IDENTITY takes center stage to help feds modernize IT security

White House and NIST guidelines — and the rise of Identity API Platforms — give agencies more flexible, less costly approaches to managing identity and access.

By FedScoop Staff

It wasn't that long ago that perimeter-based security controls provided the bulk of an agency's IT defenses. That era — like the perimeters themselves — has all but dissolved as self-contained enterprise network environments have given way to the cloud, mobile platforms and interconnected application services.

However, what's also changed for government agency executives and their IT departments are the federal identity, credential and access management (ICAM) requirements agencies must now meet in today's sprawling IT ecosystem.

Those requirements, formalized in a May 21, 2019, White House Office of Management and Budget memorandum (M-19-17), go well beyond updating the ways agencies must manage and monitor how employees, contractors and the public securely accesses government IT systems and services. They also make clear that agency executives — including CFOs, top operating and contracting officers as well as IT teams — are all now responsible for ensuring their agency :

- **Improves digital interactions** with the public leveraging ICAM technologies.
- **Supports cross-government identity** federation and interoperability.
- **Creates a single comprehensive ICAM** policy, process and technology solution roadmap.
- **Shifts its security focus** beyond perimeter controls and making identity "the underpinning" for managing risks posed by users and information systems accessing federal resources.

From an agency point of view, "The memo has provided more teeth to require accountability," observed David Trzcinski, branch chief for security policy and compliance in the CIO office at the Small Business Administration. "Everyone has responsibility and is put on notice that this is a requirement, whether you're talking about your internal users or about your public citizen users."

The upshot for citizens, added SBA Chief Technology Officer Sanjay Gupta during a FedScoop interview, is the increased support the memo provides for streamlining identity authentication portals for SBA users. It will also help accelerate efforts already underway to "deploy a single gateway into SBA so a citizen only needs to create one identity across the different programs that they are interacting with at the SBA," he said.

A MORE MODERN APPROACH

Gupta, however, also underscored the memo's underlying importance. "It reconfirmed our expectations and goals to modernize our IT portfolio and improve the user experience both externally and internally." And it established more modern and common sense approaches to identity and access management, he said, such as federating identity credentials across the government.

"One of the common issues we face is onboarding people — federal staff as well as contract staff — sometimes for just 90 day pilot initiatives," he explained. The process of making individuals with existing federal credentials at, say, the Department of Homeland Security (DHS), "go through the same rigamarole to authorize them access to [SBA] information systems, facilities and security areas — we waste a lot of money and time in this process." That's not to mention terminating accounts when contractors or employees leave. "Imagine the amount of productivity drag all this causes," he said.

Federal IT experts, including David M. Temoshok, at the National Institute of Standards and Technology (NIST), and Jamie Danker, a former DHS directorate privacy director now at Easy Dynamics Corp, each agreed there's a lot to like about the new ICAM guidelines. The memo not only lays out clear support and authority for interagency federation of authentication processes, but also gives agencies needed flexibility for getting there.

"Agencies can give the public more options and allow them to bring non-government furnished authenticators to their digital identity when they access digital services," said Danker. "This policy enables strong authentication to government services, reduces cost, and reduces the number of authenticators individuals use in their daily lives," she said, calling it a "win-win for agencies and citizens."

Temoshok, a senior policy advisor for applied cyber security at NIST's Information Technology Laboratory, concurred, noting that "M-19-17 gives very clear support and direction to federate authentication processes — both to PIV (personal identity verification) as well as [public forms of] authentication and access control where that makes sense."

