and access management (ICAM). They need a better way to manage and secure users, applications and services used by customers in an evolving and expanding enterprise.

Identity—not the network—is the new secure point because “the network perimeter is starting to disappear,” said Ted Girard, vice president, Public Sector at Okta. Data in multiple locations is difficult to manage and protect. “Identity becomes the critical control point and that is the basis of the zero trust framework.”

Digital transformation allows agencies to extend their reach and more easily talk with citizens and partner agencies; identity is crucial to connecting them, Girard said. It “has to be a part of every single conversation because it is the center point of connecting all these different users and technologies.”

Often people “are conditioned from an ICAM perspective that these are complex, difficult projects that take a long time,” Girard said. However, cloud-based identity solutions move very quickly, offer users a “frictionless experience,” and help accelerate other digital transformation projects.



Buy-in from senior leadership is essential for success, even for small projects. Starting with a small pilot to get quick wins can build support. “Getting quick wins helps change the mindset and culture of the organization,” he said.

The discipline of ICAM is always evolving to reflect changing agency technology, culture and missions, said LaChelle LeVan, acting director, federal identity, Credential and Access Management (FICAM)

Program Office, at GSA. “There is never a time when it is actually done,” she said. “You have to be adaptable.”

Agencies should approach identity and access management from different perspectives, depending on mission and who they are sharing their data with. Identity and access management cut across multiple disciplines, and even small projects must fit into an overall enterprise strategy, she said.

“It takes a cross-cutting discipline,” LeVan said.

If an agency is just beginning, it should get stakeholders and mission owners at the table to understand the challenges, mission needs and priorities that will inform decisions. Although there may be many solutions, there has to be one overarching mindset.

An agency should share talent; ensure that their privacy, governance and compliancy issues are being addressed; focus on identity lifecycle management and reconsider how they evaluate risk, she said.

“We don’t want to duplicate cost. We don’t want to duplicate effort,” LeVan said.

“Identity... has to be a part of every single conversation because it is the center point of connecting all these different users and technologies.”

– TED GIRARD, VICE PRESIDENT, PUBLIC SECTOR OKTA