> ***"Unlike putting in an intrusion detection system, IAM projects involve people, technology and business process. So organizational change management is critical."***
>
> - Michael Wyatt, *Deloitte*

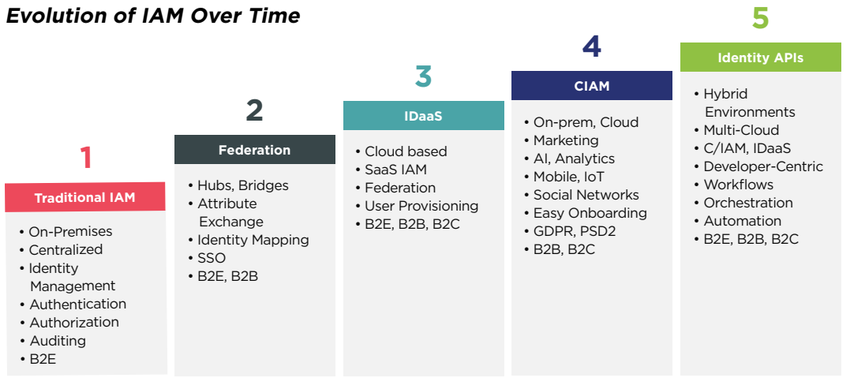
Perhaps of greater importance, he suggested: The OMB policy memo "rescinded some previous (security assurance) policies that had become out of date" and "paid particular attention to digital risk management processes — elevating the posture of ICAM controls and ICAM risk management within the structure of overall agency risk management," he said. Agencies will also benefit, he said, from requirements that their identity strategies align with industry-accepted practices codified in NIST's suite of "Digital Identity Guidelines" (SP 800-63-3).

THE NEW AGE OF ICAM APIS

Fortunately for agencies, the tools for managing and federating identity and access management have evolved significantly from the days when ICAM mostly relied on siloed identity gateways managed and stored on-premises.

The advent of platforms that use APIs designed expressly around IAM now make it possible for agencies to manage

Evolution of IAM Over Time



Source: KuppingerCole Analysts

identity and access controls that can span across on-premises systems, the cloud, and even multi-cloud environments. They also enable agencies to centrally support the different functional requirements of IAM, federation, ID-as-a-Service and customer-based IAM as well as various workflows and orchestration needs.

The emergence of "Identity API Platforms" has in fact, grown into a whole new market segment, according to Richard Hill at KuppingerCole Analysts, an independent information security and risk management analyst organization headquartered in Europe.

These new API capabilities are making it vastly easier — and less costly — for agencies and their developers to improve the onboarding and user experience for citizens and employees, with single sign-on and identity provisioning in addition to making systems more secure.

IT MODERNIZATION POWERED BY IDENTITY

Michael Wyatt, national managing principal for identity solutions at Deloitte, saw those capabilities unfold firsthand working with the State of Texas, which serves 29 million citizens. Faced with the pressing need to modernize its IT systems, state officials and Deloitte recognized an opportunity to also overhaul a byzantine collection of online services — and create a single statewide portal where citizens could seamlessly register and sign in once to whatever applications were needed behind the scenes to accomplish their tasks.

The need for a centrally deployed ICAM platform that could connect to existing applications using APIs became obvious, said Wyatt; and so did the challenges.

"Unlike putting in an intrusion detection system, identity management projects involve people, technology and business process," he said. "A good example of this is the challenge of information sharing across agencies. The fact that people are involved means that organizational change management is critical. Another challenge is sunk cost. Agencies have spent a lot of money to stand up on-premises enterprise systems."

However, the success of a pilot project, using an open source ICAM system from ForgeRock and APIs to interface with an existing state service, demonstrated to state officials that a central IAM platform could improve citizen services. Deloitte project leaders report it took just two months to connect the first agency service application and the ICAM platform to the new Texas.gov portal, with subsequent connections picking up speed.

> ***"Instead of protecting just the front door, you're protecting every object behind the door individually."***
>
> - Ashley Stevenson, ForgeRock

Dave Fletcher, chief technology officer for the State of Utah, faced an even steeper challenge, trying to migrate more than 1,400 online services and legacy applications into a consolidated IT environment. That led Fletcher to embark two years ago on a sweeping deployment of a centralized access management platform from ForgeRock that could meet a number of needs.

"We have a lot of federal partners as well as federal data that has requirements that we have to ensure meet a certain level of security," Fletcher said in a recent interview. "So, we wanted to make sure we had the ability to implement various types of authentication and authorization." He also needed a way to give state employees more consistent user data across departments, such as connecting social services data across state agencies using APIs.

> ***"The emergence of Identity API Platforms has grown into a whole new market segment."***
>
> - Richard Hill, KuppingerCole Analysts

Since initiating the conversion process, "We've tied over 900 services and applications to the ForgeRock identity platform," Fletcher said, adding that Utah's IAM consolidation move will help save the state $15 million in reduced IT operating costs.

ENABLING GRANULAR SECURITY CONTROLS

Perhaps the most important benefit, however, of investing in more modern and agile ICAM platforms — beyond lower costs and improved user experience — is the increased control and security it provides.

"Modern IAM platforms make it easier for agencies to establish IT environments that can support continuous authentication, or continuous authorization — giving you protection beyond the perimeter," said Ashley Stevenson, formerly chief architect for ICAM at the DHS and now vice president for product and solution marketing at ForgeRock.

"The government has focused for a long time on HSPD-12 security credentials, and they still play a central role in the new OMB guidelines. But today's ICAM solutions allow you to authenticate users beyond a level of credential assurance; expanding to include numerous dynamic inputs to achieve intelligent risk assessment. Instead of protecting just the front door, you're protecting every object behind the door individually."

He added, that goes for applications and IT systems that reach into federal agency data centers, as well as individuals and connected devices.

"Identities are the fabric of the digital economy whether it's within the enterprise or between government and citizen," concluded Wyatt. "The emphasis on continuous authentication... and interoperability are really important, because today we have silos of identity among organizations, which adds friction and risk in the current state that we're in."

The OMB policy memo is a great start to moving in the right direction, he said. His advice to federal and state government agencies: "Recognize that identity initiatives are not unlike a big ERP initiative. The investment in organizational change management and communications management is a critical success factor. Engaging at the right level and across organizations is key as is sponsorship from the top down."

Click here for more information on how ForgeRock can help your agency modernize its ICAM strategy.

fedscoop FORGEROCK

15 FEATURES TO LOOK FOR IN A MODERN ICAM PLATFORM:

To securely manage users, devices and applications accessing federal resources, look for ICAM platforms that offer

Advanced Authentication - To specify the exact conditions in which a resource can be accessed.

Intelligent Authentication - Using easily configured authentication tree frameworks offering more flexibility, choice and security than traditional authenticators.

Mobile Authentication - Providing flexible, simple to deploy, and easy to use mobile authentication, with passwordless logins and frictionless multi-factor authentication.

Adaptive Risk – To assess risks during the authentication process, based on risk scoring.

Authorization – Providing basic to highly advanced, fine-grained entitlements that can be exported and imported via XACML.

Push Authorization – Enable consumers to securely and conveniently approve high risk transactions and events, via mobile phone notifications.

Federation – Share heterogeneous systems or domain boundaries securely using standard identity protocols.

Single Sign-On (SSO) – Provides multiple mechanisms for SSO, in a single domain or multiple domains, with built-in Security Token Service (STS) and multi-protocol hub capability.

Social Sign-On – Has the option to allow users to login directly with their existing social accounts.

Auth 2.0 Proof of Possession & Device Registration – Ensures that a token presented by a web browser accessing an application, or an IoT device connecting to a back-end system, is being presented by its rightful owner.

DevOps and Developer Support – Designed from the ground up for interoperability and easy use by developers.

High Availability and Scalability – Scales easily, and works in complex, multi-site failover environments.

Common Auditing Architecture – Provides comprehensive log data to correlate events and transactions.

Improves User Experience – Enables users to experience more services, using frictionless passwordless logins push authentication through a central platform.

Reduces Operational Cost and Complexity – Can function as a hub, leveraging existing identity infrastructures, and provide multiple integration paths to simplify deployment and operations.